TERMS & DEFINITIONS OF INTEREST FOR COUNTERINTELLIGENCE PROFESSIONALS

Wisdom begins with the definition of terms
-- Socrates

2X. The manager of the counterintelligence and human intelligence missions at various levels of DoD structure, including joint, command, service, and task force. The 2X structure includes the Counterintelligence Coordinating Authority (CICA) and the Human Intelligence Operations Center (HOC). (AR 381-20, Army CI Program, 25 May 2010) Also see *J2X*.

-- Also, the counterintelligence and human intelligence advisor to the C/J/G/S-2. Denotes the 2X positions at all echelons. The 2X staff conducts technical control and oversight for all counterintelligence and human intelligence entities with[in] their operational purview. It coordinates, de-conflicts, and synchronizes all counterintelligence and human intelligence activities at each level of command. (Army FM 2-22.2, Counterintelligence, Oct 2009)

Term also refers to the staff section that the 2X leads.

Interesting historical note: During World War II the counterintelligence element of the Office of Strategic Services (OSS) was known as "X-2" (Counter Espionage Branch). The OSS--predecessor to today's Central Intelligence Agency--was established on 13 June 1942 by order of President Roosevelt. Also "XX" was the Double-Cross System, a World War II counterespionage and deception operation controlled British military intelligence; see *The Double-Cross System*, Yale University Press (1972) by Sir John Cecil Masterman,

603 Referral. See *Section 603 Referral*.

811 Referral. See *Section 811 Referral*.

This Glossary is designed to be a reference for counterintelligence (CI) professionals within the Department of Defense (DoD); however other CI professionals may find it of use. It provides a comprehensive compilation of unclassified terms that may be encountered when dealing with the dynamic discipline of counterintelligence and related activities. Where some words may several meanings within the counterintelligence or intelligence context, a variety of definitions are included.

Definitions within this Glossary cite an original source document. The quotes selected, as well as the views and comments expressed in the shadow boxes are those of the editor and do not necessarily reflect the official policy or position of the Department of Defense, the Office of the National Counterintelligence Executive, the Intelligence Community, the Office of National Intelligence, or the United States Government.

This Glossary is periodically updated. Users are encouraged to submit proposed changes, corrections, and/or additions. Please provide a source citation for any recommended definitions.

Editor: COL Mark L. Reagan (USA Ret), mmreagan@msn.com

A ==========

A-Space (abbreviation for *Analytical Space*). A-Space transitioned to i-Space -- see "i-Space." A-Space was a virtual work environment that provided "analysts" from across the Intelligence Community a common platform for research, analysis and collaboration.

Abort. To terminate a mission for any reason other than enemy action. It may occur at any point after the beginning of the mission and prior to its completion. (previously in Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, hereafter referred to as JP 1-02)*

Abduction. [One of the four basic types of reasoning applied to intelligence analysis,] it is the process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar explanation. (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *deduction; induction; scientific method.*

> For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003) and *Critical Thinking and Intelligence Analysis* by David T. Moore, JMIC Press (2006).

Access. In counterintelligence and intelligence use: 1) A way or means of approach to identify a target; 2) Exploitable proximity to or ability to approach an individual, facility, or information that enables target to carry out the intended mission. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the ability and opportunity to obtain knowledge of classified sensitive information or to be in a place where one could expect to gain such knowledge. (Counterintelligence Community Lexicon, June 2000, hereinafter referred to as CI Community Lexicon)

-- Also, the ability or opportunity to obtain knowledge of classified or sensitive information. (IC Standard 700-1, 4 Apr 2008 and DoD Manual 5200.01-Vol 1, Information Security Program, 24 Feb 2012)

-- Also, the ability and opportunity to obtain knowledge of classified information. (DoD Manual S-5240.09-M, OFCO Procedures & Security Classification Guide, 13 Jan 2011 and DSS Glossary)

> Access generally refers to the ability of a human source/asset (either CI or HUMINT) to perform a specific operational task within the limits of acceptable risk. Types of access include direct, indirect, first-hand, second-hand, etc.

Access Agent. An individual used to acquire information on an otherwise inaccessible target. (Human Derived Information Lexicon Terms and Definitions for HUMINT, Counterintelligence, and Related Activities, April 2008, hereinafter referred to as HDI Lexicon) Also see *agent*.

-- Also, an agent whose relationship or potential relationship with a foreign intelligence personality allows him or her to serve as a channel for the introduction of another controlled agent for the purpose of recruitment of the target. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

---

* Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms* (JP 1-02), as amended; available online at: <http://www.dtic.mil/doctrine/dod_dictionary/> Note: also available online at: <https: //jdeis.js.mil>

-- Also, a person who facilitates contact with a target individual or entry into a facility. (*Spycraft: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda*, 2008; hereinafter referred to as Spycraft)

Access Agents

Another method of identifying and keeping track of suspected intelligence personnel is to recruit people close to suspects, known in the jargon as "access agents." Counterintelligence operators can seek out secretaries, janitors, chauffeurs, interpreters, neighbors, or friends and request that they pass on information about the target's predilections and behavior.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert and Counterintelligence* (1995), pp. 218-219

Access to Classified Information. The ability and opportunity to obtain knowledge of classified information. Persons have access to classified information if they are permitted to gain knowledge of the information or if they are in a place where they would be expected to gain such knowledge. Persons do not have access to classified information by being in a place where classified information is kept if security measures prevent them from gaining knowledge of the information. (JP 1-02)

Accommodation Address. An address for a person or organization that does not occupy the premises. (HDI Lexicon, April 2008)

-- Also, an address where regular posted mail, or sometimes another type of communication, is received and then held for pickup or forwarded, transmitted, or relayed to a member of a intelligence service who does not occupy the premises. Sometimes called a mail drop, live letterbox, or cutout. (AFOSI Manual 71-142, OFCO, 9 Jun 2000 and Spy Book)

-- Also, a "safe" address, not overtly associated with intelligence activity, used by an agent to communicate with the intelligence service for whom he working. (FBI -- Affidavit: USA vs. Robert Philip Hanssen, 16 Feb 2001)

-- Also, an address with no obvious connection to an intelligence agency, used for receiving mail containing sensitive material or information (Spycraft)

-- Also, a prearranged temporary address or location where an intelligence operative may receive mail clandestinely from a third party. (*Encyclopedia of the CIA*, 2003)

ACIC. See *Army Counterintelligence Center*.

Acknowledged SAP. A SAP [Special Access Program] whose existence is acknowledged but its specific details (technologies, materials, techniques, etc.) are classified as specified in the applicable security classification guide. (DoDD 5205.07, SAP Policy, 1 July 2010) Also see *unacknowledged SAP*.

-- Also, a Special Access Program that is acknowledged to exist and whose purpose is identified (e.g., the B-2 or the F-117 aircraft program) while the details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and the risk of compromise. Program funding is generally unclassified. Note: Members of the four Congressional Defense Committees are authorized access to the program. (DSS Glossary)

Acoustic Intelligence (ACINT). Intelligence derived from the collection and processing of acoustic phenomena. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Acoustical Security. Those security measures designed and used to deny aural access to classified information. (DSS Glossary and AR 381-14, Technical Counterintelligence, 30 Sep 2002)

Acoustical Surveillance. Employment of electronic devices, including sound-recording, -receiving, or -transmitting equipment, for the collection of information. (JP 1-02)

Acquisition Special Access Program. A special access program established primarily to protect sensitive research, development, testing, and evaluation or procurement activities in support of sensitive military and intelligence requirements. (DSS Glossary)

Acquisition Security Database (ASDB). A classified DoD database designed to support Program Managers, Research Technology Protection (RTP), Anti-Tamper, Counterintelligence, OPSEC, and Security personnel supporting DoD Acquisition Programs with automated tools and functionality to enable efficient and cost-effective identification and protection of Critical Technologies (CT) and Critical Program Information (CPI).

-- Also, [proposed definition] the DoD horizontal protection database providing online storage, retrieval, and tracking of CPI and supporting Program Protection documents in order to facilitate comparative analysis of defense systems' technology and align CPI protection activities across the DoD. (*Draft* DoDI 5200.39, CPI Identification and Protection within RDA Programs)

> All DoD CI personnel providing CI support to RDA should obtain an ASDB account.
>
> ASDB is a key database for CI support to Research Development & Acquisition (RDA) which provides on-line storage and retrieval of Program Protection Plans (PPPs), Anti-Tamper Plans, Technology Assessment/Control Plans, Multi-Disciplined Counterintelligence Threat Assessments, Program Protection Implementation Plans, OPSEC Plans and Security Classification Guides (SCGs).
>
> On SIPRNet see <https://asdb.strikenet.navy.smil.mil>

Acquisition Systems Protection (ASP). The safeguarding of defense systems anywhere in the acquisition process as defined in DoD Directive 5000.1, the defense technologies being developed that could lead to weapon or defense systems, and defense research data. ASP integrates all security disciplines, counter-intelligence, and other defensive methods to deny foreign collection efforts and prevent unauthorized disclosure to deliver to our force uncompromised combat effectiveness over the life expectancy of the system. (DoD 5200.1-M, Acquisition Systems Protection Program, Mar 1994)

Actionable Intelligence. Intelligence information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process. (ICS Glossary and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Active Cyber Defense. The Department of Defense's real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities to defend networks and systems. (DoD Strategy for Operating in Cyberspace, May 2011)

Active Measures. In Russian, *aktivnyye mery* or *aktivnyye meropriyatiya*. …Soviet KGB tradecraft jargon for operation involving disinformation, manipulation of communist-front organizations, agent-of-influence operations, forgeries and counterfeiting. (The CIA Insider's Dictionary by Leo D. Carl, 1996)

-- Also, influence operations organized by the Soviet government. These include white, gray, and black propaganda, as well as disinformation. (Encyclopedia of Espionage, Intelligence, and Security by The Gale Group, Inc)

-- Also, the Soviet term for strategies that in the West would be described as black propaganda. The purpose was to denigrate ‘‘the main adversary’’ by using whatever disinformation channels were available to spread false stories, plant bogus reports into the media, spread untrue rumors, and support Soviet foreign policy objectives by undermining confidence in its opponents. (Historical Dictionary of Cold War Counterintelligence by Nigel West)

-- Also, a form of political warfare conducted by Soviet intelligence and security services to influence the course of world events. Active measures ranged “from media manipulations to special actions involving various degrees of violence" and included disinformation, propaganda, counterfeiting official documents, assassinations, and political repression, such as penetration in churches, and persecution of political dissidents. (Extract from Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive: The KGB in Europe and the West*, 2000)

The scale of the Soviet’s active measures campaign, and the KGB’s involvement in the development and execution of specific items of disinformation was disclosed by a KGB officer, Anatoli Golitsyn, following his defection in Helsinki in December 1961.

_____

Active measures proved highly relevant to the Western counterintelligence community because it was in the KGB’s interests to subvert the CIA, by suggesting it was driven by corruption and influenced by dishonest politicians. The key to successful campaigns proved to be the deliberate distortion of known facts, mixed with an element of fabrication. […] In addition, there is some evidence to suggest that the KGB attempted to protect some of its most vital sources by interfering in Western mole hunts through the introduction of false or misleading clues to throw the investigations onto unproductive lines of inquiry.

-- Nigel West, *Historical Dictionary of Cold War Counterintelligence*

_____

For more information see: *Soviet Active Measures in the "Post-Cold War" Era 1988-1991*, A Report Prepared at the Request of the United States House of Representatives Committee on Appropriations by the United States Information Agency, June 1992. Copy available on line at: <http://intellit.muskingum.edu/russia_folder/pcw_era/index.htm>

Also see *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference* by Fletcher Schoen and Christopher J. Lamb, Institute for National Strategic Studies, National Defense University, June 2012; copy available on line at: <http://www.ndu.edu/inss/news.cfm?action=view&id=160>

Activity Based Intelligence (ABI). A discipline of intelligence where the analysis and subsequent collection is focused on the activity and transactions associated with an entity, a population or an area of interest. (NGA)

ABI is a multi-intelligence approach based on persistent collection of intelligence over a broad area from multiple sources. Geospatial Intelligence (GEOINT), coupled with human domain analytics, is the foundation of ABI.

The National Geospatial-Intelligence Agency (NGA) is at the forefront of the ABI push within the Intelligence Community. The ubiquitous nature of geo-spatial intelligence (GEOINT), coupled with Human Domain Analytics (HDA), forms the true foundation of ABI.

See **“**A Brief Overview of Activity Based Intelligence and Human Domain Analytics,” (Sep 2012) by Mark Phillips available on line at: <http://trajectorymagazine.com/images/winter2012/A_Brief_Overview_of_ABI.pdf>

_____

ABI is an inherently multi-INT approach to activity and transactional data analysis to resolve unknowns, develop object and network knowledge, and drive collection.

-- Cited by Letitia A. Long, Director NGA, in her article “Activity Based Intelligence: Understanding the Unknown,” in *The Intelligencer: Journal of U.S. Intelligence Studies*, Vol 20 No. 2, Fall/Winter 2013, p. 7

_____

ABI is really a new tradecraft that builds on top of something that's been around for awhile called 'patterns of life.'

-- Jordan Becker, Vice President & General Manger for GEOINT-ISR, BAE Systems, Quoted in "GEOINT Tradecraft: Human Geography" by Greg Slabodkin, *DefenseSystems*, Vol 7, No. 6, Oct/Nov 2013, p. 7

Activity Security Manager. The individual specifically designated in writing and responsible for the activity's information security program, which ensures that classified information (except SCI which is the responsibility of the SSO appointed by the senior intelligence official) and CUI are properly handled during their entire life cycle. This includes ensuring information is appropriately identified, marked, stored, disseminated, disposed of, and accounted for, as well as providing guidance on the handling of security incidents to minimize adverse effects and ensure that appropriate corrective action is taken. The security manager may be assigned responsibilities in other security disciplines such as personnel and physical security, etc. (DoD Manual 5200.01-Vol 1, Information Security Program, 24 Feb 2012)

Ad-Hoc Requirement (AHR). A HUMINT collection requirement with a limited emphasis, based on time or other requirements. (Defense HUMINT Enterprise Manual 3301.02, Vol II Collection Operations, 23 Nov 2010)

-- Also, an intelligence need that was not addressed in [a] standing tasking. (National HUMINT Glossary)

Adaptive Planning. The joint capability to create and revise plans rapidly and systematically, as circumstances require. Also see *Adaptive Planning and Execution (APEX); intelligence planning*.

Adaptive Planning and Execution (APEX). A Department of Defense system of joint policies, processes, procedures, and reporting structures, supported by communications and information technology, that is used by the joint planning and execution community to monitor, plan, and execute mobilization, deployment, employment, sustainment, redeployment, and demobilization activities associated with joint operations. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Adequate Security. Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. (NIST, Glossary of Key Information Security Terms, May 2013)

Adherents. [In counterterrorism usage] individual who have formed collaborative relationships with, act on behalf of, or are otherwise inspired to take action in furtherance of the goals of al-Qa'ida—the organization and ideology—including b engaging in violence regardless of whether such violence is targeted at the United States, its citizens, or its interests. (National Strategy for Counterterrorism, June 2011)

Ad-hoc HUMINT Requirement (AHR). A HUMINT collection requirement with a limited emphasis, based upon time or other requirements. (DHE-M 3301.001, DIA HUMINT Manual, Vol I, 30 Jan 2009 w/ chg 2)

Adjudication. Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted or retain eligibility for access to classified information, and continue to hold positions requiring a trustworthiness decision. (DSS Glossary)

Administrative Control (ADCON). Direction or exercise of authority over subordinate or other organizations in respect to administration and support. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Admission. A polygraph examinee's acknowledgement of a fact or a capable statement associated with a relevant issue. (AR 381-20, Army CI Program, 25 May 2010)

Advanced Persistent Threat (APT). An extremely proficient, patient, determined, and capable adversary, including two or more of such adversaries working together. (DoDI 5205.13, Defense Industrial Base Cyber Security/Information Assurance Activities, 29 Jan 2010)

-- Also, an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. (NIST, Glossary of Key Information Security Terms, May 2013)

-- Also, a cyberattack campaign with specific, targeted objectives, conducted by a coordinated team of specialized experts, combining organization, intelligence complexity, and patience. (Cybersecurity and Cyberwar)

-- Also, cyber attacks mounted by organizational teams that have deep resources, advanced penetration skills, specific target profiles and are remarkably persistent in their efforts. They tend to use sophisticated custom malware that can circumvent most defenses, stealthy tactics and demonstrate good situational awareness by evaluating defenders responses and escalating their attack techniques accordingly. (<www.hackingtheuniverse.com/infosec/isnews/advanced-persistent-threat>; accessed 5 Jan 2010)

The technological (cyber) APT has been used by actors in many nations as a means to gather intelligence on individuals, and groups of individuals of interest. See additional information at:
-- <http://www.businessweek.com/magazine/content/08_16/b4080032220668.htm>
-- <http://www.prometheus-group.com/blogs/36-web-security/152-anatomy-of-apt.html>
-- <http://en.wikipedia.org/wiki/GhostNet>

Also see Mandiant Report, *APT1: Exposing One of China's Cyber Espionage Units*, undated (circa Feb 2013); copy available at: <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>

Adverse Information. Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security. (DoD Manual 5220.22-M, National Industrial Security Program Operating Manual, 28 Feb 2006)

Adversarial Supply Chain Operation (ASCO). ASCOs are the actions taken across the entire supply chain life-cycle to attck and exploit the supply chain. ASCOs can include threatening or exploiting the supply chains. These operations are carried out through compromise, subversion, and exposure of material and components to or through the supply chain. The implications of ASCOs are possible adverse effects to mission assurance affecting material, system operations and key capabilities. (DIA) Also see *supply chain, supply chain risk, supply chain risk management*.

Adversary. An individual, group, organization, or government that must be denied essential information. (DoD Manual 5200.1-M, Acquisition Systems Protection Program, Mar 1994)

-- Also, a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

-- Also, any individual, group, organization, or government that conducts or has the intent and capability to conduct activities detrimental to the US Government or its assets. Adversaries may include intelligence services, political or terrorist groups, criminals, and private interests. (CI Community Lexicon)

-- Also, any foreign individual, group, organizations, or government that conducts or has the intent and capability to conduct activities detrimental to the national security or defense of the United States or its assets, including foreign intelligence services, political or international terrorist groups, and insurgents. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (NIST, Glossary of Key Information Security Terms, May 2013)

Adversary Collection Methodology. Any resource and method available to and used by an adversary for the collection and exploitation of sensitive/critical information or indicators thereof. (DSS Glossary)

Adversary Intelligence Systems. Resources and methods available to and used by an adversary for the collection and exploitation of critical information or indicators thereof. (DoDD 5205.02E, DoD OPSEC Program, 20 Jun 2013)

Advisory Tasking. A term used in collection management to refer to collection notices that are discretionary rather than directive in nature, with the receiving agency determining whether the requirement is relevant to the mission of the agency and whether the agency has the resources to collect against it. (AR 381-20, Army CI Program, 25 May 2010)

AFOSI. Acronym, see *Air Force Office of Special Investigations*.

Agency. In intelligence usage, an organization or individual engaged in collecting and/or processing information. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Agent. In intelligence usage, one who is authorized and trained to obtain or to assist in obtaining information for intelligence or counterintelligence purposes. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *agent of influence; agent of a foreign entity; asset; foreign intelligence agent.*

-- Also, a person who engages in clandestine intelligence activities under the direction of an intelligence organization, but is not an officer, employee, or co-opted worker of that organization. (National HUMINT Glossary)

-- Also, an individual other than an officer, employee, or co-opted worker of an intelligence service to whim specific intelligence assignments are given by an intelligence service. An agent in a target country can be operated by a legal or illegal residency or directly by the center. An agent can be of any nationality. (FBI FCI Terms)

-- Also, 1) A person who engages in clandestine intelligence activity under the direction of an intelligence organization but who is not an officer, employee, or co-opted worker of that organization; 2) An individual who acts under the direction of an intelligence agency or security service to obtain, or assist in obtaining, information for intelligence or counterintelligence proposes; [and] 3) One who is authorized or instructed to obtain or assist in obtaining information for intelligence or counterintelligence purposes. (ICS Glossary)

> *Typically, the aim of an espionage operation is to recruit an **agent** [emphasis added], usually a foreign person, to carry out the actual spying. The person who targets, recruits, trains, and runs the agent is, in American parlance, the 'case officer.'*
>
> -- Arthur S. Hulnick, "Espionage: Does It Have a Future in the 21st Century?" *The Brown Journal of World Affairs;* v XI: n 1 (2004).

…[T]ypes of agents—singletons, sleepers, illegal spies actively running one or more sources, illegal residents running a group of other illegals, and so forth.

-- Peter Wright, *Spycatcher* (1987), p. 139

Espionage is one of the toughest games played. An agent in the right place is hard to find, but when he is found he should be regarded as a pearl beyond price.

-- David Nelligan, *The Spy in the Castle* (1968)

Agent-in-Place. A person who remains in a position while acting under the direction of a hostile intelligence service, so as to obtain current intelligence information. It is also called a recruitment-in-place. (FBI -- Affidavit: USA *vs*. Robert Philip Hanssen, 16 Feb 2001) Also see *recruitment-in-place (RIP).*

Agent of Influence. An agent of some stature who uses his or her position to influence public opinion or decision making to produce results beneficial to the country whose intelligence service operates the agent. (AFOSI Manual 71-142, OFCO, 9 Jun 2000) [Originally a Soviet term]

-- Also, a person who is directed by an intelligence organization to use his position to influence public opinion or decision-making in a manner that will advance the objective of the country for which that organization operates. (ICS Glossary)

-- Also, an individual who acts in the interest of an adversary without open declaration of allegiance and attempts to exercise influence covertly, but is not necessarily gathering intelligence or compromising classified material, is known as an agent of influence. (Historical Dictionary of Cold War Counterintelligence, 2007)

-- Also, an agent operating under intelligence instructions who uses his official or public position, and other means, to exert influence on policy, public opinion, the course of particular events, the activity of political organizations and state agencies in target countries. (KGB Lexicon: The Soviet Intelligence Officer's Handbook, edited by KGB archivist Vasiliy Mitrokhin, 2002).

An agent of influence is a person who uses his or her position, influence, power, and credibility to promote the objectives of an alien power…, in ways unattributable to that power, Such agents may operate openly or surreptitiously, and their effectiveness depends on their position and the extent to which they are prepared to misuse it, but any degree of deliberate support for an adversary power, especially if applied in an underhanded way, savours of treachery.

-- Chapman Pincher, *Traitors: The Anatomy of Treason*, First U.S. Edition (1999), p. 34

Agent of a Foreign Entity. A person who engages in intelligence activities under the covert direction of a foreign intelligence or security entity, but is not an officer, employee, or co-opted worker of that entity. (ONCIX Analytic Chiefs Working Group, Jan 2011) Also see *agent; agent of a foreign power; asset.*

Agent of a Foreign Power. Means: (1) any person other than a United States person, who – (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (C) engages in international terrorism or activities in preparation therefore; or (2) any person who - (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power; (D) knowingly enters the United States under a false or fraudulent identity for or on behalf

of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C). (Source: 50 USC § 1801b) Also see *foreign power*.

Agent Handler. An [intelligence] officer or principal agent who directly manages an agent or agent network. (National HUMINT Glossary) Also see *case officer*.

Agent Net. An intelligence gathering unit of agents supervised by a principal agent who is operating under the direction of an intelligence officer. An agent net can operate in either the legal or illegal field. (ICS Glossary and FBI FCI Terms)

Agent Recruitment Cycle (ARC). See *recruitment cycle*.

Air Force Office of Special Investigations (AFOSI). U.S. Air Force's major investigative service; a federal law enforcement and investigative agency operating throughout the full spectrum of conflict, seamlessly within any domain; conducting criminal investigations and providing counterintelligence services. (<www.osi.andrews.af.mil>; accessed 27 June 2012)

AFOSI Mission: Identify, exploit and neutralize criminal, terrorist and intelligence threats to the Air Force, Department of Defense and U.S. Government.

AFOSI Capabilities:
-- Protect critical technologies and information
-- Detect and mitigate threats
-- Provide global specialized services
-- Conduct major criminal investigation
-- Engage foreign adversaries and threats offensively

Source: AFOSI web site (accessed 27 June 2012)

Fact sheet at: <http://www.osi.andrews.af.mil/library/factsheets/factsheet_print.asp?fsID=4848&page=1>

All-Source Analysis. An intelligence activity involving the integration, evaluation, and interpretation of information from all available data sources and types, to include human intelligence, signals intelligence, geospatial intelligence, measurement & signature intelligence, and open source intelligence. (DoDD 5240.01, DoD Intelligence Activities, 27 Aug 2007) Also see a*nalysis; analysis and production*; *counterintelligence analysis.*

-- Also, an intelligence activity involving the integration, evaluation, and interpretation of information from all available data sources and types, to include HUMINT, SIGINT, MASINT, GEOINT, OSINT, and CI. (DoDI 5105.21, DIA, 18 Mar 2008) {note this definition includes *counterintelligence*}.

All-source analysis can transform raw intelligence, data, and information into knowledge and understanding.

Integrated all-source analysis should also inform and shape strategies to collect more intelligence…. The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots."

-- Final Report of the National Commission on Terrorist Attacks Upon the United States (2004)

All-Source Intelligence. 1) Intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence. 2) In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, intelligence information derived from several or all the intelligence disciplines, including SIGINT, HUMINT, MASINT, OSINT, and GEOINT. (ODNI, U.S. Intelligence – An Overview 2011)

-- Also, the integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations. (ADRP 2-0, Intelligence, Aug 2012)*

> * Note: supersedes the definition in Army FM 2-0, *Intelligence*, 23 Mar 2010.
>
> ADRP = Army Doctrinal Reference Publication.
> ADRPs are available online at <hhtps://armypubs.us.army.mil/doctrine/index.html>

Alliance. The relationship that results from a formal agreement between two or more nations for broad, long-term objectives that further the common interests of the members. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Alias. A false identity used while carrying out authorized activities and lawful operations. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

-- Also, an alternative name, used for cover purposes. (Defense HUMINT Enterprise Manual 3301.002, Vol II, Collection Operations, 23 Nov 2010)

-- Also, a false name. (National HUMINT Glossary)

-- Also, a false name assumed by an individual for a specific and often temporary purpose, i.e., to conceal a true identity from persons or organizations with whom he or she is in contact. Also called a pseudonym or cover name. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, an assumed name, usually consisting of a first and last name, used by an individual for a specific and often temporary purpose. (FBI FCI Terms)

Alternate Meet. A prearranged meeting that takes place in the event a regularly scheduled meet is missed for any reason. (FBI FCI Terms)

Alternative Analysis. [Analysis that] involves a fairly intensive, though time limited, effort to challenge assumptions or to identify alternative outcomes, depending on the technique employed, with the results captured, implicitly or explicitly, in a written product delivered to relevant policy-makers.(CIA - Sherman Kent Center for Intelligence Analysis)

> Alternative analysis includes techniques to challenge analytic assumptions (e.g., “devil’s advocacy”), and those to expand the range.
>
> See article “Rethinking “Alternative Analysis” to Address Transnational Threats” at: <https://www.cia.gov/library/kent-center-occasional-papers/vol3no2.htm>

Alternative Compensatory Control Measures (ACCM). Measures designed to safeguard sensitive intelligence and operations when normal security measures are either not sufficient to achieve strict controls over access to information, but where strict SAP [Special Access Program] access controls are either not required or are too stringent. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, used to safeguard sensitive intelligence or operations and support information (acquisition programs do not qualify) when normal measures are insufficient to achieve strict need-to-know controls, and where Special Access Program controls are not required. (DSS Glossary)

> ACCMs are not Special Access Programs (SAPs). Guidance for ACCMs is contained in DoD Manual 5200.01, Vol 3, *DoD Information Security Program: Protection of Classified Information*, 24 Feb 2012,

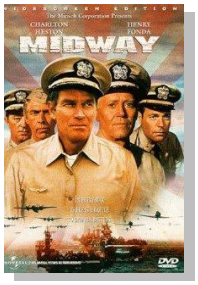
Ambassador. Diplomatic official of the highest rank who is accredited to a foreign sovereign or government, or to an international organization, as the resident representative of the sending government or appointed for a specific diplomatic assignment. (Department of State) Also see *Chief of Mission*.

A U.S. ambassador serving abroad symbolizes the sovereignty of the United States and serves as the personal representative of the President of the United States. Ambassadorial duties include negotiating agreements, reporting on political, economic and social conditions, advising on policy options, protecting American interests, and coordinating the activities of all U.S. Government agencies and personnel in the country.

Analysis. [In intelligence usage] the process by which information is transformed into intelligence; a systemic examination of information to identify significant facts, make judgments, and draw conclusions. (ODNI, U.S. Intelligence – An Overview 2011) Also see a*nalysis and production; all-source analysis; counterintelligence analysis; intelligence analysis*.

-- Also, the process by which collected information is evaluated and integrated with existing information to produce intelligence that describes the current—and attempts to predict the future—impact of the threat, terrain and weather, and civil considerations on operations. (Army FM 2-0, Intelligence, 23 Mar 2010)

-- Also, a stage in the intelligence processing cycle whereby collected information is reviewed to identify significant facts; the information is compared with and collated with other data, and conclusions, which also incorporate the memory and judgment of the intelligence analyst, are derived from it. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)



INTELLIGENCE ANALYSIS…

"Joe, you're guessing!"
Navy Capitan Matthew Garth
(Charlton Heston)

"Sir, we like to call it analysis."
Naval Intelligence Officer Joseph Rochefort
(Harold Rowe "Hal" Holbrook, Jr.)
-- The movie *Midway* (1976)

Analysis is the process by which people transform information into intelligence. It includes integrating, evaluating, and analyzing all available data -- which is often fragmented and even contradictory -- and preparing intelligence products.

Former DCI Richard Helms noted that despite all the attention focused on the operational (collection) side of intelligence, *analysis* is the core of the process to inform decision makers.

_____

It is of the highest importance in the art of detection to be able to recognize, out of a number of facts, which are incidental and which are vital.

-- Sherlock Holmes
From A. Conan Doyle's "The Reigate Squire" June 1893
(M. Hardwick, *The Complete Guide to Sherlock Holmes,* 1986, pp. 86-87)

_____

Analysis is the thinking part of the intelligence process
-- James B. Bruce and Roger Z. George

_____

It is not enough, of course, simply to collect information. Thoughtful analysis is vital to sound decisionmaking.
-- President Ronald Reagan (4 Dec 1981)

_____

…[A]nalysis must always be timely, responsive and relevant to… customer's needs.

-- LTG Michael T. Flynn, USA, Director Defense Intelligence Agency (Jul 2012)

Intelligence analysts select and filter information; they interpret the resultant evidence, put it into context, and tailor it to meet… customers' needs. In short, analysts and analysts only, create intelligence.

-- David T. Moore, "Species of Competencies for Intelligence," *American Intelligence Journal* (2005)

Analysis must do more than just describe what is happening and why; it must identify a range of opportunities… Analysis is the key to making sense of the data and finding opportunities to take action.

-- DNI 2006 Annual Report of the US Intelligence Community (Feb 2007)

The primary purpose of analytic effort is "sensemaking" and understanding, not producing reports; the objective of analysis is to provide information in a meaningful context, not individual factoids.

-- Jeffrey R, Cooper, *Curing Analytical Pathologies*, Center for the Study of Intelligence (Dec 2005), p. 42

Today, U.S. intelligence analysts spend roughly 80 percent of their time gathering intelligence but only 20 percent analyzing it.

-- LTG Bob Noonan (USA Ret) and Greg Wenzel, "Fixing the 'I' in ISR," *DefenseNews*, 24 Sep 2012, p. 45

Analysts are the voice of the Intelligence Community

-- WMD Report (31 Mar 2005), p. 388

Analysts must absorb information with the thoroughness of historians,
organize it with the skill of librarians, and disseminate it with the zeal of journalists.

--TRADOC Pam 525-2-1, *US Army Functional Concept for Intelligence 2016-2028*, 13 Oct 2010; p. 66

Intelligence analysis is inherently an intellectual activity
that requires knowledge, judgment, and a degree of intuition.

Selected references for **intelligence analysis**:

Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency), 1999.
Copy available online at: <http://www.archive.org/details/PsychologyOfIntelligenceAnalysis>
Also at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/index.html>

Richards J. Heuer, Jr. and Randolph H. Pherson, *Structured Analytical Techniques for Intelligence Analysis* (Washington, DC; CQ Press), 2010.

Richards J. Heuer, Jr, *Improving Intelligence Analysis with ACH*, 2005.
This learning aid extracts, revises, and partially updates those portions of the author's book, *Psychology of Intelligence Analysis* [cited above], that deal with Analysis of Competing Hypotheses (ACH) and with how and why the ACH software helps intelligence analysts reduce the risk of surprise. ACH software is available at: <http://www2.parc.com/istl/projects/ach/ach.html>

Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: Origins, Obstacles, and Innovation* (Washington, DC: Georgetown University Press), 2008.

Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach*, rev. ed. (Washington, DC: CQ Press), 2007; also paperback 2012

David A. Schum, *Evidence and Inference for the Intelligence Analyst* (Lanham, MD: University Press of America) 1987.

Morgan Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*, rev. ed. (New York: Three Rivers Press), 1998.

Robert S. Sinclair, *Thinking and Writing: Cognitive Science and Intelligence Analysis,* revised edition (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency), 2010.
Copy available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/thinking-and-writing.html>

David T. Moore, *Sensemaking: A Structure for an Intelligence Revolution* (Washington, DC: National Defense Intelligence College, 2011).
Copy available at <http://ni-u.edu/ni_press/pdf/Sensemaking.pdf>

A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis (Washington, DC: U.S. Government), 2009.
Copy available at: <https://www.cia.gov/library/ publications/publications-rss-updates/tradecraft-primer-may-4-2009.html>

A Compendium of Analytic Tradecraft Notes, Volume I, Notes 1-10, reprinted (Washington, DC: Central Intelligence Agency), 1997.
Copy available at: <http://www.au.af.mil/au/awc/awcgate/cia/tradecraft_notes/contents.htm>

The Sherman Kent Center for Intelligence Analysis Occasional Papers, (CIA).
*A*vailable online at: <https://www.cia.gov/library/kent-center-occasional-papers/index.html>

Frank Watanabe, "Fifteen Axioms for Intelligence Analysts." *Studies in Intelligence*, CIA, Semiannual Edition, No. 1, 1997, pp. 45-47.
Copy available on line at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol40no5/pdf/v40i5a06p.pdf>

Also see Mark Lowenthal, PhD, *Intelligence: From Secrets to Policy,* 5th Edition (CQ Press), 2011.

Analysis and Production. In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012) Also see *analysis; all-source analysis; counterintelligence analysis.*

-- Also, the ability to integrate, evaluate, and interpret information from available sources and develop intelligence products that enable situational awareness. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Analysis of Competing Hypothesis (ACH). Identification of alternate explanations (hypothesis) and evaluation of all evidence that will disconfirm rather that confirm hypotheses. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005)

ACH a highly effective technique when there is a large amount of data to absorb and evaluate. It is particular appropriate for controversial issues when analysts want to develop a clear record that shows what theories they have considered and how they arrived at their judgments.

See Richards J. Heuer, Jr, *Improving Intelligence Analysis with ACH*, Nov 2005 (Learning Aid, ACH Version 2.0). This learning aid extracts, revises, and partially updates those portions of the author's book, *Psychology of Intelligence Analysis* [cited above], that deal with Analysis of Competing Hypotheses (ACH) and with how and why the ACH software helps intelligence analysts reduce the risk of surprise.

ACH software available for download at: <http://www2.parc.com/istl/projects/ach/ach.html>

Analysis Report. A type of DoD CI analytical product prepared IAW DoDI 5240.18; it may require in-depth study and research, but generally is not as involved as an assessment. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013). Also see *Counterintelligence Analytical Product*.

Analytic Outreach. The open, overt, and deliberate act of an IC [Intelligence Community] analyst engaging with an individual outside the IC to explore ideas and alternate perspectives, gain new insights, generate new knowledge, or obtain new information. (ICD 205, Analytic Outreach, 16 Jul 2008)

Analytic Tradecraft. The practiced skill of applying learned techniques and methodologies appropriate to an issue to mitigate, gain insight, and provide persuasive understanding of the issue to members of the U.S. Government and its allies. (DIA, *A Tradecraft Primer: Basic Structured Analytic Techniques,* March 2008).

Note: The source document (First Edition) cited above is no longer available online. The current version: *Tradecraft Primer: Structured Analytic Techniques*, 3rd Edition (3 March 2010) is now Defense Intelligence Reference Document, *Analytic Methodologies*, DIA-01-1003-001A, and is controlled as UNCLASSIFIED//FOR OFFICIAL USE ONLY.

Anomalies. Foreign power activity or knowledge, inconsistent with the expected norms that suggest prior foreign knowledge of US national security information, processes or capabilities. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007 with change 1 dated 30 Dec 2010) See *anomalous activity; anomaly*.

-- Also, irregular or unusual activities that may cue the analyst on the existence of FISS and ITO [international terrorist organizations] activity. (Army FM 2-22.2, Counterintelligence, Oct 2009)

CI anomalies differ from CI indicators (see *potential espionage indicators*). CI anomalies surface as a result of FIE activities, whereas CI indictors are manifested in an insider's actions, activities, and/or behaviors.

_____

Recognizing the importance of CI anomalies in the early detection and neutralization of espionage, a White House Memorandum of August 23, 1996 called for a more systematic approach to the handling of CI anomalies. The memorandum emphasized the need for, and value of, timely participation of CI elements in detecting and reporting CI anomalies indicating threats to U.S. national security.

-- DIA tri-fold, *Counterintelligence Anomalies: What are They and Why Should We Look for Them?*, Jan 2012

_____

Look for the anomalies…
Look for the odd bits that seem to be out of focus, or out of sequence.
Look for the inexplicable.

-- Sean Flannery, *Crossed Swords*, 1989

Anomalous Activity. Irregular or unusual deviations from what is usual, normal, or expected; activity inconsistent with the expected norm. See *anomalies; anomaly*.

-- Also, [in DoD cyber usage] network activities that are inconsistent with the expected norms that may suggest FIE [Foreign Intelligence Entity] exploitation of cyber vulnerabilities or prior knowledge of U.S. national security information, processes, or capabilities. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010 with change 1 dated 16 Oct 2013)

Anomalous Behavior Analysis

[The CI] analyst seeks out strange or puzzling behavior pointing to a counterintelligence problem even before it is known to exist. There are various kinds of anomalous behaviors that might tip off an analyst about a foreign intelligence service's successful operations. One is strategic behavior. When a foreign government starts using the same secret technology as another government, the analyst who finds this out may hypothesize that it because such secrets have been stolen.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 196

Anomaly. Activity or knowledge, outside the norm, that suggests a foreign entity has foreknowledge of U.S. information, processes, or capabilities. (DoDD 5240.06, CIAR, 17 May 2011 with change 1 dated 30 May 3013) See *anomalies, anomalous activity, anomaly-based detection.*

Anomaly-based Detection. The process of comparing CI, security, IA [Information Assurance], LE [law enforcement], and AT/FP [antiterrorism and force protection] behaviors and activities that are deemed normal against other observed events to identify significant deviations and or anomalous behavior. (DoDI 5240.26, Countering Espionage, International Terrorism, and Counterintelligence Insider Threat, 4 May 2012 with change 1 dated 15 Oct 2013)

-- Also, the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. (NIST, Glossary of Key Information Security Terms, May 2013)

Anomaly Detection

The systems and processes used to assess deviant or unscheduled activities or presences which may indicate anomalous activities or unauthorized access. This interpretation assumes a baseline norm from which deviations are assumed to indicate some type of intrusion.

-- Julie K. Petersen, *Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications* (2001)

Anti-Tamper. Systems engineering activities intended to deter and/or delay exploitation of critical technologies in a U.S. defense system in order to impede countermeasure development, unintended technology transfer, or alteration of a system. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008)

Note: DoDI 5200.39 under revision, proposed revised definition for AT: *Systems engineering activities intended to prevent, or delay exploitation of CPI in U.S. defense systems to impede countermeasure development, unintended technology transfer, or alteration of a system due.* (Draft circa Feb 2014)

DoD Anti-Tamper Executive Agent: chartered by the Under Secretary of Defense (Acquisition, Technology, and Logistics), and assigned to the Directorate for Special Programs, Office of the Assistant Secretary of the Air Force for Acquisition.

Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. (JP 1-02; and JP 3-07.2, Antiterrorism, 24 Nov 2010)

Also see DoDI 2000.12, *DoD Antiterrorism Program*, 1 Mar 2012 (w/ chg 1) and DoD O-2000.12-H, *DoD Antiterrorism Handbook*, 1 February 2004

Apportionment. In the general sense, distribution for planning of limited resources among competing requirements. (JP 1-02)

Apprehension. The taking of a person into custody or the military equivalent of "arrest." Under Rule 304, Manual for Courts Martial (MCM), the restraint of a person by oral or written order directing him to remain within specified limits. (AR 381-20, Army CI Program, 25 May 2010)

Area of Responsibility (AOR). The geographical area associated with a combatant command within which a geographic combatant commander has authority to plan and conduct operations. (JP 1-02)

Army Counterintelligence Center (ACIC). The Army's counterintelligence analysis and production center.

ACIC's mission is to provide timely, accurate, effective multidiscipline counterintelligence analysis in support of the US Army combating terrorism program, ground systems technologies, and counterintelligence investigations, operation, and activities. The ACIC is a subordinate unit of the 902d Military Intelligence Group, US Army Intelligence and Security Command, located at Fort Meade, Maryland.

Army G-2X. The element which manages and provides technical control of the CI and HUMINT missions in the Army. (AR 380-20, Army CI Program, 25 May 2010)

Arrest. The act of detaining in legal custody. An "arrest" is the deprivation of a person's liberty by legal authority in response to a criminal charge. (www.ojp.usdoj.gov; accessed 29 Apr 2013)

ASDB. Acronym, see *Acquisition Security Database*.

Assassination. The murder or attempted murder of DoD personnel for political or retaliatory reasons by international terrorists or agents of a foreign power. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, to murder (usually a prominent person) by a sudden and/or secret attack, often for political reasons. (Wikipedia; accessed 15 Feb 2010)

"[The KGB] did everything from plotting ways to poison the capital's water systems to drawing up assassination plans for US leaders."

-- Oleg Kalugin, Former Major General in the KGB
as cited in Andrew & Mitrokhin, *The Mitrokhin Archive* (1999)

Assassination constitutes an act of murder that is prohibited by international law and Executive Order 12333. In general, assassination involves murder of a targeted individual for political purposes. Example, the 1978 "poisoned-tip umbrella" killing of Bulgarian defector Georgi Markov by Bulgarian State Security agents on the streets of London falls into the category of an act of murder carried out for political purposes, and constitutes an assassination.

"Wet Work" – a term originated within the Soviet intelligence – describes the art of assassination. In 1965, Peter Deriabin, a KGB defector, testified to a Senate committee –

> *"The [KGB] thirteenth department is responsible for assignation and terror. This Department is called the department of wet affairs, or in Russian 'Mokrie Dela'…. 'Mokrei' means 'wet' and in this case 'mokrie' means 'blood wet'."*

Unquestionably the most neglected aspect of U.S. counterintelligence. EO 12333 specifically provides that "*Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against… **assassinations** [emphasis added] conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities."

The word *assassin* is derived from the word Hashshashin (Arabic: حشّاشين, ħashshāshīyīn, also Hashishin, Hashashiyyin, or Assassins). It referred to the Nizari branch of the Ismāʿīlī Shia founded by the Persian Hassan as-Sabbah during the Middle Ages. They were active in Iran from the 8th to the 14th centuries, and also controlled the castle of Masyaf in Syria. The group killed members of the Muslim Abbasid, Seljuq, and Christian Crusader élite for political and religious reasons.

The important thing to know about any assassination or an attempted assassination is not who fired the shot, but who paid for the bullet.

-- Eric Ambler, *A Coffin for Dimitrios* (1939)

Assessment. 1) a continuous process that measures the overall effectiveness of employing joint force capabilities during military operations; 2) determination of the progress toward accomplishing a task, creating a condition, or achieving an objective; 3) analysis of the security, effectiveness, and potential of an existing or planned intelligence activity; and 4) **[in human source operations] judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents."** [emphasis added] (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

-- Also, [In CI analysis usage] a type of DoD CI analytical product prepared IAW DoDI 5240.18; it requires in-depth study and research. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013). Also see *Counterintelligence Analytical Product*.

-- Also, [in intelligence usage], appraisal of the worth of an intelligence activity, source, information, or product in terms of its contribution to a specific goal, or the credibility, reliability, pertinence, accuracy, or usefulness of information in terms of an intelligence need. (National HUMINT Glossary)

Assessment--within the human source environment…

"A process of getting to know and understand people and describing them."
-- Robert R. Holt, *Assessing Personality* (1971)

Effective assessment of human beings is an art

From an Agent Handler perspective…
"…[F]inding a likely candidate, getting to know him personally, ascertaining his interests, uncovering his vices and possible Achilles' heel."
-- Victor Cherkashin, KGB Counterintelligence Officer and author of *Spy Handler* (2005)

Asset. Any human or technical resource available to an intelligence or security service for operational purposes. (FBI FCI Terms) Also see *agent; foreign intelligence agent; Intelligence asset; source.*

-- Also, [in human source operations] a recruited source. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, any resource—human, technical, or otherwise—available to an intelligence or security service for operational use. In U.S. usage, usually a person. (Spy Book)

-- Also, [in defense critical infrastructure usage] a distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned or operated by domestic, foreign, public, or private sector organizations. (DoDD 3020.40, Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *defense critical infrastructure program*.

-- Also, [in critical infrastructure protection] person, structure, facility, information, material, or process that has value. (DHS Lexicon, 2010) Also see *crucial infrastructure*.

Asset Owner. [In DCIP usage,] the DoD Components with responsibility for a DoD asset, or organizations that own or operate a non-DoD asset. (DoDI 3020.45, DCIP Management, 21 Apr 2008) Also see *task asset, task critical asset*.

Asset Validation. In intelligence use, the process used to determine the asset authenticity, reliability, utility, suitability, and degree of control the case officer or others have. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *Source Validation*.

The cardinal rule in tradecraft is: Never, ever fall in love with your agent.
-- Robert D. Chapman, Retired CIA Operations Officer
"Patriot or Traitor?" Book review of *A Secret Life* in *International Journal of Intelligence and Counterintelligence*, Vol 18 No 2 (Summer 2005), p. 367

Some human intelligence agencies do a poor job of validating human sources.

The story of 'Curveball'—the human source who lied to the Intelligence Community about Iraq's biological weapons programs—is an all-too familiar one. Every agency that collects human intelligence has been burned in the past by false reporting; indeed, the Intelligence Community has been completely fooled several times by large-scale double-agent operations run by, among others, the Cubans, East Germans, and Soviets. It is therefore critical that our human intelligence agencies have excellent practices of validating and vetting their sources.
-- WMD Report, Chapter 7 - Collection, p. 367*
* Available online at: <https://www.fas.org/irp/offdocs/wmd_chapter7.pdf>

-- Also, the process used to determine the asset authenticity, reliability, utility, suitability, and degree of control the case officer or others have. This process continues through the life of the relationship. It may be more or less formal depending on the sensitivity of the relationship and the nature of the source. For clandestine sources, particularly foreign nationals, the process is usually formal and revalidation is required on a periodic basis. Whether or not it is conducted formally, it must be a well-planned and thought out activity. (DoD CI Collection IWG Handbook, TTP for CI Collection, Collection Management, and Collection Operations, 8 Aug 2006)

In the spy trade asset validation is simply
a system of measures to establish the reliability and veracity of sources.
-- Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present*, 2013, p. 255

_____

For any organization that collects human intelligence, having an independent system for asset validation is critical to producing reliable, well-vetted intelligence.
-- WMD Report (31 Mar 2005), p. 455

_____

Every intelligence service has the problem of distinguishing…
between a bona fide volunteer and a penetration agent who has been sent by the other side. This is no easy matter.
-- Allen W. Dulles, *The Craft of Intelligence* (2006), p. 121

_____

See DoDI S-3325.07, *Guidance for the Conduct of DoD Human Source Validation* (U) and National HUMINT Manager Directive 001.008, *HUMINT Source Validation*.

Assign. 1) To place units or personnel in an organization when such placement is relatively permanent, and/or where such organization controls and administers the units or personnel for the primary function, or greater portion of the functions, of the unit or personnel; or 2) To detail individuals to specific duties or functions where such duties or functions are primary and/or relatively permanent. (JP 1-02 and JP 5-0, Joint Operations Planning, 11 Aug 2011) Also see *attach.*

Assumption. A supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action. (JP 1-02 and JP 5-0, Joint Operations Planning, 11 Aug 2011)

Asylum. Protection granted by the U.S. Government within the United States to a foreign national who, due to persecution or a well-founded fear of persecution on account of his or her race, religion, nationality, membership in a particular social group, or political opinion, is unable or unwilling to avail himself or herself of the protection of his or her country of nationality (or, if stateless, of last habitual residence). (DoDI 2000.11, Procedures for Handling Requests for Asylum and Temporary Refuge, 13 May 2010)

Asymmetric Threat. An adversary strength that can be used against a friendly vulnerability. An adversary may pursue an asymmetric advantage on the tactical or strategic level by identifying key vulnerabilities and devising asymmetric concepts and capabilities to strike or exploit them. To complicate matters, our adversaries may pursue a combination of asymmetries. (USD/I Taking Stock of Defense Intelligence Report, 22 Jan 2004)

-- Also, a broad and unpredictable spectrum of military, paramilitary, and information operations, conducted by nations, organizations, or individuals or by indigenous or surrogate forces under their control, specifically targeting weaknesses and vulnerabilities within an enemy government or armed force. (Source: Michael L. Kolodzie, US Army, circa 2001)

-- Also, a broad and unpredictable spectrum of risks, actions, and operations conducted by state and non-state actors that can potentially undermine national and global security. (Cyber Threats to National Security, Symposium Five, 2011)

Asymmetric Warfare. Combat between two or more state or non-state actors whose relative military power, strategies, tactics, resources, and goals differ significantly. (Cyber Threats to National Security, Symposium Five, 2011)

Atmospherics. Information regarding the surrounding or pervading mood, environment, or influence on a given population. (DoDD 3600.01, Information Operations, 14 Aug 2006 with Chg 1, 23 May 2011)

Attach. 1) The placement of units or personnel in an organization where such placement is relatively temporary; or 2) The detailing of individuals to specific duties or functions where such functions are secondary or relatively temporary. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *assign.*

Attaché. A diplomatic official or military officer attached to an embassy or legation, especially in a technical capacity. Also see *Senior Defense Official / Defense Attaché (SDO/DATT).*

Authenticate. A challenge given by voice or electrical means to attest to the authenticity of a message or transmission. (JP 1-02)

Authentication. 1) A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator; 2) A means of identifying individuals and verifying their eligibility to receive specific categories of information; 3) Evidence by proper signature or seal that a document is genuine and official; and 4) In personnel recovery missions, the process whereby the identity of an isolated person is confirmed. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

Authenticator. A symbol or group of symbols, or a series of bits, selected or derived in a prearranged manner and usually inserted at a predetermined point within a message or transmission for the purpose of attesting to the validity of the message or transmission. (JP 1-02)

B ==========

Background Investigation (BI). An official inquiry into the activities of a person designed to develop information from a review of records, interviews of the subject, and interviews of people having knowledge of the subject. (IC Standard 700-1, 4 Apr 2008) See *personnel security investigation*.

> The Office of Personnel Management, Federal Investigative Services (OPM-FIS) provides investigative products and services for over 100 Federal agencies to use as the basis for suitability and security clearance determinations as required by Executive Orders, et al. OPM provides over 90% of the Government's background investigations, conducting over two million investigations a year.
>
> See OPM web site at: <http://www.opm.gov/investigations/background-investigations/>

Backdoor. Typically unauthorized hidden software or hardware mechanism used to circumvent security controls. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Backstop. Arrangements made to support a cover so that inquiries about the cover will elicit responses that make the cover appear to be true. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

-- Also, the arrangement made by documentary or oral means to support a cover story so that inquiries about it will elicit responses indicating the story is true. (ICS Glossary & AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, to make arrangements made through documentary, oral, technical, fiscal, legal, or other means to support covers (both individual and organizational). A backstopped cover provides sufficient documentation to protect an identity in the immediate area or circumstance and in primary U.S. Government and commercial information systems. A backstopped cover is constructed to withstand routine scrutiny. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, an arrangement made to support a cover story. (FBI FCI Terms)

Backstopping. Arrangements made to support covers and activities. (HDI Lexicon, April 2008)

-- Also, arrangements made through documentary, oral, technical, fiscal, physical, or other means to support covers (both individual and organizational). A backstopped cover provides sufficient documentation to project an identity in the immediate area or circumstance and in primary USG and commercial information systems. Backstopping cover may be constructed to withstand scrutiny ranging from casual or unwitting general population to a targeted hostile adversary. (DTM 08-050, Defense Cover Program Guidance (U), 31 Mar 2009 w/ chg 2 dated 14 Apr 2011)

-- Also, verification and support of cover arrangements for an agent [case officer or intelligence operative] in anticipation of inquiries or other actions that might test credibility of his or her cover. (Spy Book)

-- Also, a CIA term for providing appropriate verification and support of cover arrangements for an agent or asset in anticipation of inquiries or other actions which might test the credibility of his or its cover. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Badge. A distinctive official device usually made of cast metal, which is provided by the DoD Component and worn or carried by the bearer as a sign of authority. (DoDI 5240.25, Counterintelligence Badges and Credentials, 30 Sep 2011 with change 1 dated 15 Oct 2013) Also see *credentials*.

Basic Intelligence. Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. (JP 1-02)

Beacon. A device typically fastened to an object or individual that transmits a radio signal in order to track its location. The technological discipline is called beaconry. (Spycraft)

Behavioral Science Consultant. A professional with extensive training in behavioral science, mental health, psychiatry, or psychology. (Previously in JP 2-01.2, CI & HUMINT Support to Joint Operations, 13 Jun 2006)

> Behavioral Science Consultants are psychologists and forensic psychiatrists, not assigned to clinical practice functions, but to provide consultative services to support authorized law enforcement, counterintelligence or intelligence activities, including detention and related counterintelligence, intelligence, interrogation, and detainee debriefing operations.

Bilateral Collection. A collection activity run jointly with a foreign intelligence service. (Previously in DoDI S-5240.17, CI Collection, 12 Jan 2009) Also see *multilateral.*

> Bilateral: Activities conducted with only a single foreign nation.

Bilateral/BILAT Operation. An operation run jointly with a foreign intelligence service or between two US intelligence/CI services. (CI Community Lexicon) Also see *unilateral operation.*

Bigot Case. An investigation that due to the sensitivity of the subject or the nature of the investigation, requires that it be handled on a strict need to know basis. Access to these investigations is controlled by maintaining a list of personnel who have been approved for access, called a "bigot list." (AR 381-20, Army CI Program, 25 May 2010) Also see *bigot list*, *compartmentation.*

Bigot List. Tradecraft jargon for any list of names of cleared personnel having restricted access (need-to-know) to a sensitive operation, investigation or to special access/compartmented intelligence. Also see *bigot case, compartmentation*.

-- Also, a restrictive list of persons who have access to a particular, and highly sensitive class of information. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

> *In some instances, a case, due to its sensitivity or the sensitivity of the information involved, will require that it be handled on a strict need-to-know basis. These cases are often referred to as BIGOT cases because access to them is controlled by a BIGOT list.*
>
> -- Army FM 2-22.2, *Counterintelligence*, October 2009
>
> ---
>
> According to a variety of sources, the term dates back to World War II when Allied orders for officers were stamped "TO GIB" for those being sent to Gibraltar for preparations for the invasion of North Africa; later their orders were stamped "BIG OT" (TO GIB backwards) when they were sent back to begin planning Operation OVERLORD, the invasion of Normandy. In WWII, it was convenient, in trying to find out if someone had access to highly restricted NEPTUNE and OVERLORD planning information, to ask "are you bigoted?" An indignant answer of "no" ended that part of classified discussion.

Biographical Intelligence. That component of intelligence that deals with individual foreign personalities of actual or potential importance. (JP 1-02)

Biometrics. The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *biometrics enabled-intelligence.*

-- Also, a general term used alternatively to describe a characteristic or a process. *As a characteristic:* A measurable biological (anatomical & physiological) and behavioral characteristic that can be used for automated recognition. *As a process:* Automated methods of recognizing an individual based on measurable biological (anatomical & physiological) and behavioral characteristics. (DoDD 8521.01E, DoD Biometrics, 21 Feb 2008)

-- Also, the measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition; examples include fingerprint, face, and iris recognition. (NSPD 59 / HSPD 24, Biometrics for Identification and Screening to Enhance National Security, 5 Jun 2008)

-- Also, measurable biological (anatomical and physiological) and behavioral characteristic that may be used for automated recognition of the identity of a person or to verify his claimed identity. Includes fingerprints, iris/retina, voice, facial, DNA, fingernail, and thermal signature. (AR 381-20, Army CI Program, 25 May 2010)

"Biometrics has become a non-lethal weapons systems in complex, irregular warfare environments. When you enroll a person in biometric systems now in use on the battlefield, you take away from our enemies the ability to remain anonymous. It's a high impact tool in the ongoing War on Terror and gives tactical commanders a decisive edge in today and tomorrow's battlespace."

-- LTG John F. Kimmons, U.S. Army G-2

The Secretary of the Army is the DoD Executive Agent for DoD Biometrics.

The term "biometrics" also describes both a *process* and a *characteristic*. As a process, biometrics consists of the automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Two basic types of biometrics: 1) *physical characteristics*, e.g., face, hand & finger geometry, iris, and vein structure; and 2) *behavioral characteristics*, e.g., voice, handwriting, typing, rhythm, and gait. For general information see <http://www.howstuffworks.com/biometrics.htm>

See Army TC 2-22.82, *Biometrics-Enabled Intelligence*, March 2011

Also see John Woodward, "Biometrics in the War on Terror," RAND Corporation (Dec 2005); available at -- <http://www.rand.org/commentary/2005/12/18/UPI.html>

Biometrics-Enabled Intelligence (BEI). Intelligence information associated with and or derived from biometrics data that matches a specific person or unknown identity to a place, activity, device, component, or weapon that supports terrorist / insurgent network and related pattern analysis, facilitates high value individual targeting, reveals movement patterns, and confirms claimed identity. (DoDD 8521.01E, DoD Biometrics, 21 Feb 2008) Also see *biometric-enabled watch list (BEWL).*

-- Also, the intelligence derived from the processing of biologic identity data and other all-source for information concerning persons of interest. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, the information associated with and/or derived from biometric signatures and the associated contextual information that positively identifies a specific person and/or matches an unknown identity to a place, activity, device, component, or weapon. (ADRP 2-0, Intelligence, Aug 2012)

BEI is a specialized analytical discipline that relies on all-source collections and a distinct processing, exploitation, reporting, and dissemination enterprise to integrate the information from U.S. and non-U.S. biometric collection and processing capabilities into all-source intelligence analysis for the purpose of monitoring or neutralizing the influence and operational capacity of individuals, cells, and networks of interest.

-- TC 2-22.82, *Biometrics-Enabled Intelligence*, March 2011, p. 1-9

Biometrics-Enabled Watch List (BEWL). Any list of interest with individuals identified by biometric sample instead of by name, and the desired/recommended disposition instructions for each individual. (TC2-22.82, Biometrics-Enabled Intelligence, March 2011)

> Within DoD, BEWL is a decision aid to help commanders determine what action to take when encountering a person of interest.

Black. 1) tradecraft jargon for inconspicuousness in the sense of being free of hostile surveillance [*going black*: become free of surveillance before conducting an operational act]; and 2) CIA tradecraft jargon for clandestine or covert. (Leo D. Carl, *The CIA's Insider Dictionary*, 1996)

-- Also, being free of hostile surveillance while on a clandestine mission; also refers to being in place undetected or unknown, such as flying in black. (A Spy's Journey)

-- Also, BLACK: designation applied to encrypted information and the information systems, the associated areas, circuits, components, and equipment processing that information. Also see *RED*. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Black Bag Job. [Tradecraft jargon] a surreptitious entry operation usually conducted by the FBI against a domestically located foreign intelligence target. (Spy Dust) Also see *surreptitious entry.*

> **Aka Covert Entry…**
>
> *Tactical Operations, a supersecret unit of FBI break-in artists who conduct court-authorized burglaries [covert entries] in homes, offices, and embassies to plant hidden microphones and video cameras and snoop into computers. …In any given year, TacOps conducts as many as four hundred of what the FBI calls covert entries. Eighty percent are conducted in national security cases relating to terrorism or counterintelligence.*
>
> *Over the years, the FBI has conducted successful covert entries at the Russian and Chinese embassies or their official diplomatic establishments, as well as at the homes of their diplomats and intelligence officers.*
>
> *Going up against foreign intelligence agencies is the biggest challenge because they set traps to detect entries.*
>
> -- Ronald Kessler, *The Secrets of the FBI* (2011), pp 2, 7, 11, & 173
>
> ---
>
> "Black Bag" -- *The term applied to clandestine entries of premises containing information that is likely to be of exceptional importance. The material may range from cryptographic data to the membership rolls of target organizations.*
>
> -- Nigel West, *Historical Dictionary of International Intelligence*.

Black List. [A list that] contains the identities and locations of individuals whose capture and detention are of prime importance, or individuals who have been determined to be intelligence fabricators. (CI Community Lexicon) Also see *Gray List; White List*.

-- Also, an official counterintelligence listing of actual or potential hostile collaborators, sympathizers, intelligence suspects, or other persons viewed as threatening to the security of friendly military forces. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

> Previous DoD definition in JP 1-02: an official counterintelligence listing of actual or potential enemy collaborators, sympathizers, intelligence suspects, and other persons whose presence menaces the security of friendly forces. *Note: this definition rescinded by JP 2-01.02, 11 Mar 2011.*
>
> ---

Examples of individuals who may be included on a Black List:
1) Known or suspected enemy or hostile espionage, sabotage, terrorist, political, and subversive individuals.
2) Known or suspected leaders and members of hostile paramilitary, partisan, or guerrilla groups.
3) Political leaders known or suspected to be hostile to the military and political objectives of the United States and/or an allied nation.
4) Known or suspected officials of enemy governments whose presence in the theater of operations poses a security threat to the U.S. Forces.
5) Known or suspected enemy collaborators and sympathizers whose presence in the theater of operations poses a security threat to the U.S. Forces.
6) Known enemy military or civilian personnel who have engaged in intelligence, CI, security, police, or political indoctrination activities among troops or civilians.
7) Other enemy personalities such as local political personalities, police chiefs, and heads of significant municipal and/or national departments or agencies.

-- USMC, MCWP 2-6 (previously 2-14), *Counterintelligence*, 5 Sep 2000

Black Swan Event. An event that is rare, predictable only in retrospect, with extreme impacts.

Blow [Tradecraft jargon] to expose—often unintentionally—personnel, installations or other elements of a clandestine activity or organization. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976) Also see *blown*.

Blown [Tradecraft jargon] to have one's cover exposed; to have an operation become public. (A Spy's Journey)

Bona Fides. The lack of fraud or deceit: a determination that a person is who he/she says he/she is. (National HUMINT Glossary)

Tradecraft jargon for credentials which establishes the credibility of a human source.

———————————

The determination of a defector or agent's bona fides, the verification of their truthfulness, is critical to the assessment of the information they provide.

-- Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present*, 2013, p. 77

-- Also, good faith. In personnel recovery, the use of verbal or visual communication by individuals who are unknown to one another, to establish their authenticity, sincerity, honesty, and truthfulness. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

-- Also. the lack of fraud or deceit: a determination that a person is who he/she says he/she is. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, physical and/or oral exchanges employed by an unknown individual to prove identity and foster trust. (HDI Lexicon, April 2008)

-- Also, documents, information, action, codes, etc., offered by an unknown or otherwise suspected individual to establish his or her good faith, identification, dependability, truthfulness, or motivation. (ICS Glossary & AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Border Crosser. An individual, living close to a frontier, who normally has to cross the frontier frequently for legitimate purposes. (JP 1-02)

Botnet. A collection of zombie PCs [personal computers]. Botnet is short for robot network. A botnet can consist of tens or even hundreds of thousands of zombie computers. A single PC in a botnet can automatically send thousands of spam messages per day. The most common spam messages come from zombie computers. (McAfee Labs - Threat Glossary) Also see *zombie*.

-- Also, Botnets, or Bot Networks, are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet. (CRS Report PL32114, 29 Jan 2008)

-- Also, A network of "zombie" computers controlled by a single actor. Botnets are a common tool for malicious activity on the Internet, such as denial-of-service attacks and spam, since they provide free 9stolen) computation and network resources while hiding the identity of the controller. (Cybersecurity and Cyberwar)

> Botnets have been described as the
> ***"Swiss Army knives of the underground economy"***
> because they are so versatile.

Brevity Code. [In intelligence usage] Communications security (COMSEC) term for a code used only for shortening the length of a message, but not to conceal its content. (Cited as FBI Glossary in *CIA's Insider's Dictionary* by Leo D. Carl) [Note: although the brevity code does not conceal content (the actual words used), it can be used to conceal true meaning]

-- Also, [non intelligence usage] a code which provides no security but which has as its sole purpose the shortening of messages rather than the concealment of their content. (JP 1-02; JP 3-04; and FM 1-02.1, Multi-Service Brevity Codes, Jun 2005)

Brief Encounter. A short and discreet operational contact. (HDI Lexicon, April 2008) Also see *brush contact; brush pass*.

-- Also, any brief physical contact between a case officer and an agent under threat of surveillance. (CI Centre Glossary)

Brush Contact. A discreet momentary contact, usually prearranged between intelligence personnel, during which material or oral information is passed. (ICS Glossary & AFOSI Manual 71-142, OFCO, 9 Jun 2000) Also see *brush pass; brief encounter*.

> *Such a contact is extremely brief as well as surreptitious,*
> *and usually it is quite secure if well executed.*
> -- Victor Marchetti & John D. Marks,
> *The CIA and the Cult of Intelligence,* 2nd edition (1980), p 230

-- Also, a discreet, usually prearranged momentary contact between intelligence personnel when information or documents are passed. Also known as a brief encounter. (FBI FCI Terms)

-- Also, a technique used by case officers to receive [or] exchange information from an agent clandestinely without betraying any signs of recognition between participants. The objective is to complete the transaction without detection by any hostile surveillance. (*Historical Dictionary of Cold War Counterintelligence,* 2007)

> ***Brush Contact*** – credited largely to Haviland Smith, who served as the CIA station chief in Prague from 1958 to 1960. See Benjamin Weiser, *A Secret Life: The Polish Officer, His Covert Mission, and the Price He Paid to Save His Country* (2004)
>
> *"He found that if he walked along a street and turned right, he created a gap in which the agents [surveillance] trailing him would lose sight of him for a few seconds…. Do not elude surveillance, accept it as a way of life."*

Brush Pass. A brief operational encounter (seconds or less) in which the case officer passes something (verbally or physically) to or receives something from the agent, or a two-way exchange takes place. (National HUMINT Glossary) Also see *brief encounter; brush contact*.

-- Also, a discreet, monetary contact during which something is exchanged. (HDI Lexicon, April 2008)

-- Also, a brief encounter where something is passed between a case officer and an agent. (CI Centre Glossary)

-- Also, the clandestine, hand-to-hand delivery of items or payments – made as one person walks past another in a public place [The Russian Foreign Intelligence Service (SVR) refers to a brush pass as a "flash meeting"]. (FBI – Court Affidavit re: Russian Illegals, 25 June 2010)

Bug. [Tradecraft jargon] 1) Concealed listening device or other equipment used in audio surveillance; 2) To install such a device; the term "bugged" refers to a room or object that contains a concealed listening device. (Spy Book)

-- Also, a concealed listening device or microphone, or other audiosurveillance device; also to install the means for audiosurveillance of a subject or target. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Bugging… Electronic Surveillance

Bugging is a term in common use that refers to the various forms of clandestine electronic surveillance, or eavesdropping. See *Spycraft*, pp. 405-416, for details.

Bug -- *a covert or clandestine listening or viewing device that is noted for its small, inconspicuous (bug-like) size. Bugs used to primarily mean primarily listening devices, small microphones that could be hidden in plants or phone handsets, but the term now is also used to describe tiny pinhole cameras that are as small as audio bugs used to be twenty years ago. A bug may be wired or wireless and may or may not be sending information a recording device.*

-- Julie K. Petersen, *Understanding Surveillance Technologies: Spy Devices, Their Origins & Applications* (2001)

[The FBI's] Engineering Research Facility at Quantico… makes custom-designed bugging devices, tracking devices, sensors, and surveillance cameras to watch and record bad guys. It also develops ways to penetrate computers and defeat locks, surveillance Cameras, and alarm and access control systems.

…state-of-the-art FBI bug… a circuit board that is the size of a postage stamp and the thickness of two stacked quarters "It's a transmitter and stereo recorder… it records for about twenty-one hours, and will transmit to a local receiver in encrypted form…. This is actually big in comparison to some of our bugs."

-- Ronald Kessler, *The Secrets of the FBI* (2011), pp 8-9 and 227-228

Bugged. Room or object that contains a concealed listening device. (JP 1-02)

Burned. [Tradecraft jargon] When a case officer or agent is compromised, or a surveillant has been made by a target, usually because they make eye contact. (CI Centre Glossary)

Burn Notice. *Within DoD: None – term removed from JP 1-02 per JP 2-0 Joint Intelligence (22 Oct 2013).*

Previously defined in JP 1-02 as: an official statement by one intelligence agency to other agencies, domestic or foreign, that an individual or group is unreliable for any of a variety of reasons.

C ==========

Campaign. A series of related military operations aimed at achieving strategic or operational objectives within a given time and space. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *DoD Strategic CI Campaign*.

Campaign Plan. A joint operation plan for a series of related military operations aimed at achieving strategic or operational objectives within a given time and space. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *Campaign; Campaign Planning; DoD Strategic CI Campaign*.

Campaign Planning. The process whereby combatant commanders and subordinate joint force commanders translate national or theater strategy into operational concepts through the development of an operation plan for a campaign. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *campaign; campaign plan*.

Capability. The ability to execute a specified course of action. (A capability may or may not be accompanied by an intention.) (JP 1-02)

Capability Gap. The inability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. The gap may be the result of no existing capability or lack of proficiency or sufficiency in existing capability.

Captured or Detained Personnel. Any person captured, detained, held, or otherwise under the control of DoD personnel (military or civilian). This does not include DoD personnel or DoD contractor personnel being held for law enforcement purposes. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

Car Pick-Up. A personal meeting wherein the handler picks up the source. (HDI Lexicon, April 2008)

Car Toss. A form of dead drop using a concealment device thrown to a preselected site from a vehicle traveling along a designated route. (HDI Lexicon, April 2008) Also see *brief encounter; brush contact, brush pass.*

-- Also, the method of conveying information clandestinely by throwing a package into, or out of, a vehicle is known as the "car toss." (*Historical Dictionary of Cold War Counterintelligence*, 2007)

> *[P]ull just far enough ahead of [surveillance] so that when he turned a curve…. or disappeared over a small hill, he was able to create ten- to twenty-second gaps during which he could throw a soda can or bottle out the window and in to a ditch by the road. In such "car tosses", beepers might be placed inside the object along with a message, so that the agent with a small radio could find it easily.*
>
> -- Benjamin Weiser, *A Secret Life* (2004) pb, p.79

Carbons. Paper that produces secret writing [SW] through the use of chemicals. (FBI FCI Terms and Spy Book) Also see *secret writing*.

-- Also, paper invisibly impregnated with chemicals which, when used in accordance with directions, will produce secret writing. Illegals and agents often posses carbons which appear as ordinary sheets in writing pads that are manufactured in the target country. (AFOSI Manual 71-142, OFCO, 9 June 2000)

Carve-Out. A provision approved by the Secretary or Deputy Secretary of Defense that relieves DSS [Defense Security Service} of its National Industrial Security Program obligation to perform industrial security oversight functions for a DoD SAP [Special Access Program]. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

-- Also, a classified contract for which the Defense Security Service (DSS) has been relieved of inspection responsibility in whole or in part. (DSS Glossary)

CARVER. A special operations forces acronym used throughout the targeting and mission planning cycle to assess mission validity and requirements. The acronym stands for criticality, accessibility, recuperability, vulnerability, effect, and recognizability. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

Case. The framework which not only acts as the repository for all logically/physically related facts, issues, allegations and products (outputs) associated with the investigative process, but also serves to document, in a case file, the approvals, authorities, waivers, plans, notes and other artifacts relevant to that particular instance of the process. (ONCIX Insider Threat Detection – Glossary)

-- Also, an intelligence operation in its entirety; the term also refers to a record of the development of an intelligence operation, how it will operate, and the objectives of the operation. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

> Can also be used as a verb, to case, meaning to surreptitiously observe a physical location to determine its suitability for possible future operational use.
>
> Previously defined in DoD (JP 1-02) as: 1) An intelligence operation in its entirety; or 2) Record of the development of an intelligence operation, including personnel, modus operandi, and objectives. Approved for removal per JP 2-0 *Joint Intelligence* (22 Oct 2013).

Case Officer (C/O). A professional employee of an intelligence or counterintelligence organization who is responsible for providing directions for an agent operation and/or handling intelligence assets. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; CI Community Lexicon; and ICS Glossary) Also see *Agent Handler*.

-- Also, [an intelligence employee] who is responsible for managing and directing agents (assets) in the field. Case officers are sometimes referred to as "operations officers." (*Encyclopedia of the CIA*, 2003)

> *"…the case officer's job is to handle operational cases and assets; this is to say the case officer recruits and directs foreign indigenous spies who are known as "agents."*
>
> -- Fred Rustmann, Jr., "Debunking the CIA Case Officer Myth," *AFIO Newsletter*; 25: 1&2 (2002)

Casing. Reconnaissance of an operating area, whether for surveillance or for personal or impersonal communications. (CI Community Lexicon)

-- Also, a study of a site to determine operational suitability. (HDI Lexicon, April 2008)

-- Also, covert or clandestine inspection or surveillance of an area, place, or building to determine its suitability for operational use or its vulnerability to an intelligence operation. (AFOSI Instruction 71-101, 6 Jun 2000 and AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Catastrophic Event. Any natural or man-made incident, including terrorism, which results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013) Also see *complex catastrophe*.

Caveat. A designator used with or without a security classification to further limit the dissemination of restricted information, e.g., FOUO and NOFORN. (IC Standard 700-1, 4 Apr 2008)

-- Also, a designator used with a classification to further limit the dissemination of restricted information. (JP 1-02 and JP 3-07.4, Joint Counterdrug Operations, 13 Jun 2007)

Cell. [In intelligence usage,] a small group of individuals who work together for clandestine or subversive purposes.

CELLEX. See *cellular telephone exploitation*.

Cellular Telephone Exploitation (CELLEX). Exploitation of cellular phones at the logical or physical level to extract cogent contextual information, includes holistic examinations of mobile devices and associated digital media (e.g., SIM cards, media cards).

Center [British spelling: *Centre*]. The headquarters site in the home country where control of intelligence and espionage operations in foreign countries is maintained. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, intelligence service headquarters. (FBI FCI Terms)

Center of Gravity (COG). The source of power that provides moral or physical strength, freedom of action, or will to act. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Central Intelligence Agency (CIA). An independent US Government agency responsible for providing national security intelligence to senior US policymakers. Primary mission: collect, analyze, evaluate, and disseminate foreign intelligence to assist the President and senior US government policymakers in making decisions relating to national security. Major components: National Clandestine Service (NCS), Directorate of Intelligence, Directorate of Science & Technology and Directorate of Support. (cia.gov) Also see *National Clandestine Service*.

We do espionage. That is the nature of what we do. We steal secrets.

-- DCI George Tenet, 23 June 1998
Interview in *Studies in Intelligence*, 42:1 (1998)

Director CIA is designated the Functional Manager for human intelligence IAW EO 12333; and is also the National HUMINT Manager IAW ICD 304, Human Intelligence.

Director CIA coordinates the clandestine collection of foreign intelligence through human sources or through human-enabled means and counterintelligence activities outside the United States (EO 12333).

The CIA may engage in covert action at the President's direction and in accordance with applicable law; see *covert action*.

_____

The Director CIA serves as the head of the Central Intelligence Agency and reports to the Director of National Intelligence. The CIA director's responsibilities include:

-- Collecting intelligence through human sources and by other appropriate means, except that he shall have no police, subpoena, or law enforcement powers or internal security functions;
-- Correlating and evaluating intelligence related to the national security and providing appropriate dissemination of such intelligence;
-- Providing overall direction for and coordination of the collection of national intelligence outside the United States through human sources by elements of the Intelligence Community authorized to undertake such collection and, in coordination with other departments, agencies, or elements of the United States Government which are authorized to undertake such collection, ensuring that the most effective use is made of resources and that appropriate account is taken of the risks to the United States and those involved in such collection; and
-- Performing such other functions and duties related to intelligence affecting the national security as the President or the Director of National Intelligence may direct.

The function of the Central Intelligence Agency is to assist the Director of the Central Intelligence Agency in carrying out the responsibilities outlined above.

Source: https://www.cia.gov/about-cia/index.html (accessed 20 Aug 2012)

CFIUS. See *Committee of Foreign Investment in the United States*.

Chain of Custody. A chronological written record reflecting the release and receipt of evidence from initial acquisition until final disposition. (AR 195-5, Evidence Procedures, 25 Jun 2007) Also see *evidence; chain of evidence*.

-- Also, a process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a process used to maintain and document the chronological history of the evidence. (Documents should include name or initials of the individual collecting the evidence, each person or entity subsequently having custody of it, dates the items were collected or transferred, agency and case number, victim's or suspect's name, and a brief description of the item.) (Crime Scene Investigation: A Guide for Law Enforcement, Sep 2013)

> Chain of Custody is a process used to document the chronological history of evidence to maintain the security, integrity and accountability of its handling.

Chain of Evidence. A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) Also see *evidence; chain of custody*

Chairman's Guidance (CG). Provides a common set of assumptions, priorities, intent, and critical planning factors required to develop future strategies and plans. It is an integral part of the strategy development process. CG may be established pursuant to conducting a Joint Strategy Review, to preparing a Joint Vision, or to Drafting a new National Military Strategy; or it may be provided separately if deemed appropriate. (CJCSI 3100.01A, Joint Strategic Planning System, 1 Sep 1999)

Chancery. The building upon a diplomatic or consular compound which houses the offices of the chief of mission or principal officer. (JP 1-02)

Characterization. [In critical infrastructure protection usage] the analytic decomposition of functions, systems, assets, and dependencies related to supporting DoD operational capabilities and assets. DoDD 3020.40, (DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010, w/ chg 2 dated 21 Sep 2012)

Chief of Mission (CoM). The principal officer in charge of U.S. Diplomatic Missions and U.S. offices abroad, which the Secretary of State has designated as diplomatic in nature. The CoM reports to the President through the Secretary of State. Also see *Ambassador*.

-- Also, the principal officer (the ambassador) in charge of a diplomatic facility of the United States, including any individual assigned to be temporarily in charge of such a facility. The CoM is the personal representative of the President to the country of accreditation and is responsible for the direction, coordination, and supervision of all US Government executive branch employees in that country (except those under the command of a US area military commander). The security of the diplomatic post is the CoM's direct responsibility. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011)

> The U.S. Ambassador to a foreign country, for example, is the Chief of the U.S. Mission (CoM) in that country. Other CoMs include the Chiefs of permanent U.S. Missions to international organizations (e.g., the U.S. Mission to International Organizations in Vienna), the Principal Officers of Consulates General, and the U.S. Interest Section in the Swiss Embassy in Havana.

The CoM has full responsibility and authority for the direction, coordination, and supervision of all USG executive branch employees in country and at international organizations, regardless of their employment categories or location, except those under command of a U.S. area military commander or on the staff of an international organization.

Chief of Station (CoS). The senior United States intelligence officer in a foreign country, and is the direct representative of the Director National Intelligence, to whom the officer reports through the Director Central Intelligence Agency. Usually the senior representative of the Central Intelligence Agency assigned to a US Mission. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Choke Point. A narrow passage--such as a bridge, tunnel, or Metro station--used as a surveillance or countersurveillance tool for channeling the opposing force or monitoring their passage. (CI Centre Glossary)

CHROME. Acronym for *Counterintelligence and Human Intelligence Requirements-Reporting and Operations Management Environment*. Interoperable, synchronized information technology architecture to replace and retire legacy software systems to accelerate workflow, increase efficiency, and broaden intelligence sharing within DoD and across the IC. (DoD FCIP Strategy FY 2013-2017)

Church Committee (aka the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities). A U.S. Senate committee chaired by Senator Frank Church (D-ID) in 1975. A precursor to the U.S. Senate Select Committee on Intelligence (SSCI), the committee investigated intelligence gathering by the CIA, FBI, and NSA after certain activities had been revealed by the Watergate affair. (Wikipedia at <http://en.wikipedia.org/wiki/Church_Committee>)

In 1975 and 1976, the Church Committee published fourteen reports on the formation of U.S. intelligence agencies, their operations, and the alleged abuses of law and of power that they had committed, together with recommendations for reform, some of which were put in place. Under recommendations and pressure by this committee, President Gerald Ford issued Executive Order 11905 (ultimately replaced in 1981 by President Reagan's Executive Order 12333).

Regarding counterintelligence see Book I *Foreign and Military Intelligence*, pp. 163-178

Copies of the Church Committee reports at the following two web sites:
-- <http://www.intelligence.senate.gov/churchcommittee.html>
-- <http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm>

CI. See *counterintelligence*.

CI-21. Counterintelligence for the 21st Century. (See White House Fact Sheet, "The PDD on CI-21: Counterintelligence for the 21st Century" – copy at <http://www.fas.org/irp/offdocs/pdd/pdd-75.htm>)

Designed to provide a national counterintelligence system which is predictive and proactive, one that includes integrated oversight of national CI activities across government and the private sector. Established: 1) the National CI Policy Board of Directors (Dir FBI, Dep SECDEF, DDCI, and DoJ Representative); 2) the National CI Executive (NCIX); and the Office of the National CI Executive.

_____

"The general premise behind CI-21 is to try and determine what are America's true equities, and then extend this interagency cooperation in a systematic way to try and better protect those assets and deter acts of espionage that target them. We can no longer afford to focus our counterintelligence efforts only after an incident has sparked a full criminal case, because at that point it's too late. The damage has already been done."

-- DCI George Tenet quoted in "Anti-Terror Alliance," *Government Executive Magazine*, 1 Feb 2001

_____

"CI-21 is a manifestation of a process… we all began to realize that the threats to U.S. security were changing in a way that our traditional organizations and structures couldn't match… Globalization and technology were lowering traditional boundaries between what constitutes an international or domestic threat, and terrorists, drug cartels, spies and hackers were all leaping those boundaries with impunity."

-- John MacGaffin, Former ADDO, CIA and Former FBI Consultant who spearhead CI-21

CI Campaign. See *DoD Counterintelligence Campaign*.

CI Mission Tasking Authority. See *Counterintelligence Mission Tasking Authority*.

Cipher. Any cryptographic system in which arbitrary symbols (or groups of symbols) represent units of plain text of regular length, usually single letters; units of plain text are rearranged; or both, in accordance with certain predetermined rules. (JP 1-02) Also see *code; cipher pad*.

Cipher Pad. A small thin pad of paper sheets having nonrepetitive key, usually machine printed. A sheet is used once for enciphering and another sheet used once for deciphering a communication. Occasionally called a one-time pad (OTP). (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

CISO Acronym for Counterintelligence Staff Officer. Within DoD, term rescinded.

Note: within DoD this term replaced by "*Command CI Coordinating Authority*" or CCICA.

CIR. Acronym for Counterintelligence Incident Report.

Civil Authorities. Those elected and appointed officers and employees who constitute the government of the United States, the governments of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, United States territories, and political subdivisions thereof.
(JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

Civil Aviation Intelligence. Activities undertaken to understand how trends in the global civil aviation industry impact U.S. interests; or detect, analyze, monitor, and warn of illicit activity or threats to the United States, its allies, or its interests involving civil aviation. (DoDI 3115.14, Civil Aviation Intelligence, 29 Jul 2011)

Civil Disturbance. *Within DoD: None -- term removed from JP 1-02.*

Previous defined in JP 3-28, Civil Support (14 Sep 2007) as: Group acts of violence and disorder prejudicial to public law and order.

Civilian Internee. A civilian who is interned during armed conflict, occupation, or other military operation for security reasons, for protection, or because he or she committed an offense against the detaining power. (JP 3-63, Detainee Operations, 30 May 2008)

Clandestine. Any activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy or concealment. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) See *clandestine collection; clandestine intelligence; clandestine intelligence activity; clandestine intelligence collection clandestine operation; covert.*

-- Also, any HUMINT [Human Intelligence] or other activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy or concealment. (ICD 304, HUMINT, 1 Mar 2007 and DoDD S-5200.37, Management & Execution of Defense HUMINT, 9 Feb 2009)

-- Also, any illicit/illegal activity that is designed not to be detected by anyone, including a local security service. Concealed, hidden, secret, or surreptitious operation conducted without the knowledge of anyone but the organization conducting the operation or investigation. (CI Community Lexicon)

-- Also, method of conducting operations with secrecy by design. Differs from covert in that covert conceals the identity of the sponsor, whereas clandestine conceals the identity of the operation. (National HUMINT Glossary)

-- Also, secret or hidden activity conducted with secrecy by design. (ICS Glossary, 1978)

Clandestine, from the Latin *clam*, "secretly, in private."

Words have meaning… clandestine and covert are not synonymous

_____

"I don't take lightly the distinction between clandestine and covert…
It makes all the difference in the world."

-- Senator Jay Rockefeller, Senate Select Committee on Intelligence

Clandestine Collection. The acquisition of protected intelligence information in a way designed to protect the source, and conceal the operation, identity of operators and sources, and actual methodologies employed. (Previously in DoDI S-5240.17, CI collection, 12 Jan 2009) Also see *clandestine intelligence; clandestine intelligence collection.*

Clandestine Intelligence. Intelligence information collected by clandestine sources. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Clandestine Intelligence Activity. An activity conducted by or on behalf of a foreign power for intelligence purposes or for the purpose of affecting political or governmental processes if the activity is conducted in a manner designed to conceal from the U.S. Government the nature or fact of such activity or the role of such foreign power; also, any activity conducted in support of such activity. (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010)

Clandestine Intelligence Collection. The acquisition of protected intelligence information in a way designed to conceal the nature of the operation and protect the source. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the acquisition of protected intelligence information in a way designed to protect the source. (National HUMINT Glossary)

Clandestine Operation. An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

-- Also, activities to accomplish intelligence, CI, or similar activities in such a way as to maintain secrecy or concealment especially for the purpose of deception or subversion. (CI Community Lexicon)

-- Also, a pre-planned secret intelligence information collection activity, technical operation, or covert political, economic, propaganda, or paramilitary action conducted so as to assure the secrecy of the operation; encompasses clandestine collection, counterintelligence, and covert action. (National HUMINT Glossary)

-- Also, any HUMINT or other activity or operation sponsored or conducted by governmental departments or agencies with the intent to assure secrecy or concealment. (DHE-M 3301.002, Vol II, Collection Operations, 23 Nov 2010)

Clandestine operations are sometimes incorrectly referred to as "covert operations." Although both are secret and sensitive activities, the terms are not interchangeable. See c*overt operation*.

Clandestine Nuclear Threat. A nuclear or radiological attack by anyone for any purpose, against the United States and/or U.S. military operations, and delivered by means other than (military) missiles or aircraft. A large subset of this threat is the smuggling of nuclear weapons, devices, or materials for use against the United States. (DSB Report, Jun 2004)

Today, it would be easy for adversaries to introduce and detonate a nuclear explosive clandestinely in the United States.

-- Defense Science Board Report (June 2004)*

*Copy of "Report of the Defense Science Board Task Force Report on Preventing and Defending Against Clandestine Nuclear Attack," June 2004 available at: <http://www.acq.osd.mil/dsb/reports/ADA429042.pdf>

Clandestine Service. See *National Clandestine Service (NCS); Defense Clandestine Service (DCS).*

Classification. The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Classification—Driving Security

The classification system is designed primarily to protect the confidentiality of certain military, foreign policy, and intelligence information. It deals only with a small slice of the government' information that requires protection although it drives the government's security apparatus and most of its costs.

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, pp.7

Classified Information. Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, information or material designated and clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statue or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security. (50 USC § 426[1])

Classified Information Procedures Act (CIPA). The tool with which the proper protection of classified information may be ensured in indicted cases. After a criminal indictment becomes public, the prosecutor remains responsible for taking reasonable precautions against the unauthorized disclosure of classified information during the case. This responsibility applies both when the government intends to use classified information in its case-in-chief as well as when the defendant seeks to use classified information in his/her defense. (18 USC, App III, Sec 1-16) Also see *graymail*.

Congress enacted CIPA (Public Law 96-456) in 1980. The procedural protections of CIPA protect unnecessary disclosure of classified information. The primary purpose was to limit the practice of "graymail" by criminal defendants in possession of sensitive government secrets.

"Gray mail" refers to the threat by a criminal defendant to disclose classified information during the course of a trial. The gray mailing defendant essentially presented the government with a "Hobson's choice": either allow disclosure of the classified information or dismiss the indictment.

CIPA is a procedural statute that balances the right of a criminal defendant with the right of the sovereign to know in advance of a potential threat from a criminal prosecution to its national security. CIPA's provisions are designed to prevent unnecessary or inadvertent disclosures of classified information and to advise the government of the national security "cost" of going forward.

See: <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm02054.htm>

Classified Military Information (CMI). Information requiring protection in the interest of national security and is limited to three classifications: TOP SECRET, SECRET and CONFIDENTIAL as described in Executive Order 13526, *Classified National Security Information* (previously EO 12958 13526) and which is under the control or jurisdiction of the DoD or its Departments or Agencies.

Basic USG policy provided in National Security Decision Memorandum (NSDM) 119 "Disclosure of Classified United States Military Information to Foreign Governments and International Organizations": CMI is a national security asset which must be conserved and protected and which must be shared with foreign governments and international organizations only where there is a clearly defined advantage to the U.S.

Copy of NSDM 119 at: <http://www.nixonlibrary.gov/virtuallibrary/documents/nsdm/nsdm_119.pdf>

Classified National Intelligence (CNI). National intelligence as defined in 50 USC 401a(5), classified pursuant to EO 13526. (ICD 703, Protection of Classified National Intelligence Including Sensitive Compartmented Information, 21 Jun 2013) Also see *Sensitive Compartmented Information*.

Protection of CNI, including SCI, is also achieved through adherence to counterintelligence (CI) and security practices.

-- ICD 703, *Protection of Classified National Intelligence, including Sensitive Compartmented Information*, 21 Jun 2013, p. 2

Clean. [Tradecraft jargon] To be free of hostile surveillance. (*A Spy's Journey*)

Clean Phone. Tradecraft jargon which typically refers to a disposable, pre-paid cellular telephone that cannot be traced back to the original retail purchaser or subsequent user(s).

Clearance. Formal security determination by an authorized adjudicative office that an individual is authorized access, on a need to know basis, to a specific level of collateral classified information (TOP SECRET, SECRET, CONFIDENTIAL). (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Cleared Contractor (CC). A person or facility operating under the National Industrial Security Program (NISP), that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level (and all lower levels). There are approximately 8500 cleared contractors with over 13,000 facilities. (DSS - Glossary to Insider Threat Awareness Course)

The Defense Security Service (DSS) refers to "cleared contractors" as they support DoD as well as other U.S. Government Departments and Agencies. DSS oversees the protection of U.S. and foreign classified information and technologies in the hands of industry under the National Industrial Security Program (NISP). "The NISP applies to all Executive Branch Departments and Agencies and to all cleared contractor facilities located within the United States" (para 1-102, NISPOM).

Cleared Defense Contractor (CDC). A company or academic institution (i.e., university or college) that has entered into a security agreement with the DoD, and was granted a facility (security) clearance enabling the entity to be eligible for access to classified information of a certain category, as well as all lower categories. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

-- Also, a subset of contractors cleared under the NISP who have contracts with the Department of Defense. Therefore, not all cleared contractors have contracts with DoD. (DSS - Glossary to Insider Threat Awareness Course)

Click-jacking. Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowingly perform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed “Like” and “Share” buttons on social networking sites. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks>)

Coalition. An arrangement between two or more nations for common action. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *alliance*; *multinational.*

Coast Guard Counterintelligence Service (CGCIS). Component of Coast Guard Intelligence that provides full-spectrum counterintelligence support to the U.S. Coast Guard. Office symbol: CG-2-CI.

> *CGCIS preserves the operational integrity of the Coast Guard by shielding its operations, personnel, systems, facilities and information from Foreign Intelligence and Security Services (FISS), and the intelligence efforts of terrorist organizations, drug trafficking elements and other organized crime groups, and adversaries, and insider threats. CGCIS supports the identification, understanding, neutralization, and exploitation of the operations of FISS and of non-state actors who employ intelligence tradecraft. CGCIS manages the Foreign Visitor Program, providing tailored foreign intelligence threat and awareness briefings specific to foreigners visiting Coast Guard commands. CGCIS also conducts foreign travel briefs and debriefs, providing tailored foreign intelligence threat and awareness briefings on FISS, terrorism, and criminal threats, and health concerns to educate Coast Guard personnel traveling to high-threat countries.*
>
> -- Coast Guard Publication 2-0, *Intelligence*, May 2010

Code. 1) Any system of communication in which arbitrary groups of symbols represent units of plain text of varying length. Codes may be used for brevity or for security; 2) a cryptosystem in which the cryptographic equivalents (usually called "code groups"), typically consisting of letters or digits (or both) in otherwise meaningless combinations, are substituted for plain text elements which are primarily words, phrases, or sentences. (Previously in JP 1-02) Also see *cipher*.

-- Also, system of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a system of communication in which arbitrary groups of symbols represent units of plain text. Codes may be used for brevity or for security. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

> *“There is no sharp theoretical line between codes and ciphers; [a] useful distinction is that code operates on linguistic entities, dividing its raw material into meaningful elements and cipher does not.”*
>
> -- David Kahn, *The Code Breakers* (1967)

Code Book. Document containing plain text and code equivalents in a systematic arrangement, or a technique of machine encryption using a word substitution technique. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Code Word. A single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans, activities or operations classified CONFIDENTIAL or higher. (DoDI 5205.11, Management, Administration, and Oversight of DoD Special Access Programs, 6 Feb 2013)

-- Also, a single classified word assigned to represent a specific SAP or portions thereof. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

-- Also, 1) A word that has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation; and 2) A cryptonym used to identify sensitive intelligence data. (JP 1-02 and JP 3-50, Personnel Recovery, 20 Dec 2011)

-- Also, a prearranged word used in communication or conversation to disguise the identity of someone or something or to convey a meaning other than its conventional meaning. (AFOSI Manual 71-142, 9 Jun 2000) Also see *nickname*.

Cold Pitch. Recruitment approach without prior development or, in some cases, contact. (National HUMINT Glossary)

> *The confrontational "cold pitch" was one of the riskiest methods, putting great psychological pressure on a target, and often failed. Even when successful, it often produced agents whose handlers had to maintain constant pressure on them to stay involved. When such agents had a chance to cut their ties—when they were assigned to new posts or when communications with their contacts became risky—they often took it.*
>
> -- Victor Cherkashin, KGB Counterintelligence Officer and author of *Spy Handler* (2005)
>
> ---
>
> *Nobody likes cold pitches because they're the worst technique in the profession of intelligence. It's going up to somebody whom you don't know and asking them to do the equivalent of going to bed with you. It's a very intimate, and if you're not developing it from a practical interrelationship human kind of way, 99.9 percent of the folks will say no.*
>
> -- Michael T. Rochford, Chief, Espionage Section, Counterintelligence Division, FBI as quoted in *The Secrets of the FBI* (2011) by Ronald Kessler, p. 125

Cold War. Term generally used to describe the long-term, but nonshooting, conflict or state of tension between the United States and the Soviet Union that lasted from the close of World War II in 1945 until the collapse of the Soviet Union in 1991. (*Encyclopedia of the CIA*, 2003)

COLISEUM. See *Community On-Line Intelligence System for End-Users and Managers*.

Collaborating Analytical Center (CAC). An intelligence organization that has responsibility to support and assist a Responsible Analytical Center (RAC) produce an intelligence product to answer a specific COCOM Intelligence Task List (ITL) task or sub-task. CACs may provide all-source analysis, application of analysis, or single-source analysis, exploitation, or reporting. DoD organizations that may serve as CACs include: Combat Support Agencies (DIA, NSA, NGA), the COCOM JIOCs, and the Service Intelligence Centers (NGIC, ONI, NASIC & MCIA). (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007)

Collateral. All national security information classified Confidential, Secret, or Top Secret under the provisions of an Executive Order for which special systems of compartmentation (such as SCI or SAPs) are not formally required. (DoDI 5200.01, 9 Oct 2008)

Collation. The organizing of relevant information in a coherent way, looking at source and context. It includes evaluating the information for accuracy, completeness, and meaning. (Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach*, 2004)

Collection. In intelligence usage, the acquisition of information and the provision of this information to processing elements. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012) Also see *counterintelligence collection*; *clandestine intelligence collection; intelligence collection; military counterintelligence collection*.

-- Also, the acquisition of information to meet an intelligence requirement. (ICD 300, 3 Oct 2006)

> ICD 300 (*Management, Integration, and Oversight of Intelligence Collection and Cover Action*, 3 Oct 2006) establishes DNI policy to integrate, prioritize, and maximize IC collection capabilities and activities to produce timely and useful national intelligence information for policymakers, Defense, and other intelligence consumers.

-- Also, the identification, location, and recording and storing of information— typically from an original source and using both human and technological means—for input into the Intelligence Cycle for the purpose of meeting a defined tactical or strategic intelligence goal. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, the exploitation of sources by collection agencies, and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. (National HUMINT Glossary)

-- Also, the acquisition of information by any means and its delivery to the proper intelligence processing unit for use in the production of intelligence. (Senate Report 94-755, Book I, 26 Apr 1976)

"*Collection is the gathering of valued information, much of it by clandestine means."*

-- Roy Godson, Dirty Tricks or Trump Card: US Covert Action and Counterintelligence (1995), p.1

"*The collection of information is the foundation of everything that the Intelligence Community does. While successful collection cannot ensure a good analytical product, the failure to collect… turns analysis into guesswork*."

-- *WMD Report* (2005); p. 351

EO 12333, *US Intelligence Activities*, directs that IC elements use the least intrusive collection techniques feasible within the United States or directed against US persons abroad (para 2.4 - Collection Techniques).

Collection Agency. Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Collection Asset. A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Collection Emphasis. Identifies new short- to intermediate-term information needs in response to unforeseen situations, emerging crises, or contingencies. It can be used to register additional or refined requirements in connection with a unique collection opportunity. (DoD CI Collection Integrated Working Group Handbook 1-02, 8 Aug 2006)

Collection Management (CM). In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and re-tasking, as required. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

CM has two distinct functions: collection requirements management (CRM) and collection operations management (COM). CRM established the collection need and COM provides the "how to" for conducting the actual collection. See *collection requirements management* and *collection operations management.*

"The matters that interest an intelligence service are so numerous and diverse that some order must be established in the process of collecting information."

-- Allen W. Dulles, *The Craft of Intelligence* (2006), p.75

Collection Management Authority (CMA). Within DoD, CMA constitutes the authority to establish, prioritize, and validate theater collection requirements, establish sensor tasking guidance, and develop theater-wide collection policies. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Collection Manager. An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Collection Operations Management (COM). The authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *collection management*; *collection requirements management*.

> COM is the process by which it is determined **"how"** a requirement will be answered within an intelligence discipline and "who" will execute the collection activity.
>
> _____
>
> *"Essentially, CRM is what gets done in the collection cycle, while COM is how it gets done."*
> -- ODNI, *U.S. National Intelligence – An Overview 2011*

Collection Plan. A systematic scheme to optimize the employment of all available collection capabilities and associated processing, exploitation, and dissemination resources to satisfy specific information requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013)

> The collection plan determines how a collection requirement will be satisfied.

Collection Planning. A continuous process that coordinates and integrates the efforts of all collection units and agencies. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Collection Posture. The current status of collection assets and resources to satisfy identified information requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Collection Requirement. A valid need to close a specific gap in intelligence holdings in direct response to a request for information (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *intelligence requirement; information requirements*.

-- Also, 1) An intelligence need considered in the allocation of intelligence resources. Within the Department of Defense, these collection requirements fulfill the essential elements of information and other intelligence needs of a commander, or an agency; or 2) An established intelligence need, validated against the appropriate allocation of intelligence resources (as a requirement) to fulfill the essential elements of information and other intelligence needs of an intelligence consumer. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Collection Requirements Management (CRM). The authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either the direct tasking of assets over which the collection manager has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *collection management; collection operations management*.

> CRM is the process by which it is determined **"what"** will be collected and by "which" intelligence discipline. CRM defines "what" intelligence systems must collect and focuses on the requirements of the customer; it is all-source oriented and advocates "what" information is necessary for collection.

Collection Resource. A collection system, platform, or capability that is not assigned or attached to a specific unit or echelon which must be requested and coordinated through the chain of command. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Collection Strategy. An analytical approach used by collection managers to determine which intelligence disciplines can be applied to satisfy information requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Collection Support Brief (CSB). A supplement to a collection requirement on key country topics, technical subjects, and other complex issues. It provides more detailed tutorial information for HUMINT collectors regarding technical developments, organizations, facilities, and personalities associated with the collection topic. (DHE-M 3301.002, Vol II, Collection Operations, 23 Nov 2010)

Collector. A person who acquires information or services from a source. (HDI Lexicon, Apr 2008)

Combat Intelligence. *Within DoD: None – term removed from JP 1-02 per JP 2-0 Joint Intelligence 22 Oct 2013.*

> Previously defined in JP 1-02 as: that knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations.

Combat Support Agency (CSA). A Department of Defense agency so designated by Congress or the Secretary of Defense that supports military combat operations. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Combatant Command (COCOM) A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Combatant Command (command authority). Nontransferable command authority, which cannot be delegated, of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces; assigning tasks; designating objectives; giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013) Also see *Unified Command Plan*.

Combatant Commander (CCDR). A commander of one of the unified or specified combatant commands established by the President. (JP 1-02) Also see *Unified Command Plan*.

Combating Terrorism (CbT). Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. (JP 1-02 and JP 3-26, Counterterrorism, 13 Nov 2009)

-- Also, within DoD, encompasses all actions taken to oppose terrorism throughout the entire threat spectrum including terrorist use of CBRNE devices. Actions taken include AT, counterterrorism, terrorism consequence management, and intelligence support (collection, analysis, and dissemination of terrorism-related information). (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013)

Combat Support Agency (CSA). A Department of Defense agency so designated by Congress or the Secretary of Defense that supports military combat operations. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Command and Control (C2). The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Command Counterintelligence Coordinating Authority (CCICA). The senior command representative to conduct and exercise staff coordination authority over CI activities. Develops and implements the Combatant Command's CI strategy and plans, serves as the focal point for CI issues impacting the command, identifies command resource requirements, and coordinates CI support to the command. Formerly known as "CI Staff Officer" [or CISO]. (DoDI 5240.10, CI in the Combatant Commands and Other DoD Components, 5 Oct 2011 with change 1 dated 15 Oct 2013)

Note: this term is approved for inclusion in the next edition of JP 1-02.

-- Also, the Combatant Commander's senior representative for CI. The CCICA serves as the authoritative point of contact for the Combatant Command on CI issues and activities and assists in exercising the command's CI activities. JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *Counterintelligence Coordinating Authority (CICA)*.

The CCICA is a CI subject matter expert and the senior CI adviser to the Combatant Command. DoD Instruction 5240.10 directs that the CICCA shall be either a military O5/O6 or civilian equivalent, and shall have CI experience [not further defined].

For additional information see JP 2.01.2, *CI & HUMINT in Joint Operations*, 11 Mar 2011 (para 2a)

Commander's Critical Information Requirement (CCIR). An information requirement identified by the commander as being critical to facilitating timely decision-making. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Committee of Foreign Investment in the United States (CFIUS). An interagency committee that serves the President in overseeing the national security implications of foreign investments. (Department of Treasury website at <http://www.treas.gov/offices/international-affairs/exon-florio/>)

CFIUS has 12 members under the chairmanship of the Secretary of Treasury consisting of: the Secretaries of State, Defense, Commerce, and Homeland Security, the Attorney General, Director OMB, Director of the Office of Science and Technology Policy, Assistant to the President for National Security Affairs, Assistant to the President for Economic Policy, US Trade Representative, and Chairman of the Council of Economic Advisers.

-- Department of Treasury website (cited above)

Originally established in 1975 by EO 11858 mainly to monitor and evaluate the impact of foreign investment in the United States. In 1988, EO 12661 designated CFIUS to receive notices of foreign acquisitions of U.S. companies, to determine whether a particular acquisition has national security issues sufficient to warrant an investigation and to undertake an investigation, if necessary, and to submit a report and recommendation to the President at the conclusion of an investigation.

On 26 July 2077, *the Foreign Investment and National Security Act of 2007* (PL 110-49) was enacted. The act was implemented by EO 13456 and addresses many issues, e.g., Congressional notification requirements; more stringent rules for the review and formal investigation of transactions, especially those involving foreign governments or critical infrastructure assets; requires senior-level involvement in various required certifications and reports, limiting the agencies' delegation authority; established the membership of CFIUS by statute; and created a defined role for the Director of National Intelligence as an ex-officio member who must evaluate the transaction's national security implications.

Also see CRS Report: <http://www.fas.org/sgp/crs/natsec/RL33388.pdf>

Common Operational Picture (COP). A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

-- Also, (Army) A single display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command. (ADRP 6-0, Mission Command, May 2012)

Communications Cover. Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Communications Intelligence (COMINT). Technical information and intelligence derived from foreign communications by other than the intended recipients. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *signals intelligence.*

-- Also, the capture of information, either encrypted or in "plaintext," exchanged between intelligence targets or transmitted by a known or suspected intelligence target for the purpose of tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, or analysis of the substantive meaning of the communication. COMINT is a sub-discipline of SIGINT. (ODNI, U.S. National Intelligence – An Overview 2011)

COMINT is a sub-category of signals intelligence that engages in dealing with messages or voice information derived from the interception of foreign communications. It is produced by the collection and processing of foreign communications passed by radio, wire or other electromagnetic means, and by the processing of foreign encrypted communications, however transmitted. Collection comprises search, intercept, and direction finding.

Communications Intelligence or COMINT: technical and intelligence information derived from foreign communications by other than intended recipients. COMINT activities… those activities that produce COMINT by the collection and processing of foreign communications passed by radio, wire, or other electromagnetic means… and by processing foreign encrypted communications, however transmitted. Collection comprises search, intercept and direct finding. Processing comprises range estimation, transmitter, operator identification, signal analysis, traffic analysis, cryptanalysis, decryption study of plain text, the fusion of these activities and the reporting of results.

-- NSCID 6, Signals Intelligence, 17 Feb 1972 (redacted copy, complete original version is TOP SECRET) Available at: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/docs/doc05.pdf

---

[T]here 'is' something special about communications intelligence… in a nutshell, its special value lies in the fact that this kind of intelligence is generally accurate, reliable, 'authentic,' continuous, and most of all, 'timely'.

-- NSA, A History of U.S. Communications Security (U) [Vol I], revised July 1973, p.9; originally classified SECRET/NORFORN//COMINT, declassified by NSA 10 Dec 2008)

Communications Security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (JP 1-02 and JP 6-0, Joint Communications Systems, 10 Jun 2010)

-- Also, protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, emissions security, and jamming resistance) to telecommunications and to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to COMSEC information or materials. (DoDD 4640.6 Communications Security Telephone Monitoring and Recording, 26 Jun 1981)

-- Also, measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (DoDD 5100.20, NSA, 26 Jan 2010)

-- Also, a component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material. (CNSS Instruction No, 4009, National IA Glossary, 26 Apr 2010)

Communications Security Monitoring. The act of listening to, copying, or recording transmissions of one's own circuits (or when specially agreed, e.g., in allied exercises, those of friendly forces) to provide material for communications security analysis in order to determine the degree of security being provided to those transmissions. In particular, the purposes include providing a basis for advising commanders on the security risks resulting from their transmissions, improving the security of communications, and planning and conducting manipulative communications deception operations. (previously in JP 1-02)

Community On-Line Intelligence System for End-Users and Managers (COLISEUM). The management system for production requirements and requests for information. CI production. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

-- Also, an analysis requirements management tool used throughout the DIE for tasking and managing requirements for finished intelligence production. (DoDI 3020.51, Intelligence Support to DCIP, 23 Jun 2011)

-- Also, the primary production requirements management system for the Defense Intelligence Analysis Program (DIAP). It supports the DIAP mission to consolidate and gain synergism of DoD intelligence production resources by automating the basic production requirement process defined in the DIAP and its key operational concepts. (DIA DIAP)

-- Also, an analysis requirement management tool used throughout the Defense Intelligence Community to register and track requests for information/analytical requirements, search for existing intelligence, and manage/account for analytical resources. It is a web-based application available through Intelink. (Joint Military Intelligence Training Center, *Fundamentals of COLISEUM 5.0*, Jun 2008)

> *Defense CI Components shall use the CI-approved electronic archiving system to validate, task, and disseminate production requirements for CI analysis. The approved system is the primary method to communicate analysis and production requirements within the DoD CI enterprise. Defense CI Components without access to the approved system may use COLISEUM.*
>
> -- DoDI 5140.18, *CI Analysis & Production*, 17 Nov 2009

Compartmentation. The principle of controlling access to sensitive information so that it is available only to those individuals or organizational components with an official ”need-to-know” and only to the extent required for the performance of assigned responsibilities. (National HUMINT Glossary) Also see *Bigot List*.

-- Also, establishment and management of an organization so that information about the personnel, internal organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

-- Also, management of an intelligence service so that information about personnel, organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties. (FBI FCI Terms)

-- Also, the practice of establishing specials channels for handling sensitive intelligence information. The channels are limited to individuals with a specific need for such information and who are therefore given special security clearances in order to have access to it. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- Also, the process of strictly limiting the number of people who are aware of a given intelligence operation…. Only personnel with an absolute "need to know" should be admitted into the compartment. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

> The primary purpose of compartmentation is security, to protect extremely sensitive information from compromise.
>
> _____
>
> ***An intelligence service that is careless about compartmentation pays the price.***
> -- James M. Olson, Former Chief of CIA Counterintelligence
>
> _____
>
> ***Effective compartmentation is fundamental to all secret activity….***
> -- Richard Helms, Former Director CIA (1966-1973)
> (see Richard Helms with William Hood, *A Look Over My Shoulder*, 2003, pp.184-185)
>
> _____
>
> ***[It's]…essential to practice strict compartmentation in counterintelligence investigations.***
> -- Colonel Stuart A. Herrington, US Army (Ret)
> (see *Traitors Among Us: Inside the Spy Catcher's World*,1999, pp.272-273)

Compartmented Intelligence. National intelligence placed in a DNI-approved control system to ensure handling by specifically identified and access approved individuals. (IC Standard 700-1, 4 Apr 2008)

-- Also, national intelligence information under a control system and only available to designated individuals. (National Intelligence: A Consumer's Guide - 2009).

> *Compartmented intelligence became institutionalized during World War II [SIGINT, e.g., ULTRA, MAGIC, etc.]…. Compartmentalizing information is the way they restrict what is known.*
> -- William E. Burrows, *Deep Black* (1986)
>
> _____
>
> *In the secret operations canon it is axiomatic that the probability of leaks escalates exponentially each time a classified document is exposed to another person…. Effective compartmentation is fundamental to all secret activity.*
> -- Richard Helms (Former DCI), *A Look Over My Shoulder* (2003)

Complaint-type Investigation. A counterintelligence investigation in which sabotage, espionage, treason, sedition, subversive activity, or disaffection is suspected. (JP 1-02)

Complex Catastrophe. Any natural or man-made incident, including cyberspace attack, power grid failure, and terrorism, which results in cascading failures of multiple, interdependent, critical, life-sustaining infrastructure sectors and causes extraordinary levels of mass casualties, damage or disruption severely affecting the population, environment, economy, public health, national morale, response efforts, and/or government functions. (Deputy Secretary of Defense Memorandum, 19 February 2013 cited in JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013) Also see *catastrophic event*.

Compromise. A communication or physical transfer of classified information to an unauthorized recipient. (DoDD 5200.1, DoD Information Security Program, 13 Dec 1996)

-- Also, an unauthorized disclosure of classified information. (DoDM 5200.01-Vol 1, DoD Information Security, 24 Feb 2012 and DoD 5220.22-M, NISPOM, 28 Feb 2006)

-- Also, the known or suspected exposure of clandestine personnel, installations, or other assets or of classified information or material, to an unauthorized person. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the disclosure or release of classified information to unauthorized person(s). (IC Standard 700-1, 4 Apr 2008

-- Also, type of incident where information is disclosed to unauthorized individuals or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a known or suspected exposure of clandestine personnel, installations, or other assets, or of classified information or material, to an unauthorized person. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Compromised. A term applied to classified matter, knowledge of which has, in whole or in part, passed to an unauthorized person or persons, or which has been subject to risk of such passing. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, when an operation, asset, or agent is uncovered and cannot remain secret. (CI Centre Glossary)

Compromising Emanations. Unintentional emissions that could disclose information being transmitted, received, or handled by any information-processing equipment. (ICS Glossary) Also see *TEMPEST; TEMPEST Test.*

-- Also, unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled or otherwise processed by information system equipment. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010; also NSTISSI 7002)

Computer Forensics. The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, the scientific, systematic inspection and analysis of digital media and its contents to gather information on the facts and circumstances which may connect an incident to a threat to national security or other computer use that is contrary to security of information systems or may indicative of espionage. The objectives are to perform a structured investigation, maintain the proper chain of evidence, reconstruct the activities of a computer user, and preserve the integrity of the data. (AR 381-20, Army CI Program, 25 May 2010)

Computer Intrusion. *Within DoD: None – term removed from JP 1-02 per JP 3-13, Cyberspace Operations, 5 Feb 2013.*

> Previously defined in JP 1-02 as: an incident of unauthorized access to data or an automated information system.

Computer Intrusion Detection. *Within DoD: None – term removed from JP 1-02 per JP 3-13, Cyberspace Operations, 5 Feb 2013.*

> Previously defined in JP 1-02 as: the process of identifying that a computer intrusion has been attempted, is occurring, or has occurred.

Computer Network. The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010 with change 1 dated 16 Oct 2013)

Computer Network Attack (CNA). Operations to manipulate, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (DCID 7/3, Information Operations and IC Related Activities (U), 1 Jul 1999, updated 5 Jun 2003)

> *Within DoD: None – term removed from JP 1-02 per JP 3-13, 27 Nov 2012.*
>
> Defined in the previous edition of JP 3-13, *Information Operations*, dated 13 Feb 2006, as: Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense (CND). Efforts to defend against the computer network operations of others, especially that directed against U.S. and allied computers and networks. (DCID 7/3, Information Operations and IC Related Activities (U), 1 Jul 1999, updated 5 Jun 2003)

> *Within DoD: None – term removed from JP 1-02 per JP 3-13, 27 Nov 2012.*
>
> Previously defined as: Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks.

Computer Network Exploitation (CNE). Intelligence collection and enabling operations to gather data from target or adversary automated information systems or networks. (DCID 7/3, Information Operations and IC Related Activities (U), 1 Jul 1999, updated 5 Jun 2003)

> *Within DoD: None – term removed from JP 1-02 per JP 3-13, 27 Nov 2012).*
>
> Previously defined as: Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

Computer Network Operations (CNO). *Within DoD: None – term removed from JP 1-02 per JP 3-13, 27 Nov 2012.*

> Previously defined as: comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

Computer Security (COMUSEC). The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010) Also see *Information Security (INFOSEC); Cybersecurity.*

Computer Trespasser. A person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; see 18 USC 2510 (21)(a). (AR 381-20, Army CI Program, 25 May 2010)

Computer Virus. A software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. (US Army TRADOC DCSINT Handbook 1.02, 15 Aug 2007)

-- Also, a computer program that can copy itself and infect a computer without permission or knowledge of the user. (Wikipedia; accessed 2 Oct 2007)

Concealed Monitoring. Targeting by electronic, optical, or mechanical devices a particular person or a group of persons without their consent in a surreptitious and continuous manner. Monitoring is surreptitious when it is targeted in a manner designed to keep the subject of the monitoring unaware of it. Monitoring is continuous if it is conducted without interruption for a substantial period of time. (DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect US Persons, Dec 1982)

> Concealed monitoring includes, but is not limited to the use of microphones, video cameras, beepers, beacons, transponders, and GPS locators.
>
> Within DoD, if there is a reasonable expectation of privacy, a Procedure 6 is required IAW DoD 5240.1-R. Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,

Concealment. The act of remaining hidden. (DSS Glossary)

Concealment Device (CD). A container designed to hide materials. (HDI Lexicon, April 2008)

-- Also, innocuous object designed or adapted as a container for secreting any selected material or equipment. Also called containers. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, any one of a variety of innocuous devices used to secretly store and transport materials relating to an operation. (CI Centre Glossary)

-- Also, an object modified or fabricated to contain either a device or intelligence materials for the purpose of covert storage, transport, placement within a target, or dead-dropping. (Spycraft)

Concept of Intelligence Operations. Within the Department of Defense, a verbal or graphic statement, in broad outline, of an intelligence directorate's assumptions or intent in regard to intelligence support of an operation or series of operations. (JP 2.0, Joint Intelligence, 22 Oct 2013)

Concept of Operations (CONOPS). A verbal or graphic statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using available resources. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Concept Plan (CONPLAN). In the context of joint operation planning level 3 planning detail, an operation plan in an abbreviated format that may require considerable expansion or alteration to convert it into a complete operation plan or operation order. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Conduits. Within military deception, conduits are information or intelligence gateways to the deception target. Examples of conduits include: foreign intelligence and security services, intelligence collection platforms, open-source intelligence, news media—foreign and domestic. (JP 3-13.4, Military Deception, 26 Jan 2012) See *military deception*.

Confidential. Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe. (EO 13526, Classified National Security Information, 31 Dec 2009) Also see *security classification.*

Confidential Source. Any individual or organization that provides information to the U.S. Government on matters pertaining to national security and expects, in return, that the information or relationship, or both, will be held in confidence. This definition is not to be confused with "intelligence source" as used in the Human Intelligence Community. (IC Standard 700-1, 4 Apr 2008)

-- Also, any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence. (EO 13526, Classified National Security Information, 31 Dec 2009)

-- Also [within AFOSI], any individual whose identity is being protected, with whom AFOSI establishes a formal managed relationship, and whose AFOSI directed activities result in the gathering of information or testimonial or physical evidence. This does not include those individuals who provide information as a result of their official duties or one time witness to an incident or crime. (AFOSI Manual 71-118, Vol I, Confidential Source Management, 3 Oct 2002)

Confusion Agent. An individual dispatched by his sponsor to confound the intelligence or counterintelligence apparatus of another country rather than to collect and transmit information. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- *Within DoD: None – term removed from JP 1-02 (rescinded 11 Mar 2011).*

> Previously defined in JP 1-02 as: an individual who is dispatched by the sponsor for the primary purpose of confounding the intelligence or counterintelligence apparatus of another country rather than for the purpose of collecting and transmitting information.

Congressional Intelligence Committees. The Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). Also see *SSCI; HPSCI*.

> The 1980 Intelligence Oversight Act charged the SSCI and HPSCI with authorizing the programs of US intelligence agencies and overseeing their activities.
> -- SSCI website at <http://intelligence.senate.gov/> and HPSCI at <http://intelligence.house.gov/>

Consensual Monitoring. Monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication. (Attorney General's Guidelines for Domestic FBI Operations, 29 Sep 2008)

Consolidated Adjudications Facility (CAF). The DoD CAF, under the direction of the Washington Headquarters Services (WHS)—a DoD Field Activity—grants, denies, or revokes eligibility for access to classified information and eligibility for occupancy of sensitive positions, and supports the use of automated and consolidated adjudicative processes to the maximum extent practicable in accordance with DoDD 5220.6 (Defense Industrial Personnel Security Clearance Review Program) and DoD Regulation 5200.2-R (Personnel Security Program).

> DoD established the DoD CAF to consolidate resources and standardize adjudicative processes. On May 3, 2012, the Deputy SECDEF directed a complete consolidation of the functions, resources, and assets of the Army Central Clearance Facility, Department of the Navy CAF, Air Force CAF, Joint Staff CAF, Washington Headquarters (WHS) CAF, Defense Industrial Security Clearance Office (DISCO), and the Defense Office of Hearings and Appeals (DOHA) into a single organization under the authority, direction and control of the Director of Administration and Management. The DoD CAF is located on Fort Meade, MD.

Constraint. In the context of joint operation planning, a requirement placed on the command by a higher command that dictates an action, thus restricting freedom of action. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Contact Report (CR). A report of an operational event; a format providing the officer the ability to document routine aspects of operational activities not otherwise covered by other intelligence or operational reporting. (National HUMINT Glossary)

-- Also, a report used during the conduct of source operations to document the circumstances of, and establish a historical report of the operation. (Army FM 2.22-2, Counterintelligence, Oct 2009)

Contamination. Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Continental United States (CONUS). United States territory, including the adjacent territorial waters, located within North America between Canada and Mexico. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Contingency. A situation requiring military operations in response to natural disasters, terrorists, subversives, or as otherwise directed by appropriate authority to protect US interests. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Contingency Planning Guidance (CPG). Secretary of Defense written guidance, approved by the President, for the Chairman of the Joint Chiefs of Staff, which focuses the guidance given in the national security strategy and Defense Planning Guidance, and is the principal source document for the Joint Strategic Capabilities Plan. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Contingency Operation. A military operation that is either designated by the Secretary of Defense as a contingency operation or becomes a contingency operation as a matter of law (Title 10, USC §101[a][13] and JP1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Continuity of Government (COG). A coordinated effort within the Federal Government's executive branch to ensure that National Essential Functions continue to be performed during a Catastrophic Emergency. (NSPD 51, National Continuity Program, 9 May 2007)

-- Also, a coordinated effort within the Executive Branch that ensures the continuation of minimum essential functions in any emergency situation, including catastrophic emergencies that impair or threaten day-to-day operations of departments/agencies within the branch. COG activities involve ensuring the continuity of minimum essential functions utilizing infrastructures outside the Washington Metropolitan Area (WMA) and must be capable of implementation with and without warning. (NIP - *FY 2009 Congressional Budget Justification* Book, redacted version)*

* Copy available at: <http://www.fas.org/irp/dni/cbjb-2009.pdf > (accessed 24 Jan 2013.

Continuous Evaluation. Means reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information. (EO 13467, 2 Jul 2008 & DoDI 5200.02, DoD Personnel Sceurity Program, 21 Mar 2014)

All personnel in national security positions shall be subject to continuous evaluation.
-- DoDI 5200.02, DoD Personnel Security Program, 21 Mar 2014 (encl 3, para 6)

Control. [As used in intelligence human source operations], the capacity of a case officer (and his service) to generate, alter, or halt agent behavior by using or indicating his capacity to use physical or psychological means of leverage. (Source: John P. Dimmer, Jr., “Observations on the Double Agent,” *Studies in Intelligence*, vol. 6, no. 1 (Winter 1962), pp 57-72. Declassified, originally classified SECRET)

-- Also, [in intelligence usage,] physical or psychological pressures exerted with the intent to assure that an agent or group will respond as directed. (JP 1-02)

-- Also, physical or psychological pressure exerted on an agent to ensure that he or she responds to directions from an intelligence agency or service. (Spy Book)

> *"A case officer does not control an agent the way he controls an automobile [or] the way a policeman controls an informer. The intelligence officer who thinks of control in absolutes of black and white does his operations a disservice; the areas of gray predominate."*
> -- John P. Dimmer, Jr., CIA Operations Officer (1962)

Control of Compromising Emanations (aka TEMPEST). TEMPEST Countermeasures are designed to prevent exploitation of compromising emanations by containing them within the equipment or IS [inspectable space] of the facility processing classified information. (AR 381-14, Technical Counterintelligence, 30 Sep 2002)

Controlled Information. 1) Information conveyed to an adversary in a deception operation to evoke desired appreciations; or 2) Information and indicators deliberately conveyed or denied to foreign targets to evoke invalid official estimates that result in foreign official actions advantageous to US interests and objectives. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Ops, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Controlled Source. In counterintelligence use, a person employed by or under the control of an intelligence activity and responding to intelligence tasking. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *source; control; controlled source operation*.

Controlled Source Operation (CSO). A type of offensive counterintelligence operation (OFCO); see DoDI S-5240.09, OFCO, 29 Oct 2008 (*under revision*).

Controlled Technical Services (CTS). The controlled use of technology to enhance counterintelligence and human intelligence activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Ops, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> *CTS include asset communications, validation tools, tailored form factors, and technology or tools used with sources or CI and HUMINT officers to enhance their collection efforts. CTS are a support function of CI and HIMINT and are not independent operations.*
> -- JP 2.01.2, *CI & HUMINT in Joint Operations*, 11 Mar 2011 w/ chg 1 (p. II-15)

Controlled Unclassified Information (CUI). Unclassified information that does not meet the standards for National Security Classification under Executive Order 12958 but is (1) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. (White House Memo, subj: Designation and Sharing of Controlled Unclassified Information, dated 7 May 2008)

> All federal agencies routinely generate, use, store, and share information that, while not appropriate for "classification" under EO 12958 or other authority, nevertheless requires some level of protection from unauthorized access and release. Currently this information is identified by over 100 unique markings and handling regimes, such as "Law Enforcement Sensitive," "FOUO," etc.
>
> An Interagency Task Force reviewed the CUI framework and recommended that the definition of CUI should be simplified to: *All unclassified information for which, pursuant to statute, regulation, or departmental or agency policy, there is a compelling requirement for safeguarding and/or dissemination controls*.
>
> See *Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information*, 25 August 2009, at <http://www.dhs.gov/xlibrary/assets/cui_task_force_rpt.pdf>

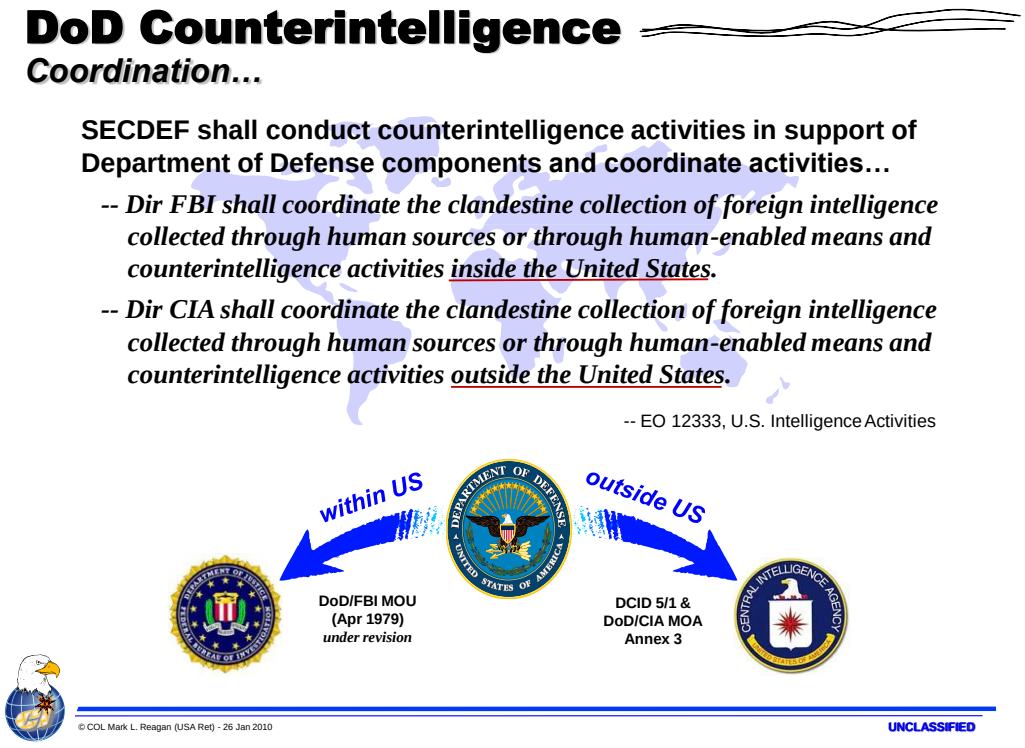
Cooperative Contact. An asset validation term referring to an individual who wittingly responds to tasking in certain areas, but is unwilling to enter into a controlled clandestine relationship. (National HUMINT Glossary)

Cooperative Detainee. A detainee who has established a pattern of answering all questions truthfully and unconditionally and, in fact, answers all questions truthfully and unconditionally. A detainee is not cooperative if the detainee refuses to answer, avoids answering, or falsely answers questions, or if the detainee is intentionally deceptive. A detainee who fluctuates between cooperation and resistance is not cooperative. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

Co-Opted Worker or Co-Optee. A national of a country, but not an officer or employee of that country's intelligence service, who assists that service on a temporary or opportunity basis. (ICS Glossary & CI Community Lexicon)

Coordination. The process of sharing information regarding planned activity, affording potentially affected parties the opportunity to comment, prior to undertaking action. The process of coordination does not infer seeking authorization for action. (DoDD S-5200.37, Management and Execution of Defense HUMINT (U), 9 Feb 2009)

-- Also, the process of sharing operational information and deconflicting activities prior to undertaking a proposed action. Coordination does not require approval or disapproval of the proposed action. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations (U), 9 Jan 2013 w/ chg 1, dated 13 Jun 2013)



EO 12333 directs that the Director FBI coordinates CI activities inside the U.S. and that Director CIA coordinates CI activities outside the U.S. For coordination of DoD CI activities see:

-- **DoD/FBI MOU**: Memorandum of Understanding between the FBI and DoD Governing Information Sharing, Operation Coordination, and Investigative Responsibilities, 2 Aug 2011
+ Annex A - Counterterrorism Information Sharing, 14 Mar 2012
+ Annex B - Counterintelligence Investigative Information Sharing, 9 Dec 2011
+ Annex C - *To be Published* -- Coordinating Counterintelligence Activities
+ Annex TBD - *To be Published* -- Joint Terrorism Task Force (JTTF)

Note: The DoD/FBI MOU (Aug 2011), along with Annexes A, B, and future annexes covering Counterintelligence and Counterterrorism Jurisdiction and Operational Activities, when approved, supersede

the MOA Between the Attorney General and the Secretary of Defense, "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation (U), dated 5 April 1979 and the 1996 supplement thereto, "MOU Regarding Coordination of Counterintelligence Matters."

The DoD/FBI MOU (2011) defines ***Operational Coordination*** as: *"The solicitation of inputs prior to undertaking a proposed action, with the understanding that no such action will be taken until any identified objections have been resolved."*

-- **DoD/CIA MOA:** Annex 3 to the Memorandum of Agreement Between the Central Intelligence Agency and the Department of Defense, "MOA Between CIA and DoD Regarding CI Activities Abroad (U)," 6 Dec 2007, classified SECRET//NOFORN

Note: Annex 3 streamlines the coordination process by assigning primary responsibility for deconfliction to DoD CI field elements and the local Chief of Station/Chief of Base and defines "coordination" as the process of sharing operational information and deconflicting activities prior to undertaking a proposed action. (USD/I Memo, subj: Procedures for Coordination of Counterintelligence Activities Outside the United States, 4 Jan 2008).

For coordination regarding HUMINT activities see ICD 304, *Human Intelligence*, 6 Mar 2008

Coordinating Authority. The commander or individual who has the authority to require consultation between the specific functions or activities involving forces of two or more Services, joint force components, or forces of the same Service or agencies, but does not have the authority to compel agreement. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Counter Surveillance. Measures or actions taken when under verified or suspected surveillance. (DoDI S-5240.15, FPRG, 20 Oct 2010) Also see *countersurveillance*; *surveillance*; *surveillance detection.*

Counter Threat Finance (CTF). Efforts to stop money that funds terrorism, proliferation, narcotics networks, espionage, WMD networks, trafficking in persons, weapons trafficking, precursor chemical smuggling, and other activities that generate revenue through illicit trafficking networks. (*A Guide to Counter Threat Finance Intelligence* by Marilyn B. Peterson, 2009) Also see *threat finance*.

Commander, U.S. Special Operations Command is the DoD CTF lead component for synchronizing DoD CTF activities.

For DoD policy see DoDD 5205.14, *DoD Counter Threat Finance Policy*, 19 Aug 2010 (w/ chg 1 dated 16 Nov 2012).

-- CTF Activities and Capabilities [within DoD]. DoD activities and capabilities, apart from those included under DoD CTFI [Counter Threat Intelligence], to deny, disrupt, destroy, or defeat finance systems and networks that negatively affect U.S. interests in compliance with all existing authorities and procedures. This includes those activities and capabilities undertaken with other Government agencies and/or partner nations. DoD CTF counters financing used to engage in terrorist activities and illicit networks that traffic narcotics, WMDs, improvised explosive devices, other weapons, persons, precursor chemicals, and related activities that support an adversary's ability to negatively affect U.S. interests. (DoDD 5205.14, DoD Counter Threat Finance Policy, 19 Aug 2010)

-- CTF Intelligence (CTFI) [within DoD]. DoD intelligence actions, including those undertaken with other USG agencies and/or coalition partners, that involve the collection, processing, integration, evaluation, analysis, interpretation, production, and dissemination of intelligence products in support of DoD CTF activities and capabilities. (DoDD 5205.14, DoD Counter Threat Finance Policy, 19 Aug 2010)

Counterdeception. Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. *Counterdeception* does not include the intelligence function of identifying foreign deception operations. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006) Also see *deception*; *military deception*.

-- Also, the detection of deception. (Textbook of Political-Military Counterdeception: Basic Principles & Methods, August 2007)

In principle, it should always be possible to unmask a deception.
-- R.V. Jones, *Intelligence and Deception* (1981)

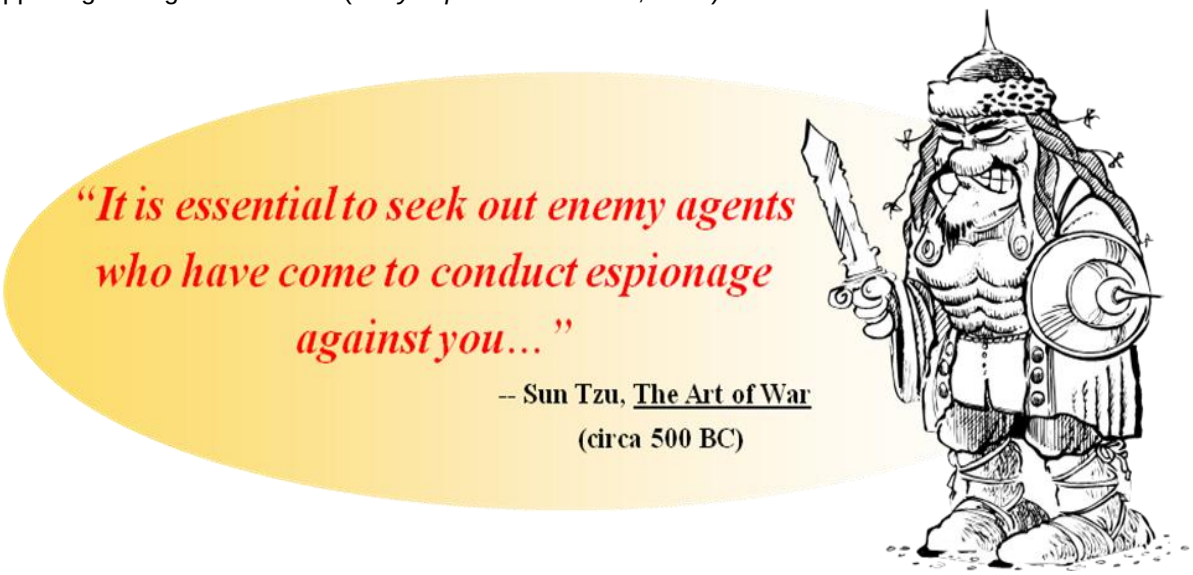
Ideal counterdeception reveals the truth behind the lie, the face beneath the mask, the reality under the camouflage.
-- Barton Whaley, *Textbook of Political-Military Counterdeception: Basic Principles & Methods* (2007)

Counterespionage (CE). That aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *counterintelligence*.

-- Also, actions undertaken to investigate specific allegations or circumstances and to acquire information concerning a person or persons involved in the violation of US espionage laws. (National HUMINT Glossary)

-- Also, those aggressive, comprehensive, and coordinated CI defensive and offensive endeavors worldwide designed to detect, identify, assess, and counter, neutralize, penetrate, or exploit the foreign intelligence threat to the Department of Defense (AR 381-20, Army CI Program, 25 May 2010)

-- Also, the act of conducting counterintelligence operations that involve the penetration of an opposing intelligence service. (*Encyclopedia of the CIA*, 2003)



Counterespionage is often touted as the aristocratic sector of secret operations.
-- Harry Rositzke, *CIA's Secret Operations* (1977)

Counterespionage… is a widely misunderstood branch of secret operations…. CE is an offensive operation, a means of obtaining intelligence about the opposition by using—or, more usually, attempting to use—the opposition's operations. CE is a form of secret intelligence operation, but it is a form so esoteric, so complex and important as to stand by itself.
-- Christopher Felix (James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

Counterespionage (CE) is the offensive, or aggressive, side of counterintelligence. It involves the identification of a specific adversary and a knowledge of the specific operation he is conducting. Counterespionage personnel must then attempt to counter these operations by infiltrating the hostile service (called penetration) and through various forms of manipulation. Ideally, the thrust of the hostile operation is turned back against the enemy.

-- Senate Report # 94-755 (aka Church Committee Report), Book I, 26 April 1976, p. 166

Counterespionage is like putting a virus into the bloodstream of the enemy.

-- Robin W. Winks, *Cloak and Glown: Scholars in the Secret War* (1987), p. 422

Counterfeit Material. An item that is an unauthorized copy or substitute that has been identified, marked, or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source. (DoDI 4140.67, DoD Counterfeit Prevention Policy, 26 Apr 2013) Also see *suspect counterfeit*.

For general background information see Senate Armed Services Committee Report 112-167, *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, 21 May 2012.

Copy at: http://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

Counterguerrilla Operations. Operations and activities conducted by armed forces, paramilitary forces, or nonmilitary agencies against guerrillas. (JP 1-02 and JP 3-24, Counterinsurgency, 22 Nov 2013)

Counterinsurgency (COIN). Comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes. (JP 3-24, Counterinsurgency, 22 Nov 2013)

...the success of a counterinsurgency depends less on defeating the terrorist, guerrilla, or military tactics of the insurgents than on uncovering and undermining the secret network and neutralizing its violent tactics. …The pivotal elements of counterinsurgency are intelligence and counterintelligence.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 165

Counterintelligence (CI). Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities. (Executive Order 12333, as amended 30 July 2008 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *counterespionage*.

Counterintelligence... the core mission simply stated --

Combating Adversarial Intelligence Threats

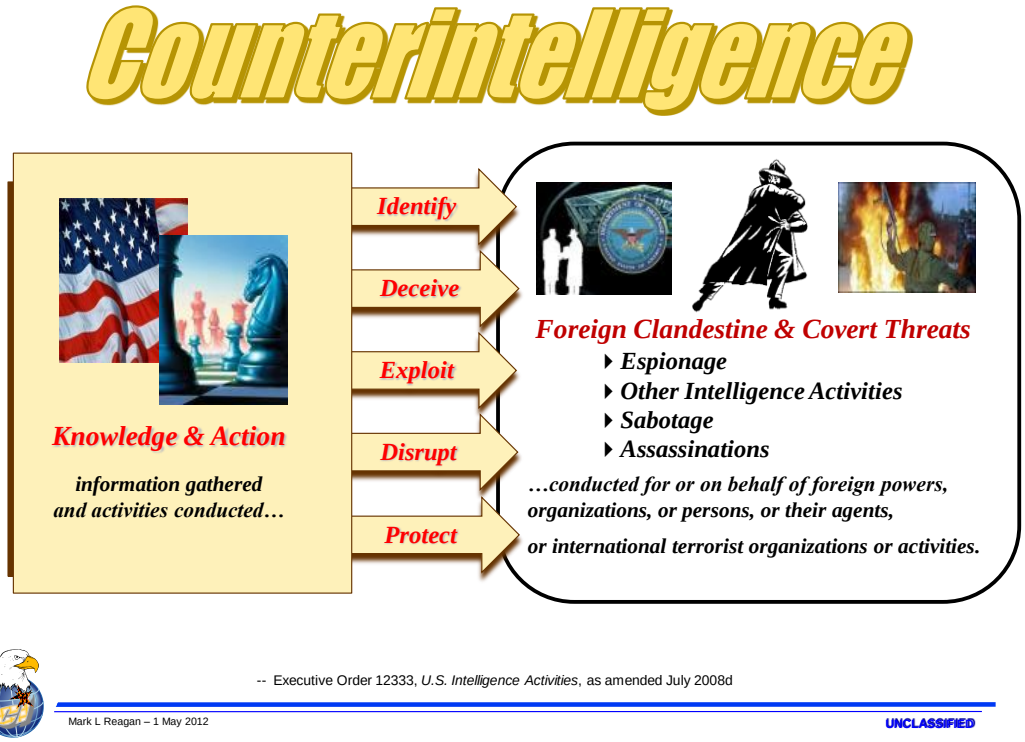
-- COL Mark L. Reagan (USA Ret)

For DoD counterintelligence policy, see DoD Directive O-5240.02, *Counterintelligence*

-- Also, information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (50 USC §401a)

Counterintelligence: [noun] intelligence activities concerned with identifying and countering the threat to security posed by hostile intelligence organizations or by individuals engaged in espionage or sabotage or subversion or terrorism.

hyperdictionary



CI "embraces all activities, human and technical, whether at home or abroad, that are undertaken to identify, assess, neutralize and exploit foreign intelligence threats… counterintelligence is inherently a strategic, national security instrument."
-- Hon. Michelle Van Cleave, NCIX, 18 Nov 2004

-- Also, intelligence activity, with its resultant product, devoted to destroying the effectiveness of inimical foreign intelligence activities and undertaken to protect the security of the nation and its personnel, information, and installations against espionage, sabotage, and subversion. Includes the process of procuring, developing, recording, and disseminating information concerning hostile clandestine activity and of penetrating, manipulating, or repressing individuals, groups, or organizations conducting such activity. (National Security Council Intelligence Directive [NSCID] No. 5, 17 Feb 1972)

-- Also, encompasses actions taken to detect and counteract foreign intelligence activity that adversely affects U.S. national security interest. (WMD Report, 31 Mar 2005)

-- Also, counterintelligence involves all those defensive and offensive activities conducted at home and abroad to protect against traditional and emerging foreign intelligence and international terrorist threats to the national security and to the national defense. (DHE-M 3301.002, Defense HUMINT Enterprise Manual, Vol II: Collection Operations, 23 Nov 2010)

-- Also, counters or neutralizes foreign intelligence and security services (FISS) and international terrorist organizations (ITO) intelligence collection efforts. It does this through collection, CI investigations, operations, analysis, production, and functional and technical services. CI includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies. It is the key intelligence community contributor to the protection of U.S. interests and equities. CI helps identify EEFIs [essential elements of friendly information] by identifying vulnerabilities to threat collection and actions taken to counter collection and operations against U.S. forces. (Army FM 2-0, Intelligence, 23 Mar 2010)

-- Also, the total action taken… by which information is gathered and activities are conducted to protect that agency against espionage, theft of materials, sabotage, assignations, or other intelligence activities conducted by, or on behalf of, hostile foreign governments or other "threatening" foreign organizations (terrorist groups, rogue military units, etc.). (*Encyclopedia of the CIA*, 2003)

-- Also, CI is a discipline and mindset that identifies, analyzes and neutralizes the efforts of others who seek to interfere with our [CIA's] ability to collect and analyze intelligence. (CIA/CIC, circa Mar 2010)

Counterintelligence's core mission can be simply stated as combating adversarial intelligence threats. It is the business of identifying and combating foreign intelligence threats through ***knowledge* and *action*** -- knowledge of and action in countering global adversarial intelligence threats posed by a variety of intelligence entities directed by foreign states, as well as non-state actors, such as transnational terrorist groups.

CI is an integral component of U.S. Intelligence—historically and doctrinally, as well as by statute, executive order and policy. CI is an "intelligence activity" in accordance with the National Security Act of 1947 and EO 12333, which both specifically define "intelligence" as including counterintelligence and foreign intelligence. CI is *intelligence activity* focused on undermining the effectiveness of -- as well as exploiting -- adversary intelligence activities directed against US national security interests. Counterintelligence is one word in the United States -- it is <u>not</u> counter intelligence (two words) or counter-intelligence (hyphenated).

CI is often confused with the foreign intelligence (FI) collection discipline referred to as human intelligence or HUMINT. Although CI and HUMINT are both intelligence activities that operate in the human domain -- ***they are distinctly different…different missions, different authorities, each focused on different content, as well as outcomes.***

The need for CI knowledge and action is much different from the need for FI collection. FI collection values the information above all, whereas CI insists on acting on that information-- *a totally different operational dynamic*.

FI [foreign intelligence] is the task of producing and analyzing otherwise unobtainable intelligence (i.e., "stealing secrets); CI focuses on preventing others from stealing secrets….

-- Andre Le Gallo, "Covert Action: A Vital Option in U.S. National Security Policy, *International Journal of Intelligence and Counterintelligence*, Vol 18 No 2 (Summer 2005), p. 354

[Foreign] intelligence is, in essence, the gathering and analysis of secret information about other nations. Its opposite twin, security, is the protection of one's own secrets. Counterintelligence seeks to protect both of the elements from foreign intelligence activities.

-- *American Counterintelligence and Security for the 21st Century*, The Institute of World Politics

---

Knowledge and <u>Action</u>…

CI *"is a strategic instrument available to states to protect themselves and advance their interests in the struggle for power, wealth, and influence. …But the end product, the mission of counterintelligence, is action—action to protect against foreigners and action to manipulate foreigners in the service of national goals."*

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995)

The primary mission of counterintelligence is to identify, neutralize, and exploit the intelligence or secret infrastructure of others. It is by its very nature both a defensive and offensive tool. … Offensively, counterintelligence helps to advance strategy and policy through knowledge about adversary intelligence and exploit an adversary's vulnerabilities to weaken or manipulate them to advantage. … But only counterintelligence… has the mission and the capabilities to understand, defend against, and exploit an adversary's secret intelligence.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence*, with new introduction by the author (paperback 2001), p. xxviii

---

CI wages "nothing less than a secret war against antagonist intelligence services."
-- U.S. Senate Report 94-755, Book I, 26 April 1976, p. 163

-- Also, CI encompasses information collections, analysis, investigations and operations conducted to identify and neutralize espionage and foreign intelligence activities, the intelligence-related activities of terrorists, and adversary efforts to degrade, manipulate or covertly influence U.S. intelligence, political processes, policy or public opinion. (NIPF [U], Jul 2006)

CI works closely with intelligence, security, infrastructure protections and law enforcement to ensure an integrated approach to the protection of U.S. forces, our intelligence and national assets, U.S. research, development and technology, and the U.S. economy.

CI is composed of both offensive and defensive elements. Offensive CI includes the penetration and deception of adversary groups. Defensive CI involves protecting vital U.S. national security related information from being obtained or manipulated by an adversary's intelligence organizations, activities and operations. This two-pronged approach forms a comprehensive CI strategy that is informed by collection results and feeds more effective CI operations.

Counterintelligence is a universal constant that should be factored in whenever U.S. intelligence or national security capabilities are deployed or when we are targeted by our adversaries. 'Every' U.S. intelligence capability and requirement needs to be protected and 'every' intelligence threat deployed against us should be countered by effective offensive and defensive CI.

-- NIPF - Intelligence Topic Definitions and Information Needs (U), July 2006

-- Also, CI may also be thought of as ***knowledge*** needed for the protection and preservation of the military, economic, and productive strength of the United States, including the security of the Government in domestic and foreign affairs against or from espionage, sabotage, and all other similar clandestine activities designed to weaken or destroy the United States. (Report of the Commission on Government Security - 1957, as cited in Church Committee Report, 26 April 1976, p. 163, footnote 1)

Counterintelligence (CI) is a special form of intelligence activity, separate and distinct from other disciplines. Its purpose is to discover hostile foreign intelligence operations and destroy their effectiveness. This objective involves the protection of the United State Government against infiltration by foreign agents, as well as the control and manipulation of adversary intelligence operations. An effort is made to both discern and decive [sic] the plans and intentions of enemy intelligence services.

Defined more formally, counterintelligence is an intelligence activity dedicated to undermining the effectiveness of hostile intelligence services.

-- Senate Report 94-755 (aka Church Committee Report), 26 April 1976 (p. 163)

Counterintelligence – Senate Report 94-755

Counterintelligence: Activities conducted to destroy the effectiveness of foreign intelligence operations and to protect information against espionage, individuals against subversion, and installations against sabotage. The term also refers to information developed by or used in counterintelligence operations. See counterespionage, countersabotage, and countersubversion [below].

Counterespionage: Those aspects of counterintelligence concerned with aggressive operations against another intelligence service to reduce its effectiveness, or to detect and neutralize foreign espionage. This is done by identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities in order to destroy. Neutralize, exploit, or prevent such espionage activities.

Countersabotage: That aspect of counterintelligence designed to detect, destroy, neutralize, or prevent sabotage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting sabotage activities.

Countersubversion: That part of counterintelligence designed to destroy the effectiveness of subversive activities through the detection, identification, exploitation, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or capable of conducting such activities.

-- Senate Report 94-755 (aka Church Committee Report), Book I – Glossary, 26 April 1976, p. 620.

Counterintelligence Activities. [An alternate term for] one or more of the five functions of counterintelligence: operations, investigations, collection, analysis & production, and functional services. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007; JP 1-02; and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *counterintelligence functions.*

Counterintelligence Activities in Cyberspace. CI activities in cyberspace include those forensics examinations of DoD affiliated information systems and other approved virtual or on-line activities to identify, disrupt, neutralize, penetrate, or exploit FIEs [Foreign Intelligence Entities]. DoD CI activities in cyberspace do not include Offensive Computer Operations as defined in NSPD-38 or the collection and processing of technical and intelligence information derived from foreign communications by other than an intended recipient. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010 with chg 1)

For additional information see --

1) JP 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations (U)*, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011 (para 3f, p. III-17, "CI Activities in Cyberspace").
2) *The DoD Strategy for Counterintelligence in Cyberspace* (28 Aug 2009).
3) *The United States Government-Wide Cyber Counterintelligence Plan - 2008* (classified).

Cyberspace is a Venue

Counterintelligence Analysis. The methodical process of examining and evaluating information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of foreign powers, international terrorists, and other entities. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007 with change 1 dated 20 Dec 2010) Also see *counterintelligence production*.

CI Function: CI Analysis & Production…

Analysis & Production

Assimilating, evaluating, interpreting, and disseminating information of CI relevancy – *a critical enabler providing insights into clandestine & covert threats*

Astute analysis is [a] critical enabler… Strategic analysis allows DoD CI to understand today's risk environment. …[it] allows the Department to learn and use an adversary's pressure points to influence its actions.

-- DoD Counterintelligence Strategy - FY 2004

"It is not enough, of course, simply to collect information. Thoughtful analysis is vital to sound decisionmaking."

-- President Ronald Reagan (4 Dec 1981)

"Analysis – Collecting information is one thing. Making sense of it and using it to frustrate and exploit foreign services is another."

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 81

Counterintelligence Analysis – the Queen of the Counterintelligence Chessboard

Intelligence Community analytical tradecraft standards established in ICD 203, *Analytical Standards*, serve to guide the writing of intelligence analysis and apply to counterintelligence analysis.

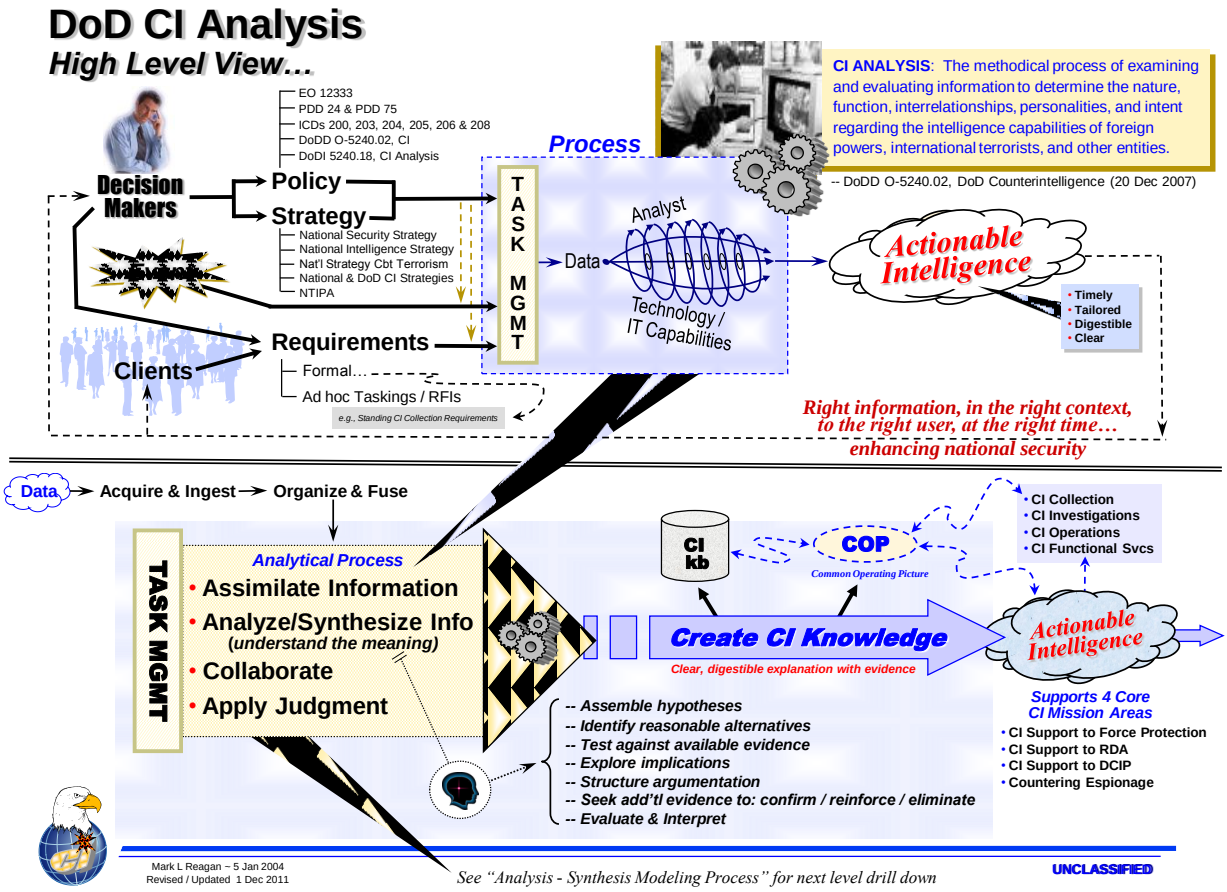
"Effective counterintelligence analysis is a tall order. Good macro-analysis is not synonymous with journalism, or narrative description, or even investigations. Macro-counterintelligence analysis is meant to be explanatory, systematic, empirical, cumulative, reliable, comprehensive, integrated, and policy relevant. Analysis should discover and connect the seemingly disconnected, illuminate hidden relationships, identify unseen linkages, reveal patterns of activity and behavior heretofore unobserved. Good counterintelligence analysis should provide reliable knowledge and authoritative judgments to policymakers and operators. The product of counterintelligence and security analysis is understanding and explanation, and if possible, to answer the questions how and why."

-- Kenneth E, deGraffenreid, *Countering Hostile Intelligence Activities as a Strategic Threat* (1989)

CI analysis drives collections, enhances CI investigative activity, shapes operations, enables mission execution, and informs decision makers

- Also, the process of examining and evaluating information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of state and non-state actors and other entities and activities of CI interest. (JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, a step in the process of producing timely, accurate, and relevant assessments regarding the actual and potential foreign intelligence and international terrorist threat to Department of Defense in which the collected information is subjected to review to identify significant facts for subsequent interpretation. (AR 381-20, Army CI Program, 25 May 2010)



Counterintelligence Analysis – the Queen of the Counterintelligence Chessboard

Analysis – Collecting information is one thing.
Making sense of it and using it to frustrate and exploit foreign services is another.
-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 81

CI Analysis… look at the details and see the passion

I can't possibly overstate the importance of good research. Everyone goes through life dropping crumbs. If you can recognize the crumbs, you can trace a path all the way back from your death certificate to the dinner and a movie that resulted in you in the first place. But research is an art, not a science, because anyone who knows what they're doing can find the crumbs, the wheres, whats, and whos. The art is in the whys: the ability to read between the crumbs, not to mix metaphors. For every event, there is a cause and effect. For every crime, a motive. And for every motive, a passion. The art of research is the ability to look at the details, and see the passion.

-- Daryl Zero, *The Zero Effect* (1998)

Analysis… often raises more questions than it answers. …remember of the basic principle: All action, whether human or physical, disturbs the environment is some way. Find that disturbance and you have a key to the action.

For analysis to play its proper CI role it must be able to survey all of the intelligence data available to one's own government, and it must be able to somehow direct the rest of CI.

-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), pp. 330-331

For a "snap shot" of CI analysis see Irvin D. Sugg, Jr., *Basic Counterintelligence Analysis in a Nutshell: Quick Reference Guide*, Joint Counterintelligence Training Academy (JCITA), n.d. Copy available at: <http://www.ntis.gov/search/product.aspx?ABBR=PB2010105593>

Counterintelligence Analysis and Production Council (CIAPC). The principal forum for coordinating CI analysis and production requirements, discussing CI analysis and production priorities within the enterprise, and discussing other IC issues. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

CIAPC Membership: The Director, Defense CI & HUMINT Center (DCHC), appoints the Chair. Core membership includes the DCHC analysis and production enterprise manager and the managers of the Defense CI Component analysis and production elements. The Chair may expand membership, to include other full-time or permanent part-time Federal employees.

Counterintelligence Analysis and Production Element. The element within a Defense CI Component that performs CI analysis in any form; produces a CI analytical product in any of the categories of CI analysis; or responds to requests for CI analysis from an internal organization and/or from organizations external to the Defense CI Component. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Counterintelligence Analysis Centers. See *ACIC, ICON, MTAC* for DoD CI Analysis Centers. .

Counterintelligence Analysis Report. A document produced by a CI analysis and production element stating the results of analysis regarding a relevant CI topic, event, situation, or development, and containing the characteristics outlined in [DoDI 5240.18] Appendix 2 to Enclosure 3. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Counterintelligence Analytical Product. Any document that contains the work of, is supported by, collaborated on, or produced by a CI analyst at any echelon within a Defense CI Component. It may or may not include CI production. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009)

Objectives of CI analytical products are to: 1) Outline, describe, or illustrate the threat posed by an Foreign Intelligence Entity (FIE) to installations, personnel, assets, operations, or resources; 2) Identify opportunities to conduct offensive CI operations (OFCO) targeting a FIE; and 3) Identify CI investigative opportunities.

CI analytical products seek to satisfy a core CI production requirement to identify people, organizations, locations, activities, and resources associated with a FIE or a target of a FIE.

Within DoD, CI analytical products are categorized based on the purpose of the product, analytical effort, the production timeline, and other distinguishing characteristics. The primary categories of CI analytical products are: 1) Assessment, 2) Analysis Report, 3) Threat Advisory, and 4) Functional Support. Associated analytical products with CI collections, investigations and operations are summarized below.

-- ***Analytical products associated with CI collections are:***

Collection Support Brief. Provides near-comprehensive background detail on a collection issue to guide and enhance collection efforts. (DoDI 5240.18, 17 Nov 2009)

Collection Source Evaluation. An evaluation of a source to determine if the information provided is valuable and credible and to ascertain the reliability and veracity of the source. (DoDI 5240.18, 17 Nov 2009)

Collection Emphasis. Supplements a standing collection requirement and identifies areas of emphasis or information gaps to the CI collector. (DoDI 5240.18, 17 Nov 2009)

Source-Directed Requirement. Established by a CI analysts based on knowledge of a source's access and placement to necessary information. (DoDI 5240.18, 17 Nov 2009)

IIR Evaluation. An analyst's evaluation of how well an IIR satisfied the intelligence requirement for which it was collected. (DoDI 5240.18, 17 Nov 2009)

-- Analytical products associated with CI investigations are:

Investigative Analysis Report. An evaluation of all available information obtained during a CI inquiry to determine if an investigation is warranted; an evaluation of an on-going CI investigation to develop leads, identify trends, patterns, or anomalies in furtherance of the investigative effort; or produced at the conclusion of a CI investigation to identify previously unknown methods of operation, describe lessons learned, and to support damage assessments when initiated. (DoDI 5240.18, 17 Nov 2009)

Investigative Source Evaluation. An evaluation of a source to determine if the information provided is valuable and credible, and to ascertain the reliability and veracity of the source. (DoDI 5240.18, 17 Nov 2009)

Investigative Support Package. An evaluation of all available information pertaining to an unknown subject CI inquiry or investigation in an effort to identify a person, place, or thing of CI interest based on analysis of the information. (DoDI 5240.18, 17 Nov 2009)

-- Analytical products associated with CI operations are:

Operational Analysis Report. An evaluation of information from a variety of sources to determine if favorable conditions are present for initiation of a CI operation and the report may offer suggestions as to the type of asset and/or the access and placement required to meet the foreign essential elements of information requirements. (DoDI 5240.18, 17 Nov 2009)

Operational Asset Evaluation. Evaluates an asset's reliability and veracity in a CI operation. (DoDI 5240.18, 17 Nov 2009)

Operational Support Package. Comprehensive analysis of all available intelligence on a target of interest to a Defense CI Component or determined to be of interest to DoD CI. It details the significance of the target, relates it to strategic objectives, identifies desired effects, and suggests methods of engagement to achieve desired results. (DoDI 5240.18, 17 Nov 2009)

Counterintelligence Assessment. A document produced by a CI analysis and production element stating the in-depth and comprehensive results of analysis regarding a relevant CI topic, event, situation, or development, and contains the characteristics outlined in [DoDI 5140.18] Appendix 2 to Enclosure 3. (DoDI 5140.18, CI Analysis & Production, 17 Nov 2009)

-- Also, an analysis of the actual or potential foreign intelligence and international terrorist threat to DoD, with the objective of protecting personnel, plans, information. Research and technology, critical infrastructure, and other national security interests. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, a DoD Component's comprehensive analysis or study of a relevant CI topic, event, situation, issue, or development. When conducted in support of an RDA program with CPI [Critical Program Information], the assessment describes the threat a foreign entity (person, representative, corporation, government, military, commercial, etc.) represents to the CPI/system assessed. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008, w/ change 1 dated 28 Dec 2010)

> The CI assessment is multidisciplinary as it includes an analysis of the diverse foreign collection modalities available, the relative effectiveness of each, and capability of the foreign entity to collect information about research efforts, the technology, and/or system under development. The assessment may include the impact to the DoD if the technology is compromised and be complimentary to, integrated with, or independent of the TTRA provided by the Defense Intelligence Community.
>
> -- DoDI 5200.39, *CPI Protection within DoD*, 16 Jul 2008, w/ chg 1 dated 28 Dec 2010

Counterintelligence Awareness. An individual's level of comprehension as to the FIE [foreign intelligence entity] threat, methods, indicators, and reporting requirements. (DoDD 5240.06, CIAR, 17 May 2011 with change 1 dated 30 May 2013)

-- Also, a state of being aware of the sensitivity of classified information one possesses, collaterally aware of the many modes of operation of hostile intelligence persons and others whose interests are inimical to the United States while being able to recognize attempts to compromise one's information, and the actions one should take, when one suspects he has been approached, to impart the necessary facts to trained counterintelligence personnel. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

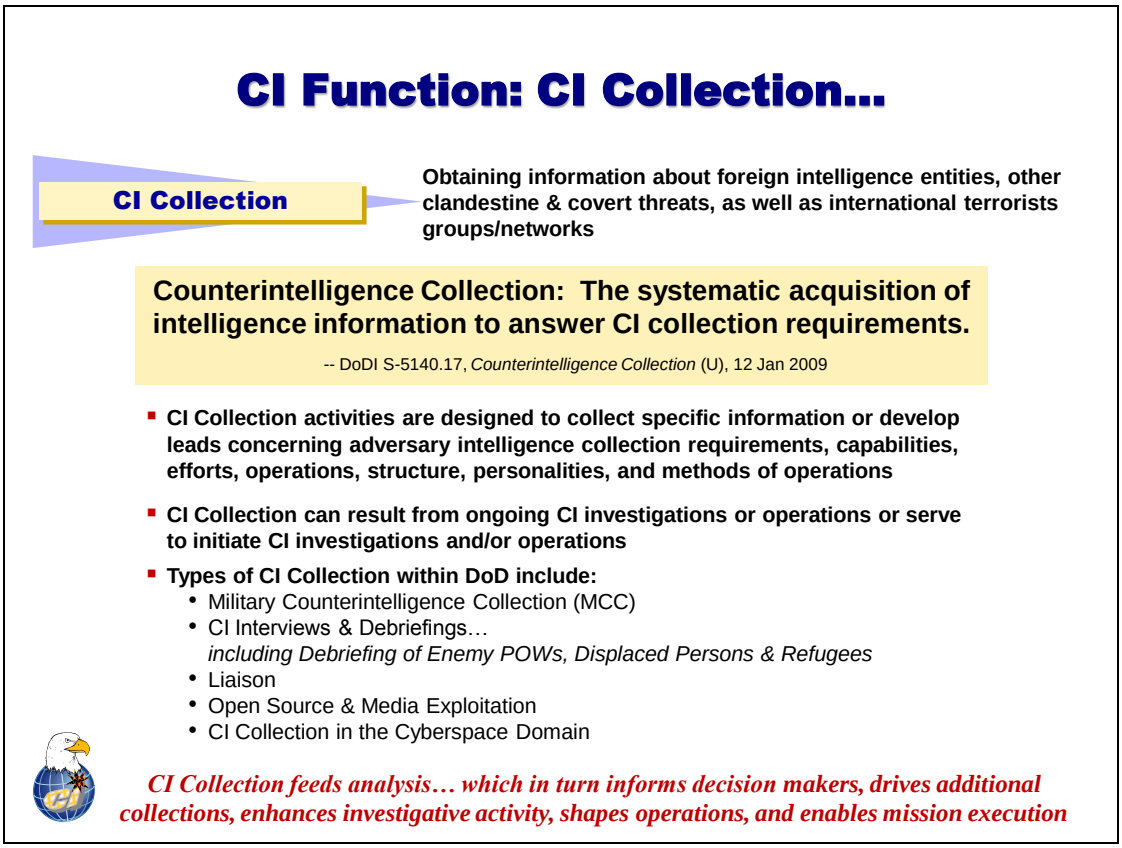
Counterintelligence Awareness Products. A DoD Component's analysis of a CI topic, event, situation, issue, or development. These products differ from an assessment in that they are often time sensitive, are published as needed or annually, and normally do not require extensive research to produce. Products of this nature ensure a consistent flow of appropriately classified or categorized threat information is available to the community to increase awareness and action as appropriate. The Defense Security Service *"Technology Collection Trends in Defense Industry"* and the Office of the National Counterintelligence Executive *"Annual Report to Congress on Foreign Economic Espionage"* are examples of products meeting this objective. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008, w/ chg 1 dated 28 Dec 2010)

Counterintelligence Campaign (CI Campaign). See *DoD Counterintelligence Campaign*.

Counterintelligence Collection. The systematic acquisition of intelligence information to answer CI collection requirements. (DoDI S-5140.17, CI Collection Activities, 14 Mar 2014) Also see *Counterintelligence Collection Activities*; *Military Counterintelligence Collection*.

> See "Counterintelligence Collection Methods" addressed in Appendix C, Joint Publication 2-01.2, *Counterintelligence and Human Intelligence in Joint Operations (U),* 16 Mar 2011 w/ chg 1 dated 26 Aug 2011.
>
> Director DIA is the Defense CI Collection Manager.

-- Also, the systematic acquisition of information (through investigations, operations, or liaison) concerning espionage, sabotage, terrorism, other intelligence activities or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons that are directed against or threaten Department of Defense interests. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations (U),16 Mar 2011 w/ chg 1 dated 26 Aug 2011)



See DoDI S-5240.17, (U) *CI Collection Activities,* 14 Mar 2014 for DoD policy and additional information.

Counterintelligence Collection Activities (CCA): CI collection activities to include military CI collection, CI questioning of EPWs and detainees, CI debriefings, liaison, open source and media exploitation, and CI collection in cyberspace. (DoDI S-5140.17, CI Collection Activities, 14 Mar 2014) Also see *Counterintelligence Collection; Military Counterintelligence Collection*.

Counterintelligence Collection in Cyberspace. The use of cyber means as the primary tradecraft methodology to engage in targeting and collecting cyber based FIE [Foreign Intelligence Entity] activities. CI Collection in cyberspace may include the use of authorized non-attributable Internet connections, development and use of national cyber personas, use of authorized obfuscation techniques, as well as appropriate digital tradecraft and cover. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010 with change 1 dated 16 Oct 2013)

Counterintelligence Collection Operations. Intelligence collection operations that use human sources and CI resources to answer validated CI requirements. CI collection operations are deliberate, planned activities primarily using human sources to satisfy one or more validated CI information requirements. (DoD CI Collection Integrated Working Group Handbook 1-02, 8 Aug 2006)

Counterintelligence Controlled Source Operation (CI CSO). A type of offensive counterintelligence operation (OFCO); see DoDI S-5240.09, OFCO, 29 Oct 2008 for detailed information.

Counterintelligence Coordinating Authority (CICA). A designated CI representative in country, the CICA coordinates, deconflicts, and/or synchronizes all joint CI issues in the country with the Service CI elements assigned to or operating within that country, and with the US embassy or consulate. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *Command Counterintelligence Coordinating Authority (CCICA).*

Counterintelligence Cyber Investigation. An investigation using techniques that identify and interdict the misuse of DoD information systems by a trusted insider or an external intruder. These investigations may involve computer intrusions, exceeding authorized network access, denial of service attacks, or the introduction of a virus or a malicious code. (Previously defined in DoDI 5240.19, CI Support to the Defense Critical Infrastructure Program, 27 Aug 2007 with change 1 dated 28 Dec 2010)

Counterintelligence Effects-Based Operations (CI EBO). As applied to counterintelligence, effects-based operations is a process for obtaining a desired strategic outcome of effect on adversary intelligence activities through the synergistic, multiplicative, and cumulative application of the full range of CI capabilities at the tactical, operational and strategic levels, to include leveraging non-CI capabilities. Successful CI effects-based operations rest on an explicit linking of CI actions to desired strategic outcomes. CI effects-based operations proactively shape the battlespace in our war against adversary intelligence activities and terrorist networks through the robust execution of *full-spectrum* CI capabilities across the entire spectrum of conflict in an orchestrated and synchronized manner to achieve national, departmental, and combatant commander objectives. (COL Mark L. Reagan, USA Ret)

Counterintelligence Enhancement Act of 2002. The act facilitates enhancement of US counterintelligence activities by: (1) enabling the counterintelligence community of the US Government to fulfill better its mission of identifying, assessing, prioritizing, and countering the intelligence threats to the United States; (2) ensuring that the counterintelligence community of the US Government acts in an efficient and effective manner; and (3) providing for the integration of all the US CI activities. The act also established the National Counterintelligence Executive (NCIX), the National CI Policy Board and the Office of the National CI Executive (ONCIX) which replaced the National Counterintelligence Center (NACIC). (§§ 901-904 PL 107-306)

> The act is available at <http://www.ncix.gov/publications/law/index.html>

Counterintelligence Equity. Facts or circumstances connecting an incident, event, or person to an actual or potential intelligence or terrorist threat to Army or DoD personnel, programs, plans, operations, installations, systems, technology, or security. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence Flags. Indicators that should alert a source handler to suspicious action that may bring the source's bona fides into question. (DoDI S-3325.07, Guidance for the Conduct of DoD Human Source Validation (U), 22 Jun 2009.)

> "CI Flags" are different from reportable CI indicators and behaviors as addressed in DoD Directive 5240.06,CI Awareness and Reporting (CAIR, 17 May 2011 w/ chg 1 dated 30 May 2013; see *potential espionage indicators*.

Counterintelligence Force Protection Detachment. See Force Protection Detachment (FPD).

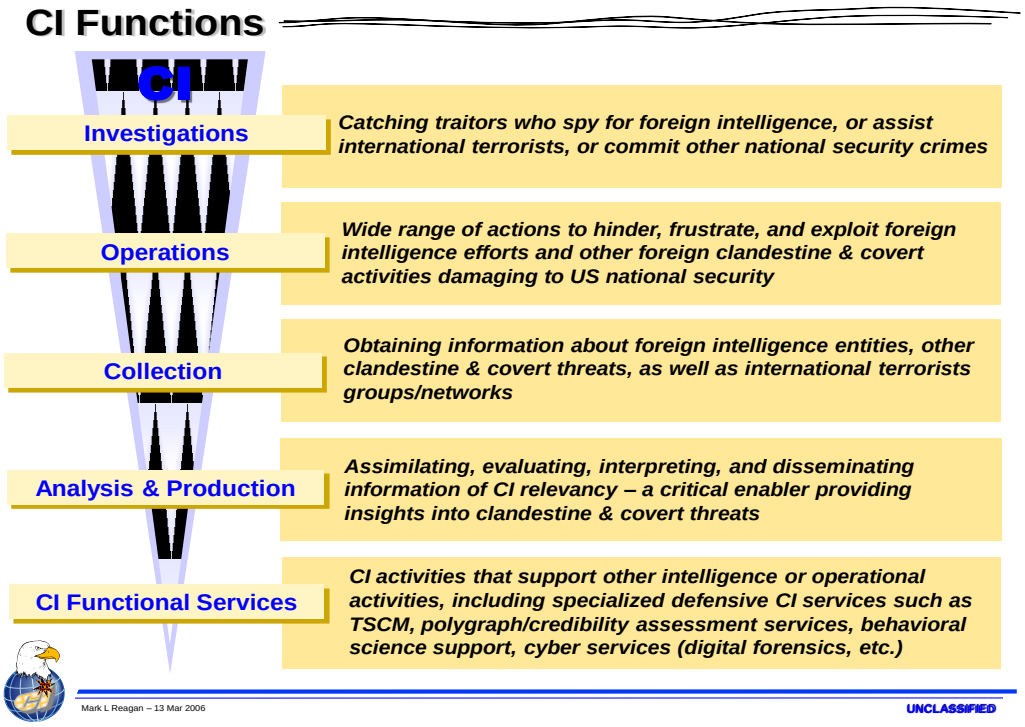
Counterintelligence Force Protection Source Operations (CFSO). Overt source collection activities of an expedient nature intended to identify threats to the command in support of the commander's force protection mission. (Marine Corps Doctrinal Publication 2-6 [previously 2-14], Counterintelligence, 5 Sep 2000, p. 2-3)

Counterintelligence Functions. The five functions of counterintelligence: operations, investigations, collection, analysis & production, and functional services. (JP 1-02) Also see *CI Activities.*

CI functions are interrelated, mutually supporting, and can be derived from one another.

Functions vs. Missions: *"Functions differ from CI missions in that missions focus on end results to be accomplished, rather than on the means for accomplishment. "*
-- Mission Area Analysis of DoD Counterintelligence, Institute for Defense Analyses, May 1999, p.7

CI functions are useful terms of reference to describe "what is done"
CI missions focus on the "end result" to be accomplished



Counterintelligence Functional Services (CIFS). CI activities that support other intelligence or DoD operations by providing specialized defensive CI services to identify and counter the intelligence capabilities and activities of terrorists, foreign powers, and other entities directed against US national security. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007 with change 1 dated 30 Dec 2010)

-- Also, activities engaged in by personnel trained in CI and conducted to detect espionage, sabotage, terrorism, or related intelligence activities of an FIE directed against the DoD, and that enable one or more of the CI functions (investigations, collection, operations, or analysis and production). (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

-- Also, CI activities that support other intelligence or DoD operational activities, providing specialized defensive CI services to identify and counter terrorism, espionage, sabotage, and related activities of Foreign Intelligence Entities. (JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

For DoD Policy see DoD Instruction, *Counterintelligence Functional Services (CIFS),* 27 Aug 2012.

For more in-depth information regarding CI functional services see Department of Defense, CI Functional Services Integrated Working Group Handbook, *Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Functional Services*, 19 Feb 2009. This handbook further defines CI functional services as: those activities that are not unique to other CI functions and that support other CI functions and missions; specialized services, which are not inherently CI but support the CI mission and functions.

Within DoD, CI functional services consist of basic CI activities (including espionage detection and CI support to military operations) and specialized services (e.g., polygraph/credibility assessments, TSCM, behavioral science support, cyber services).

Counterintelligence Functional Support Plan (CI FSP). Director Defense CI and HUMINT Center is responsible for preparation of CI FSPs as part of the Intelligence Planning process (CJCSM 3314.01). Format for CI FSPS is provided at enclosure E to CJCSM 3314.01, Intelligence Planning, 28 Feb 2008.

Counterintelligence Inquiry. An examination of the facts surrounding an incident of potential CI interest, to determine if a CI investigation is necessary. (DoDD 5240.02, CI, 20 Dec 2007 with change 1 dated 30 Dec 2010) Also see *counterintelligence investigation*.

For information regarding CI inquiries within DoD see: 1) DoDI O-5240.21, CI Inquires, 14 May 2009, which provides DoD policy and outlines the procedures for initiating and conducting CI Inquires; and 2) DoD, CI Functional Services Integrated Working Group Handbook, *Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Functional Services (U)*, 19 Feb 2009.

According to the DoD handbook on CI functional services, *"[w]ithin DoD a CI inquiry does not require "investigative authority" as it is not a CI investigation."* A **CI inquiry** is designed to gather information, identify and/or verify the credibility of potential sources and subjects(s) of CI interest, and to recommend appropriate action if the inquiry does not resolve the matter. The goal is to establish or refute a **reasonable belief** that a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged is spying, or committing espionage, sabotage, or other national security crimes (e.g., treason), or international terrorist activities. Establishment of *reasonable belief* provides the basis for opening a CI investigation. Once a *reasonable belief* is established the matter must be referred to the appropriate Military Department CI organization and/or the FBI [see Section 811 referral]. Refer to the definition of *reasonable belief*.

The DoD handbook stresses that *"[w]ithin DoD, only Military Department CI organizations have CI investigative authority and may, accordingly, use the intrusive techniques provided for in Procedures 5 through 13 of DoD 5240.1-R…. It is absolutely vital that CI personnel obtain guidance from their own organization's legal counsel as to what specific investigative techniques and activities are allowable in their organization and approval from their organization's leadership to employ those techniques in the course of CI activity."*

A CI Inquiry is not a CI investigation, but it can provide the basis for a CI investigation.

Counterintelligence Insider Threat (CI InT). A person who uses their authorized access to DoD facilities, systems, equipment, information or infrastructure to damage, disrupt operations, compromise DoD information or commit espionage on behalf of an FIE [Foreign Intelligence Entity]. (DoDD 5240.06, CIAR, 17 May 2011 with change 1 dated 30 May 2013)

-- Also, a person, known or suspected, who uses their authorized access to DoD facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise DoD information, or commit espionage on behalf of an FIE [foreign intelligence entity]. (DoDI 5240.26, Countering Espionage, International Terrorism, and Counterintelligence Insider Threat, 4 May 2012 with change 1 dated 15 Oct 2013) Also see *insider, insider threat*.

CI is one critical component in countering "insider threats," the other components are security, information assurance (IA), law enforcement, and antiterrorism/force protection.

CI Insider Threat Program Elements:
-- CI Analysis of Information Technology Auditing & Monitoring
-- CI Insider Threat Awareness & Training
-- Foreign Travel and Contact Reporting and Analysis
-- Polygraph & Credibility Assessment
-- Personnel Security, Evaluation, Analysis, and Reporting
-- Security Incident Reporting & Evaluation
-- Proactive CI Initiatives

For additional information see DoDI 5240.26, *Countering Espionage, International Terrorism, and Counterintelligence Insider Threat*, 4 May 2012

Insider threat detection should be a comprehensive US Government (USG) effort dedicated to countering potential threats and mitigating damage that could result from unauthorized disclosure of information, espionage, terrorism, and other national security crimes.
-- U.S. Government Threat Detection Guide - 2011

Counterintelligence Investigation. Formal investigative activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in spying or committing espionage, sabotage, treason, sedition, subversion, assassinations, or international terrorist activities, and to determine actions required to neutralize such acts. (DoDI 5240.04, CI Investigations, 4 Feb 2009 with change 1 dated 15 Oct 2013) Also see *counterintelligence inquiry, investigation.*

CI Function: *CI Investigations…*

By far the hardest part of any CI case is to realize that the case exists—that some person, some thing, has the enemy's hidden hand in it.
-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), p. 326

CI investigations are undertaken to determine whether a particular person is acting for or on behalf of a foreign power or international terrorist organization or whether an event is related to foreign intelligence or international terrorism.

CI investigations focus on resolving allegations of known or suspected acts that may constitute national security crimes under U.S. law or Uniform Code of Military Justice.

The agencies responsible for the investigation and ultimate referral for prosecution of violations of US espionage law (primarily Sections 792-798, Chap 37 of Title 18) are the FBI and the CI components of the military services that participate in the DoD Foreign CI Program (FCIP).

DoD Policy: ***The Secretaries of the Military Departments exercise authority, direction, and control over CI investigations and attendant matters for their respective personnel.***

-- Para 5.10.3, DoDD O-5240.02, Counterintelligence, 20 Dec 2007 w/ chg 1 dated 30 Dec 2010

CI investigations are conducted following appropriate legal standards and in a manner which will not jeopardize the potential for prosecution.

Within DoD, DIA's Office of Counterintelligence (DXC) exercises administrative and management oversight of all DoD national security investigations. All significant CI activities must be reported promptly to the DXC IAW DoDD O-5240.02 (see encl 4 for significant CI reporting criteria).

-- Also, inquiries and other activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power for espionage, treason, spying, sedition, subversion, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007 with change 1 dated 30 Dec 2010)

-- Also, includes inquiries and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign power for the purposes of conducting espionage and other intelligence activities, sabotage, assassinations, treason, international terrorist activities, and actions to neutralize such acts. (DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,* 7 Dec 1982)

-- Also, an official, systematic search for facts to determine whether a person(s) is engaged in activities that may be injurious to U.S. national security or advantageous to a foreign power. (JP 1-02 and JP 2.01.2, CI & HUMINT in Joint Operations,11 Mar 2011 w/ chg 1, dated 26 Aug 2011)

-- Also, the systematic collection of information regarding a person or group which is, or may be, engaged in espionage or other clandestine intelligence activity, sabotage, or international terrorist activities conducted for, or on behalf of, foreign powers, organizations, or persons. (CI Community Lexicon)

The first priority for all CI investigative situations is to assess for possible exploitation.

-- Army FM 2-22.2, *Counterintelligence*, October 2009

CI investigations focus on resolving allegations of known or suspected acts that may constitute national security crimes under U.S. law or Uniform Code of Military Justice (UCMJ). Investigative actions must preserve the potential for legal action and when appropriate exploit threatening intelligence collection directed against DoD. In simple terms, CI investigations seek to *identify spies and put them out of business.* CI investigations are about discovering the facts and conveying them to decision makers, while maintaining a full range of options, including apprehension, prosecution, expulsion, as well as exploitation.

"*The ultimate objective of… [DoD] CI investigations… is to detect, identify, exploit and neutralize the intelligence collection threat posed by foreign intelligence and security services and foreign terrorist groups. […] The most significant objectives of CI investigations are to minimize or prevent the loss of sensitive and classified defense information to foreign governments, and to prevent, preempt, or disrupt foreign terrorist attacks against… DoD interests"*

-- 902d MI Group Investigations Handbook, Jun 2012, p.19

"*CI investigation is an art form carried out by experts. It is not science, and throwing money and unqualified personnel or helpers at such s problem does not guarantee or even improve the chances of success. In many cases, quite the opposite results is achieved—analytical chaos with no resolution."*

-- Sandra Grimes and Jeanne Vertefeuille, *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed*, 2012, p. 189

Credentialed CI Special Agents use specialized investigative techniques and methodologies to gather intelligence (facts/evidence) about known and/or suspected acts that may constitute National Security crimes, e.g., espionage, treason, spying, etc. All investigative activities are conducted within guidelines established in applicable departmental policy/directives, Attorney General Guidelines, and U.S. federal statutes.

DoD CI investigations are conducted in a manner to "preserve" the potential for prosecution of all culpable parties identified. Although all national security investigations are conducted in a manner to preserve the potential for prosecution, this purpose is secondary to the CI mission of detecting, identifying, fully determining the extent of, and neutralizing/disrupting national security threats to the DoD and U.S. national security.

CI investigative results also contribute to the identification and elimination of security vulnerabilities; identification of current foreign intelligence tradecraft, agent handlers/operatives and their support networks; assessment of damage to DoD and National Security; and improvement of the overall DoD security posture, as well as assisting decision makers in risk management decisions.

DoD CI investigations are conducted in accordance with DoDI 5240.04, *CI Investigations*. The DoD agencies responsible for CI investigations and the ultimate referral for prosecution of violations of US espionage law (primarily §§ 792-798, Chap 37, Title 18 USC) are the CI components of the military departments, i.e., NCIS, AFOSI, and Army CI.

See Stuart A. Herrington, *Traitors among Us: Inside the Spy Catcher's World* (1999), for an excellent unclassified overview of two CI investigations concerning Clyde Conrad and James Hall.

Other interesting reads on CI investigative cases include –

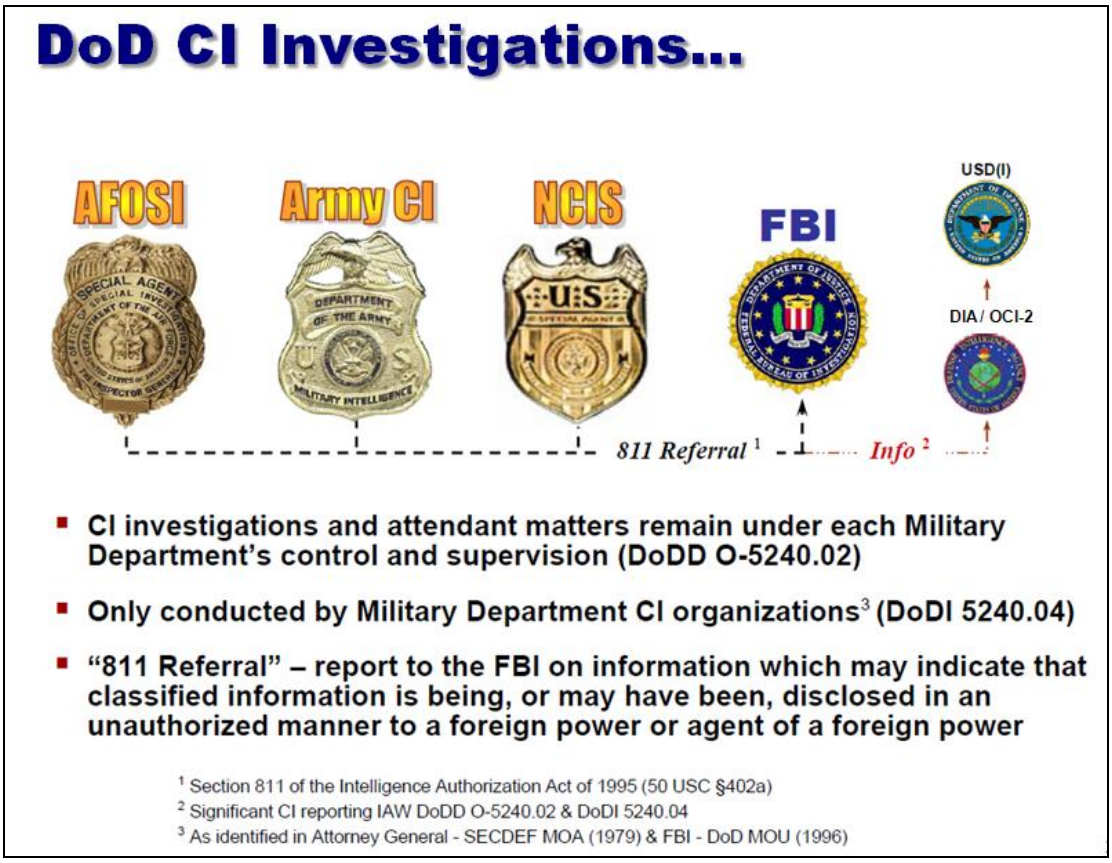
-- Scott W. Carmichael, *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy* (2007)

-- Sandra Grimes and Jeanne Vertefeuille, *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed* (2012).

Spy catching… the surgery of counterintelligence

The thankless and exhausting task of tracking down
a traitor always seems much easier in retrospect than in prospect.
The clues always seem so obvious—but only after the hunt has caught its prey.

-- Markus Wolf, Former Director HVA, East German Intelligence Service (1958-1987)



Counterintelligence Investigative Source Operation. See *Investigative Source Operation (ISO).*

Counterintelligence Mission. Exploit and defeat adversarial intelligence activities directed against US interests; protect the integrity of the US intelligence system; provide incisive, actionable intelligence to decision makers at all levels; protect vital national assets from adversarial intelligence activities; and neutralize and exploit adversarial intelligence activities targeting the armed forces. (ONCIX website: <http://www.ncix.gov/about/mission.html>)

Counterintelligence Missions. DoD CI responsibilities to support force protection; research, development, and acquisition; defense critical infrastructure; and countering espionage. (DoDD 5240.16, DoD CI Functional Services, 27 Aug 2012 with change 1 dated 15 Oct 2013)

CI Missions *vs.* CI Functions

"Functions differ from CI missions in that missions focus on end results to be accomplished, rather than on the means for accomplishment."
-- *Mission Area Analysis of DoD Counterintelligence*, Institute for Defense Analyses, May 1999, p.7

Missions focus on the "end result" to be accomplished
Functions are useful terms of reference to describe "what is done"

DoD Counterintelligence Missions

+ Countering Espionage
+ Counterintelligence Support to Force Protection (FP)
+ Counterintelligence Support to Research, Development, and Acquisition (RDA)
+ Counterintelligence Support to Defense Critical Infrastructure (DCI)

Note: The Army identified four primary CI mission areas in FM 2-22.2 as:
+ Counterespionage
+ CI Support to Force Protection
+ CI Support to Research, Development, and Acquisition
+ Cyber CI

See Army FM 2-22.2, *Counterintelligence*, Oct 2009 and ADRP 2-0, *Intelligence*, Aug 2012

Counterintelligence Mission Manager. The National Counterintelligence Executive (NCIX) serves as the Mission Manager for Counterintelligence IAW Intelligence Community Directive (ICD) 900. Also see *mission managers.*

Counterintelligence Mission Tasking Authority (CI MTA). The authority to task a Military Service CI organizations' headquarters or a Defense Agency's organic CI element to execute a specific CI mission or conduct a CI function within that organization's CI charter. (DoDD O-5240.02, CI, 20 Dec 2007)

Director, Defense CI & HUMINT Center, exercises CI MTA to ensure the effective integration and synchronization of the DoD CI community (para 5.2.3, DoDD O-5240.02).

Counterintelligence Operational Concept/Proposal. The document used to propose an offensive counterintelligence operation (OFCO) which serves as the basis for the planning, review, and approval process. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence Operational Leads (CIOLs). Interagency CI referrals from CIA operations; generally produced and disseminated by the Counterespionage Group (CEG), Counterintelligence Center (CIC) at CIA headquarters. (902d MI Group Investigative Handbook, Jun 2012 2007, p.62)

Counterintelligence Operational Tasking Authority (CIOTA). The levying of CI requirements specific to joint military activities and operations. Counterintelligence operational tasking authority is exercised through supporting components. (JP 1-02)

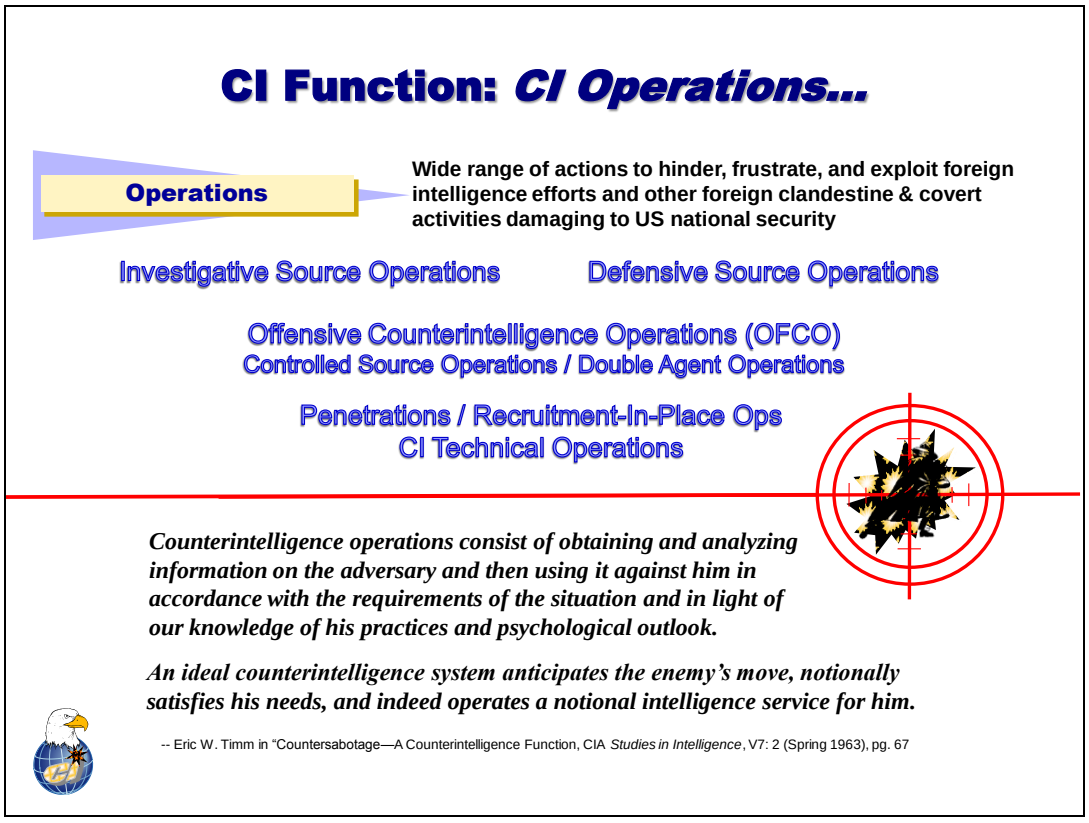
Term previously in DoDI 5240.10, dated 14 May 2004 and JP 2-01.2, dated 13 Jun 2006.

Counterintelligence Operations. Proactive activities designed to identify, exploit, neutralize, or deter foreign intelligence collection and terrorist activities directed against the United States. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *Offensive Counterintelligence Operation (OFCO); recruitment-in-place (RIP); penetration; penetration operation.*

-- Also, operations/efforts intended to negate, confuse, deceive, subvert, monitor, or control the clandestine collection operations of foreign governments or agencies. (CI Community Lexicon)

"While much of the daily work of counterintelligence is laborious and humdrum, its complex and subtle operations are very much like a giant chess game that uses the whole world as its board."

-- Allen Dulles, Former DCI
The Craft of Intelligence (1963)



Counterintelligence Operations—one of five CI functions—are conducted to:
-- manipulate, disrupt, neutralize and or destroy the effectiveness of foreign intelligence activities;
-- recruit or induce defection of foreign intelligence officers and personnel;
-- collect threat information on foreign intelligence operations, modus operandi, intelligence requirements, targeting, objectives, personalities, communications, capabilities, limitations, and vulnerabilities;
-- provide information and operations databases to support decision makers;
-- provide CI support to clandestine human intelligence operations;
-- identify past, ongoing or planned espionage;
-- support force protection, operations other than war and peacekeeping;
-- acquire foreign intelligence espionage equipment for analysis and countermeasures development;
-- develop operational data, threat data and espionage leads for future CI operations, investigations, and projects and develop the potential of these leads to enhance DoD security overall; and
-- support specific [Service], Chairman Joint Chiefs of Staff, DoD and national plans.

Source: JP 1-02 and SEVNAVINST 3850.2C, *Department of Navy Counterintelligence*, 20 Jul 2005

Counterintelligence Production. The process of analyzing all-source information concerning espionage or other multidiscipline intelligence collection threats, sabotage, terrorism, and other related threats to US military commanders, the DoD, and the US Intelligence Community and developing it into a final product that is disseminated. Counterintelligence production is used in formulating security policy, plans, and operations. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the creation of finished intelligence products incorporating CI analysis in to known or anticipated CI concerns. (DoDD 5240.02, CI, 20 Dec 2007 with change 1 dated 30 Dec 2010)

-- Also, the creation of finished intelligence products incorporating CI analysis in response to known or anticipated customer CI concerns. (JP 2.01.2, CI & HUMINT in Joint Operations, 11 Mar 2011)

-- Also, the conversion of analyzed CI information into intelligence products in support of known or anticipated user requirements. (DIA Instruction 5240.002, DIA CI Activities, 15 Jun 2005)

Counterintelligence Programs. Capabilities and activities established within an organization for the purposes of identifying, deceiving, exploiting, disrupting, or protecting against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of FIEs [Foreign Intelligence Entities]. (ICD 750, Counterintelligence Programs, 5 Jul 2013)

Counterintelligence Recruitment Lead (CIRL). An individual being assessed for possible use in a counterintelligence operation, investigation, or project as a controlled source. (AR 381-47, Offensive Counterintelligence Operations, 17 Mar 2006)

Counterintelligence-scope Polygraph (CSP). A screening polygraph examination that uses relevant questions limited to prescribed CI issues. (DoDI 5210.91, PCA Procedures, 12 Aug 2010 with change 1 dated 15 Oct 2013)

Counterintelligence Screening. A systematic process for obtaining information of CI interest from a specific person or target audience. (FM 2-22.2, Counterintelligence, Oct 2009)

> CI screening normally is non-confrontational – ***it is NOT an interrogation***. See Chapter 4, *CI Collection Program* of FM 2-22.2, Counterintelligence, Oct 2009 (page 4-5 through 4-7).
>
> CI screening should not use any of the "interrogation methods" defined in FM 2-22.3, *Human Intelligence Collector Operations*.

Counterintelligence Special Agent. Within DoD, US Government personnel (military and civilian employees) who have successfully completed an approved Counterintelligence Special Agent course of instruction, who are authorized to be issued CI Badge and Credentials (B&Cs), and who are assigned to conduct CI investigations and/or operations. .

> Within the US Army: military personnel holding the military occupational specialty (MOS) 35L, 351L, or 35E as a primary or additional specialty, and selective civilian employees in the GS-0132 career field; see AR 381-20, Army CI Program (U).

Counterintelligence Special Operations Concept (CISOC). The document used to propose a defensive counterintelligence operation, special investigative activity. Or counterintelligence source operation which serves as the basis for the planning, review, and approval process. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence Staff Officer (CISO). This term replaced by "*Command CI Coordinating Authority*" or CCICA; see DoDI 5240.10, CI in the Combatant Commands and Other DoD Components, 5 Oct 2011.

Counterintelligence Support. Conducting counterintelligence activities to protect against espionage and other foreign intelligence activities, sabotage, international terrorist activities, or assassinations conducted for or on behalf of foreign powers, organizations, or persons. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *counterintelligence*.

-- Also, the application of knowledge regarding the foreign intelligence and international terrorist threat to assist commanders, program managers, and agency heads to identify the insider threat and to protect information or technology vital to the national defense, including the force, technology, critical infrastructure, and information systems. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence Support Plan (CISP). A formal and living plan describing activities conducted by a Defense CI Component in support of a DoD RDA [Research, Development and Acquisition] program or activity with CPI [critical program information], at DoD-affiliated RDT&E facilities, and at essential CDCs [cleared defense contractor] where CPI resides. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

-- Also, a formal plan that outlines and describes the CI support to be provided to research and development facilities, RDA [Research, Development and Acquisition] programs with CPI [critical program information], and CPI resident at cleared Defense contractor facilities. CISPs are coordinated with and approved by the RDA Director, Program Executive Office, or Program Manager, as appropriate, and are an appendix to the PPP. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008, with change 1 dated 28 Dec 2010)

Defense CI Components use a CISP to integrate CI activities into RDA, manage, and document non-investigative or non-operational activities conducted. See Appendix 2 to Encl 3 of DoD Instruction O-5240.24, *CI Activities Supporting RDA*, 8 June 2001 (pp. 22-23) for specifics to include elements of a CISP.

Note: A CISP takes precedence over a *DCIP CI Coverage Plan* at supported locations where a CISP is required in accordance with DoD Instruction 5240.24, *Counterintelligence Activities Supporting RDA*.

Counterintelligence Support to HUMINT. [CI activities which] prevents the detection, neutralization or manipulation of strategic U.S. DoD HUMINT collection activities by foreign intelligence or security servives. (DIA Instruction 5240.002, *DIA Counterintelligence Activities*, 15 Jun 2005)

For additional information see Appendix D, *Counterintelligence Support to Human Intelligence (U),* JP 2-01.2, *CI & HUMINT in Joint Operations (U),* 16 Mar 2011 with chg 1 dated 26 Aug 2011

Counterintelligence Targets. CI targets include personalities, organizations, and installations (PO&I) of intelligence or CI interest, which must be seized, exploited, neutralized or protected. Also see Black List, Gray List, White List. (USMC, MCWP 2-6 [previously 2-14], Counterintelligence, 5 Sep 2000)

Counterintelligence Technical Services (CITS). Encompasses Technical Surveillance Countermeasures (TSCM) and Technical Support to Counterintelligence (TSCI). TSCM is used to detect the presence of technical surveillance devices and hazards and to identify technical security vulnerabilities that put the surveyed facility at risk. TSCI provides technical surveillance and countersurveillance in support of CI activities. Also see *Technical Surveillance Countermeasures*.

Counterintelligence Threat (CI Threat). The capability and intent of one entity to detect and counteract another's intelligence activities – the objective is to undermine the effectiveness of opposing intelligence activities.

To date, the term "CI Threat" remains undefined officially by DoD or IC policy. CI threat is often misused when actually referring to the "intelligence collection threat."

The "CI Threat" includes all activities undertaken by an adversary to identify, disrupt, manipulate, exploit, and/or destroy the effectiveness of friendly intelligence operations/activities. Specifically, CI threats are actions one country/entity directs against another's intelligence operations and other clandestine/covert activities. Hence the CI threat to US intelligence is the capability and intent of any entity to detect and counteract U.S. intelligence activities -- separate and distinct from intelligence threats. "CI threats" are not analogous to the threats of interest to counterintelligence.

From the US perspective -- the CI threat is foreign counterintelligence or security services efforts to counter -- detect, disrupt, neutralize, and exploit -- US intelligence activities or other US clandestine/covert activities.

Counterintelligence Training. Institutional training in knowledge, skills, abilities, and core competencies unique to CI missions and functions. (DoDI 3305.11, DoD CI Training, 19 Mar 2007)

-- Also, instructions and applied exercises offered through various media and methods for the acquisition, retention, and enhancement of skills, knowledge, and abilities required to counter or neutralize: intelligence collection efforts; other intelligence activities; sabotage; and terrorist activities and assassination efforts on behalf of foreign powers. (DoDI 3305.12, Intelligence and Counterintelligence Training of Non-US Persons, 25 Oct 2007 w/ chg 2 dated 15 Oct 2013)

Counterproliferation (CP). Those actions (e.g., detect and monitor, prepare to conduct counter-proliferation operations, offensive operations, weapons of mass destruction, active defense, and passive defense) taken to defeat the threat and/or use of weapons of mass destruction against the United States, our military forces, friends, and allies. (JP 1-02 and JP 3-40, Combating WMD, 10 Jun 2009)

-- Also, the activity by United States government intended to prevent the proliferation of nuclear, chemical and biological capabilities to other nations. (HPSCI Report, 27 Jul 2006)

Countermeasure. Anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, action, device, procedure, technique, or other measure that reduces or eliminates one or more vulnerabilities. (DoD Insider Threat IPT Final Report, 24 Apr 2000)

-- Also, [in TEMPEST usage] action, device, procedure, technique, or other measure that reduces the vulnerability of any equipment that electronically processes information (NSTISSI 7002, TEMPEST Glossary, 17 Mar 1995).

Countermeasures. That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 1-02)

-- Also, defensive security programs and activities which seek to protect against both foreign intelligence collection efforts and unauthorized access to, or disclosure of, protected facilities, information, and material. (AR 380-20, Army CI Program, 25 May 2010)

-- Also, the employment of devices and/or techniques that has as its objective the impairment of the operational effectiveness of an adversary's activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities. (DSS Glossary)

-- Also, the employment of devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities. (*Draft* DoDI 5200.39, CPI Identification and Protection within RDA Programs)

-- Also, [in polygraph and credibility assessment usage] those strategies employed by examinees to affect PCA testing by the intentional application of physical, mental, pharmacological, or behavioral tactics. (DoDI 5210.21, PCA Procedures, 12 Aug 2010 w/ chg 1 dated 15 Oct 2013)

Counterproliferation. Those actions taken to defeat the threat and/or use of weapons of mass destruction against the United States, our forces, friends, allies, and partners. (JP 1-02 and JP 3-40, Combating WMD, 10 Jun 2009)

Countersurveillance. All measures, active or passive, taken to counteract hostile surveillance. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010) Also see *counter surveillance; surveillance detection.*

-- Also,…security techniques designed to detect, prevent, or deceive hostile observation of friendly operations or activities. (CI Community Lexicon)

-- Also, the total action taken to detect and frustrate hostile surveillance. (*Encyclopedia of the CIA*, 2003)

-- Also, [Counter Surveillance]. Measures or actions taken when under verified or suspected surveillance. (DoDI S-5240.15, FPRG, 20 Oct 2010 with change 1 dated 16 Oct 2013)

-- Also, the process of detecting and mitigating hostile surveillance (Stratfor - Global Intelligence)

> *An effective CS [countersurveillance] program depends on knowing two "secrets": first, hostile surveillance is vulnerable to detection because those performing it are not always as sophisticated in their tradecraft as commonly perceived; and second, hostile surveillance can be manipulated and the operatives forced into making errors that will reveal their presence.*
>
> *…CS can be performed by a person who is aware of his or her surroundings and who is watching for people who violate the principles of TEDD.* At a more advanced level, the single person can use surveillance detection routes (SDRs) to draw out surveillance.*
>
> ** The U.S. government uses the acronym TEDD to illustrate the principles one can use to identify surveillance. So, a person who sees someone repeatedly over Time, in different Environments and over Distance, or one who displays poor Demeanor can assume he or she is under surveillance. Surveillants who exhibit poor demeanor, meaning they act unnaturally, can look blatantly suspicious, though they also can be lurkers -- those who have no reason for being where they are or for doing what they are doing. Sometimes they exhibit almost imperceptible behaviors that the target senses more than observes. Other giveaways include moving when the target moves, communicating when the target moves, avoiding eye contact with the target, making sudden turns or stops, or even using hand signals to communicate with other members of a surveillance team.*
>
> -- Fred Burton, "The Secrets of Countersurveillance," *Security Weekly*, Stratfor, 6 Jun 20007; article on line at: <http://www.stratfor.com/secrets_countersurveillance>

Counterterrorism (CT). Actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks. (JP 1-02 and JP 3-26, Counterterrorism, 13 Nov 2009) Also see antiterrorism; *terrorism; combating terrorism*.

-- Also, the practices, tactics, techniques, and strategies adopted to prevent or respond to terrorist threats or acts, both real and suspected. (ODNI, U.S. National Intelligence – An Overview 2011)

> Also see *National Strategy for Counterterrorism*, June 2011 at
> < http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf >

Country Clearance. Clearance for official U.S. Government representative travel to a foreign country granted through the cognizant U.S. Embassy or U.S. Mission. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

Country Team. The senior, in-country, US coordinating and supervising body, headed by the chief of the US diplomatic mission, and composed of the senior member of each represented US department or agency, as desired by the chief of the US diplomatic mission. (JP 1-02 and JP 3-07.4, Joint Counterdrug Operations, 13 Jun 2007)

Courier. Person who carries an item or information from one person or place to another. The courier may or may not be aware of the nature of the item or information being transported. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, a messenger responsible for the secure physical transmission and delivery of documents and materials. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Cover. A protective guise used by a person, organization, or installation to conceal true affiliation with clandestine or other sensitive activities. (DoDD S-5105.61, DoD Cover and Cover Support Activities (U), 6 May 2010) Also see *cover for action; cover for status*.

-- Also, the concealment of true identity, purpose, or organizational affiliation with assertions of false information as part of, or in support of, official duties to carry out authorized activities and lawful operations. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

-- Also In intelligence usage, those measures necessary to give protection to a person, plan, operation, formation, or installation from enemy intelligence effort and leakage of information. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, actions to conceal actual friendly intentions, capabilities, operations, and other activities by providing a plausible yet erroneous explanation of the observable. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, a verifiable and documented protective guise used by a person, organization, or installation to conceal true identity or affiliation. (HDI Lexicon, April 2008)

-- Also, a protective guise used by a person, organization, or installation to prevent identification with clandestine activities and to conceal the true affiliation of personnel and the true sponsorship of their activities. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- Also, protective action taken to mask or conceal an operation or activity from an adversary. (DSS Glossary)

-- Also, a protective guise used by an individual, organization, or installation to prevent identification with intelligence activities. To hide, conceal, obscure, or otherwise protect the exact identity of an individual, unit, or activity. Supported with or without documentation and backstopping depending on the sensitivity and scope of the operation. *Cover* can be anything that masks the true nature of an activity. (CI Community Lexicon)

> DoD cover may be used to protect the Department of Defense, its intelligence sources and methods, and its clandestine tactics, techniques, and procedures from exposure to the enemy and overt association with sensitive activities. The fact that DoD uses cover to protect its activities is unclassified.
>
> For DoD policy see DoDD S-5105.61, *DoD Cover and Cover Support Activities (U),* 6 May 2010.

Cover shields secret activities from the opposition

Good cover …*reaches into the mind of the opponent, thinks as he would think, and then creates a combination of fact and fancy, of actual arrangements and contrived impressions, which the opposing mind is prepared to believe…. Cover takes an infinite variety of forms.*

The best cover is that which contains the least notional and the maximum possible legitimate material…. ***Perfect cover is an ideal, rarely achieved in practice.***

-- Christopher Felix (James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

Special Cover Measures…

There are many valid reasons for the special cover measures used by some military and intelligence organizations, such as potentially life-threatening, high-risk, covert operations and intelligence and counterintelligence investigations or operations.

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, p.19

Cover for Action. A logical reason for doing the specific action involved. (CI Community Lexicon)

-- Also, a verifiable and documented protective guise used to disguise the true intent of an individual, organization, or activity and to provide a credible explanation as to participation in a particular activity. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010) Also see *cover for status*.

> *Cover for Action. This cover, combined with the use of appropriate clandestine tradecraft techniques (e.g. alias, disguise, darkness, surveillance detection routes to and from meetings, etc.) is what provides cover and security for clandestine meetings.*
>
> -- F.W. Rustmann, Jr., "Debunking the CIA Case Officer Myth," *Association of Former Intelligence Officers (AFIO) Newsletter* (Fall 2003), <http://ctcintl.com/Debunk.htm>; accessed 7 Mar 2011

Cover for Status. A logical and backstopped reason for being in an area or processing a particular item at a particular time. (CI Community Lexicon) Also see *cover for action*.

-- Also, a verifiable and documented protective guise used to legitimize an individual's, organization's, or activity's extended presence in a particular area. (Defense HUMINT Enterprise Manual 3301.002, Vol II, Collection Operations, 23 Nov 2010)

> *Cover for Status. This is the cover that permits [a case officer] to live and work in a particular country. If the case officer is under official cover, this means he must blend into the environment of an embassy or other official US installation abroad.*
>
> -- F.W. Rustmann, Jr., "Debunking the CIA Case Officer Myth," *Association of Former Intelligence Officers (AFIO) Newsletter* (Fall 2003), <http://ctcintl.com/Debunk.htm>; accessed 7 Mar 2011

Cover Legend. A contrived scenario or story designed to explain an organizational or personal background and past or present activities, in terms intended to protect or conceal involvement in a clandestine or otherwise sensitive activity. It incorporates as much truth as possible. It must be plausible. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

-- Also, a contrived scenario, designed to explain an organizational or personal background and past or present activities, in terms intended to protect and/or conceal involvement in a clandestine or otherwise sensitive activity. It incorporates as much truth as possible. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010) Also see *cover story*.

Cover Mechanism. Any documentary, oral, technical, fiscal, logistical, or other means provided to backstop a cover. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

Cover Stop. A stop made while under surveillance that provides an ostensibly innocent reason for a trip. (CI Centre Glossary and Spy Dust)

Cover Story. Coherent and plausible account of background, residence, employment, activities, access, etc., furnished to an individual to substantiate whatever claims are necessary to successfully carry out an operation. The difference between a cover story and a legend is that a legend is furnished to an illegal or agent by FIS. (AFOSI Manual 71-142, OFCO, 9 Jun 2000) Also see *cover legend*.

-- Also, the background legend you have developed to explain who you are and why you are where you are. (*A Spy's Journey*)

> *The cover story is most frequently used to explain the visible evidences of a clandestine operation or to provide an explanation when an operations encounters difficulties.*
>
> *…cover stories in general: they should not be too precise or too detailed, and they should not be forthcoming too quickly or all at once. …To be too precise in a cover story qualitatively increases the chances of repudiation of the story; to be too detailed increases those chances quantitatively.*
>
> -- Christopher Felix (aka James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

Cover Support Activities. All measures taken to develop, coordinate, approve, activate, operate, and terminate cover. (DoDD S-5105.61, DoD Cover and Cover Support Activities (U), 6 May 2010)

Cover Within Cover. A credible confession to an act that is less serious than espionage and will explain all actions under suspicion by foreign intelligence services. (Words of Intelligence, 2nd Edition, 2011)

Covering Agent. [As used within US Army] a CI Agent who provides dedicated full or part time counterintelligence support, education, and liaison to an organization, agency, or research, development, and acquisition program. (AR 381-20, Army CI Program, 25 May 2010)

Covert. A method of conducting operations that hides the true intent, affiliation or relationship of its participants. Differs from clandestine in that covert conceals the identity of the sponsor, whereas clandestine conceals the identity of the operation. (National HUMINT Glossary) See *clandestine; covert action; covert operation*.

Covert, from the Latin *cooperire*, "to cover," means "concealed, hidden, under cover, not avowed."

Covert and clandestine are not synonymous!

Covert Action. Activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly. Covert action **does not include** activities the primary purpose of which is to acquire intelligence, **traditional counterintelligence activities** [*emphasis added*], traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities. (Section 503e, National Security Act of 1947 [50 USC §413b]) Also see *covert; covert operation; finding; special activities.*

Covert action should not be confused with missionary work.

-- Henry Kissinger
as cited in James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006), p. 33

…the overt foreign activities of the US Government must be supplemented by covert operations

NSC Directive 10/2 (dated 18 Jun 1948)
as cited in Warner, *CIA Under Truman* (1994)

Covert actions are designed to avoid revealing the role of the United States in their planning or execution. EO 12333 (as amended 30 Jul 2008) directs that no agency except CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective.

EO 12333 limits covert action, i.e., "no covert action may be conducted which is intended to influence US political processes, public opinion, policies, or media. " (EO 12333, para 2.13)

Covert action by DoD must be directed by the President, subsequently approved by the Secretary of Defense, and executed in accordance with applicable law.

Evolution of Covert Action

[I]n December 1947, the National Security Council issued a series of classified directives specifying and expanding the CIA's covert mission. The first of these directives, NSC-4-A, authorized the Director of Central Intelligence (DCI) to conduct covert psychological operations consistent with United States policy and in coordination with the Departments of State and Defense. A later directive, NSC 10/2, authorized the CIA to conduct covert political and paramilitary operations. […] The United States should ,maintain the option of reacting in the future to a grave, unforeseen threat to United States national security through covert means.

-- Church Committee – 1976 (Senate Report 94-755, Book I, 26 April 1976)

Covert action must be consistent with and supportive of national policy and must be placed appropriately within a national security policy framework. Covert action must never be used as a substitute for policy.

-- National Security Decision Directive 159, 18 Jan 1985 (originally Top Secret-Sensitive, declassified)

Covert actions are… legally distinct from clandestine missions: 'clandestine' refers to the tactical secrecy of the operation itself, 'covert' refers to the secrecy of the sponsor. ...covert action can include a wide range of activity, from propaganda and disinformation to political influence operations, economic destabilization, and paramilitary operations. Historically, the Central Intelligence Agency (CIA) has been the main agent of US covert action….

-- Jennifer D. Kinne, "Covert Action and the Pentagon," *Intelligence and National Security*, Vol. 22 No. 1, February 2007, pp. 57-58

Covert action, or to use the British term, *special political action*, is the attempt by a government or group to influence events in another state or territory without revealing its own involvement. …Covert action is really an American term-of-art that came into use after World War II.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 2

Typically, covert actions are carried out by the CIA with such assistance as may be necessary by other elements of the intelligence Community as directed by the President. U.S. law requires that all covert actions be approved prior to their execution by the President in a written 'finding' and that notification be provided to the two intelligence committees in Congress. Covert actions may involve political, economic, propaganda, or paramilitary activities.

-- WMD Report, 31 Mar 2005

Covert action is often called the "dirty tricks" side of spying. It consists of sabotage, subversion, paramilitary operations, political action, psychological; operations, and black propaganda. It is not always pretty. Covert action has historically been a relatively small part of the CIA's overall activity, but it is certainly the aspect of U.S. spying that has been the most controversial.

-- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)

The three basic types of covert action are perception management (historically known as propaganda), political action (influencing the actions of a foreign leader or government), and paramilitary operations (support to insurgents).

-- Duane R. Clarridge, *A Spy For All Season: My Life in the CIA* (1997), p. 410

Covert action is not intelligence. Rather, CA is the most sensitive technique for implanting national security policy. Operating in the space between diplomacy and military force, covert actions are the "third way" of accomplishing a nation's goals.

-- Dr. James E. Steiner (retired CIA), "Restoring the Red Line Between Intelligence and Policy on Cover Action," *International Journal of Intelligence and Counterintelligence*, Vol 19 No 1 (Spring 2006), p. 157

Covert action can serve as a more subtle and surgical tool
than forms of acknowledge employment of U.S. power and influence.

-- WMD Report (31 Mar 2005), p. 33

Security is indispensable to the successful conduct of covert action.
…[A]ccess to information on US covert action policies shall be restricted
to the absolute minimum number of persons possible.

-- President Ronald Reagan, NSSD 159 (18 Jan 1985)

Covert Channel. An unauthorized communication path that manipulates a communications medium in an unexpected, unconventional, or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Covert Channel Analysis. Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Covert Communication (COVCOM). Clandestine, hidden communication that protects both the information being shared and the relationship between the sending and receiving parties. (National HUMINT Glossary)

-- Also, any technique or device used to relay data clandestinely from case officer to agent or agent to case officer. (Spycraft)

-- Also, an agent's spy gear for communicating with his case officer. (*A Spy's Journey*)

Covert Operation. An operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. (JP 1-02 and JP 3-05, Special Operations, 18 Apr 2011) Also see *covert; covert action, clandestine operation.*

Covert refers to the secrecy of the sponsor

Clandestine operations are sometimes incorrectly referred to as "covert operations." Although both are secret and sensitive activities, the terms are not interchangeable. See *clandestine operation*.

"*Avowal of a covert operation, however implicit, is a hostile act, and it is wise never to indulge in hostile acts unless one is able and prepared to back them up."*

-- Christopher Felix (aka James McCargar), *A Short Course in the Secret War*, 4th Edition (2001)

A 1948 National Security Council Intelligence Directive defined *covert operations* as actions by the U.S. against foreign states "which are so planned and executed that any U.S. Government responsibility for them is not evident to unauthorized persons and that if uncovered the U.S. Government can plausibly disclaim any responsibility for them."

"Covert action is the term that describes our efforts to influence the course of events in a foreign country without our role being known….[it] has always been assigned to the CIA to perform, by means of unattributable propaganda, sub rosa political action, or secret paramilitary support."

-- Stansfield Turner, Former Director Central Intelligence Agency

CPI. See *Critical Program Information*.

Credentials [Counterintelligence]. An official document or set of documents presenting evidence of the identity, authority, and status of the bearer and for use in conducting authorized CI activities. (DoDI 5240.25, Counterintelligence Badge and Credentials, 30 Mar 2011 with change 1 dated 15 Oct 2013) Also see *badge; special agent*.

-- Also, official documents which identify the bearer as a representative of a specific agency or department of the U.S. Government.

Credible Information. Information disclosed or obtained by a criminal investigator that, considering its source and nature and all the circumstances, is believable enough that a trained criminal investigator can state the information is true. (DoDI 5505.7, Titling & Indexing Subjects of Criminal Investigations in DoD, 27 Jan 2012)

-- Also, information disclosed to or obtained by an investigator that, considering the source and nature of the information and the totality of the circumstances, is sufficiently believable to indicate that criminal activity has occurred and would cause a reasonable investigator under similar circumstances to pursue further the facts of the case to determine whether a criminal act occurred or may have occurred. (AR 195-2, Criminal Investigation Activities, 15 May 2009)

Credibility Assessment. The multi-disciplinary field of existing, as well as potential, techniques and procedures to assess truthfulness that relies on physiological reactions and behavioral measures to test the agreement between an individual's memories and statements. (DoDD 5210.48, Polygraph and Credibility Assessment Program, 25 Jan 2007 with change 2 dated 15 Nov 2013)

Criminal Intelligence (CRIMINT). Law enforcement information derived from the analysis of information collected through investigations, forensics, crime scene and evidentiary processes to establish intent, history, capability, vulnerability, and modus operandi of threat and criminal elements. (DoDI 2000.16, DoD Antiterrorism Standards, 2 Oct 2006)

-- Also, a category of police intelligence derived from the collection, analysis, and interpretation of all available information concerning known and potential criminal threats and vulnerabilities of supported organizations. (ATTP 3-39.20, Police Intelligence Operations, Jul 2010)

-- Also, information compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. (National Criminal Intelligence Sharing Plan, Oct 2003)

For DoD Policy see DoDI 5525.18, Law Enforcement Criminal Intelligence in DoD (Note: does not apply to counterintelligence personnel).

CRIMINT gathering is a fundamental and essential element in the all-encompassing duties of all DoD Law Enforcement Agencies. CRIMINT can aid in crime prevention, threat disruption, offender pursuit and apprehension, and evidence capture necessary for conviction.

Criminal Investigation. Investigation into alleged or apparent violations of law undertaken for purposes which include the collection of evidence in support of potential criminal prosecution. (DoDI 5505.7, Titling & Indexing Subjects of Criminal Investigations in DoD, 27 Jan 2012)

-- Also, the process of searching, collecting, preparing, identifying, and presenting evidence to prove the truth or falsity of an issue of law. (US Army, FM 3-19.13, Law Enforcement Investigations, Jan 2005)

Criminal investigation is both an art and a science.

In science, the absolute truth is often achieved. Experience has shown that in criminal investigations a less decisive hypothesis may sometimes be all that is possible to achieve.

A criminal investigation is the process of searching, collecting, preparing, identifying, and presenting evidence to prove the truth or falsity of an issue of law.

Objectives of Criminal Investigations:
- 1) *Determine if a crime was committed;*
- 2) *Collect information and evidence legally to identify who was responsible;*
- 3) *Apprehend the person responsible;*
- 4) *Recover stolen property;*
- 5) *Present the best possible case to the prosecutor; and*
- 6) *Provide clear, concise testimony.*

-- US Army, FM 3-19.13, *Law Enforcement Investigations*, Jan 2005

A criminal investigation is normally initiated when objective facts and circumstances reasonably indicate a crime has been, is being or will be committed. A criminal investigation is normally limited to: who committed the act; secure evidence to establish the elements of the offense; and support prosecution.

Also see *Crime Scene Investigation: A Guide for Law Enforcement*, Sep 3013; available on line at <http://www.nist.gov/oles/csiguide.cfm>

Criminal Investigative Information. Information compiled in the course of a criminal investigation. (AR 195-2, Criminal Investigation Activities, 15 May 2009)

Criminal Investigation Task Force (CITF). The DoD CITF is a strategic-level organization with a mission to develop and fuse police intelligence with MI [military intelligence] for the purpose of building criminal cases against terrorist criminals that have attacked U.S. interests. (ATTP 3-39.20, Police Intelligence Operations, Jul 2010)

The CITF conducts complicated criminal investigations targeting terrorists and complex criminal organizations. These cases typically cross international borders and involve criminals captured as a result of military operations, requiring coordination with international police and intelligence agencies. The CITF combines USACIDC special agents (and criminal investigators from other Services), police and intelligence analysts, and attorneys into teams. These teams synchronize and fuse information and intelligence from all available sources to conduct criminal investigations that enable criminal prosecution in U.S. or host nation legal systems.

-- ATTP 3-39.20 (FM 3-19.50), Police Intelligence Operations, July 2010

Criminal Offense. Any criminal act or omission as defined and prohibited by the Uniform Code of Military Justice, the United States Code, State and local codes, foreign law, or international law or treaty. As used herein, this term does not include military offenses as defined below. In the case of juveniles, this term refers to those acts which, if committed by an adult, would be subject to criminal sanctions. (AR 195-2, Criminal Investigation Activities, 15 May 2009)

Crisis. An incident or situation involving a threat to the United States, its citizens, military forces, possessions, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of US military forces and resources is contemplated in order to achieve national objectives. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Crisis Action Planning (CAP). The Adaptive Planning and Execution System process involving the time-sensitive development of joint operation plans and operation orders for the deployment, employment, and sustainment of assigned and allocated forces and resources in response to an imminent crisis. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Crisis Management (CrM). Measures, normally executed under federal law, to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or an act of terrorism. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

CRITIC. Critical information messages sent over the CRITICOMM System that must be delivered to the President within 10 minutes upon recognition. (DoDD 5100.20, NSA, 26 Jan 2010)

Critical Asset. A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

-- Also, *Defense Critical Asset*: an asset of such extraordinary importance to DoD operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its mission. (DoDI 2000.16, DoD Antiterrorism Standards, 2 Oct 2006)

-- Also, any asset (person, group, relationship, instrument, installation, process or supply at the disposition of an organization for use in an operational or support role) whose loss or compromise would have a negative impact on the capability of a department or agency to carry out its mission; or may have a negative impact the ability of another U.S. Government department or agency to conduct its mission; or could result in substantial economic loss; or which may have a negative impact on the national security of the U.S. (ICD 750, Counterintelligence Programs, 5 Jul 2013)

Critical Information (also called CRITIC). Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.(JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, decisions, intentions, or actions of foreign governments, organizations, or individuals that could imminently and materially jeopardize vital U.S. policy, economic, informational, or military interests to such an extent that the immediate attention of the President and the National Security Council may be required. (DoDD 5100.20, NSA, 26 Jan 2010)

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a deliberating impact on the security, national economic security, national public health and safety, or any combination of those matters. (Critical Infrastructures Protection Act of 2002 and USA Patriot Act §1016)

-- Physical or virtual systems and assets that if compromised by a physical or cyberspace incident negatively impact the national security, economic stability, public confidence, health, or safety of the United States. (DoD Strategy for Operating in Cyberspace, May 2011)

-- Also, [within DoD] infrastructure deemed essential to DoD operations or the functioning of a critical asset.

Nation's critical infrastructure and key resources, as set forth in the 2006 National Infrastructure Protection Plan (NIPP) includes the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

-- Cited in the *National Strategy for Homeland Security*

Failure of critical assets degrades or disrupts operations; cascading failures of critical infrastructure assets within and across infrastructures may lead to mission failure

-- DoD Critical Infrastructure Protection Strategy, April 2003

Copy of the 2009 *National Infrastructure Protection Plan* (NIPP) at:
<http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>

Critical Infrastructure and Key Resources (CI/KR). The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. (JP 3-27, Homeland Defense, 29 Jul 2013)

Critical Infrastructure Protection (CIP). Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013) Also see *Defense Critical Infrastructure*.

PDD-63 set as a national goal the ability to protect the nation's critical infrastructure from intentional attacks (both physical and cyber). Also see PPD-21, Critical Infrastructure Security and Resilience, 12 Feb 2013. PPD-21 identifies 16 critical infrastructure sectors; DoD is the sector-specific agency for the Defense Industrial Base (DIB).

For DoD policy see DoDD 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*.

Critical Intelligence. Intelligence that is crucial and requires the immediate attention of the commander. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Critical National Asset (CNA). Any information, policies, plans, technologies, or capabilities that, if acquired (stolen), modified, or manipulated by an adversary, would seriously threaten US national or economic security. (NIP - *FY 2009 Congressional Budget Justification Book*, redacted version)*

* Copy available at: <http://www.fas.org/irp/dni/cbjb-2009.pdf> (accessed 24 Jan 2013).

Critical Program Information (CPI). Elements or components of an RDA [research, development & acquisition] program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008 w/ change 1 dated 28 Dec 2010)

Note: DoDI 5200.39 is under revision, proposed revised definition for CPI: *U.S. capability elements that contribute to the warfigthers' technical advantage throughout the life cycle, which if compromised or subject to unauthorized disclosure, decrease the advantage. U.S. capability elements may include, but are not limited to, technologies and algorithms residing on the system, its training equipment, or maintenance support equipment.*

It is DoD policy (IAW DoDI 5200.39) to provide uncompromised and secure military systems to the warfighter by performing comprehensive protection of CPI through the integrated and synchronized application of Counterintelligence, Intelligence, Security, systems engineering, and other defensive counter-measures to mitigate risk.

Failure to apply consistent protection of CPI may result in the loss of confidentiality, integrity, or availability of CPI, resulting in the impairment of the warfighter's capability and DoD's technological superiority.

CPI includes: information about applications, capabilities, processes, and end-items; elements or components critical to a military system or network mission effectiveness; and technology that would reduce the US technological advantage if it came under foreign control.

CPI information shall be identified early in the research, technology development and acquisition processes, but no later than when a DoD Agency or military component demonstrates an application for the technology in an operational setting, in support of a transition agreement with a pre-systems acquisition or acquisition program, or in exceptional cases, at the discretion of the laboratory/technical director.

Critical Technology. Technology or technologies essential to the design, development, production, operation, application, or maintenance of an article or service which makes or could make a significant contribution to the military potential of any country, including the United States. This includes, but is not limited to, design and manufacturing know-how, technical data, keystone equipment, and inspection and test equipment. (DoDI 2040.02, International Transfers of Technology, Articles and Services, 10 Jul 2008) Also see *dual-use, technology*.

DoD Policy – Critical Technology

Dual-use and defense-related technology shall be treated as valuable national security resources, to be protected and transferred only in pursuit of national security and foreign policy objectives. Those objectives include ensuring that: critical U.S. military technological advantages are preserved; transfers which could prove detrimental to U.S. security interests are controlled and limited; proliferation of weapons of mass destruction and their means of delivery are prevented; and diversion of defense-related goods to terrorists is prevented.

See DoDI 2040.02, *International Transfers of Technology, Articles and Services*, 10 Jul 2008.

Critical Thinking. A deliberate meta-cognitive (thinking about thinking) and cognitive (thinking) act whereby a person reflects on the quality of the reasoning process simultaneously while reasoning to a conclusion. The thinker has two equally important goals: coming to a solution and improving the way she or he reasons. (David T. Moore, *Critical Thinking and Intelligence Analysis*)

-- Also, intellectual discipline of rigorously weighing evidence and assumptions, and assessing multiple hypotheses resulting in accurate, persuasive, and policy-relevant conclusions. (DIA, 2012-2017 Defense Intelligence Agency Strategy)

> *Critical Thinking and Intelligence Analysis*, National Defense Intelligence College occasional paper no. 14, March 2007.
> Copy available at <http://www.au.af.mil/au/awc/awcgate/dia/ndic_moore_crit_analysis_hires.pdf>
>
> Also see The Foundation for Critical Thinking, www.criticialthinking.org, *The Thinker's Guide to Analytical Thinking*, 2007.

Criticality. [In critical infrastructure usage] a metric used to describe the consequence of loss of an asset, based on the effect the incapacitation or destruction of the asset would have on DoD operations and the ability of the Department of Defense to fulfill its missions. (DoDI 3020.45, DCIP Management, 21 Apr 2008)

Cross-cuing. The use of one intelligence source to initiate the collection against a particular target with another intelligence collector. Also see *cueing.*

> *CI and HUMINT provide unique opportunities for enabling and cross-cuing other intelligence disciplines or capabilities. CI and HUMINT sources can enable other intelligence collection disciplines or provide time sensitive "tip off" information to cue other collection capabilities.*
> -- JP 2-01.2, *CI & HUMINT in Joint Operations*, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011, para 3b (p. V-2)

Cryptanalysis. The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption. (JP 1-02)

Cryptography. The art and science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. (DoDD 5100.20, NSA, 26 Jan 2010)

Cryptology. The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. (JP 1-02)

-- Also, the branch of knowledge that treats the principles of cryptography and cryptanalytics; and the activities involved in producing signals intelligence (SIGINT) and maintaining communications security (COMSEC). (DoDD 5100.20, NSA, 26 Jan 2010)

Cryptonym. Code name; crypt or crypto for short, always capitalized. …prefixes to code names are used to identify the nature of the clandestine source, [e.g., GT and CK] prefixes were both "diagraph" identifiers for the Soviet and East European program….. The diagraph is used in front of the cryptonym of the source as a more formal way of referring to the subject, not unlike putting "Mr." in front of "Smallwood." (Spy Dust)

-- Also, a false name used in official correspondence to hide the identity of the agent, officer, or operation. (A Spy's Journey)

Cueing. The use of one or more sensor systems to provide data that directs collection by other systems. (term previously defined in FM 2-0, Intelligence, May 2004) Also see *cross-cuing*.

Cultivation. A deliberate and calculated association with a person for the purpose of recruitment, obtaining information, or gaining control. (AFOSI Instruction 71-101, 6 Jun 2000)

-- Also, apparently casual but actually deliberate and calculated effort to gain control of an individual, induce him to furnish information, and agree to recruitment. Cultivation can extend over a considerable periods of time. (FBI FCI Terms)

Cultural Intelligence. Knowledge resulting from all-source analysis of cultural factors, which assists in anticipating the actions of people or groups of people. (National Intelligence: Consumer's Guide - 2009).

Current Intelligence. *Within DoD: None – term removed from JP 1-02 per JP 2-0 Joint Intelligence, 22 Oct 2013.*

> Previously defined as: one of two categories of descriptive intelligence that is concerned with describing the existing situation.

Custodial Interview. Interview conducted of a subject following formal arrest or detention. Subjects are made fully aware of their deprivation of freedom or their "in custody" status. (Army FM 2.22-2, CI, Oct 2009).

Cutout. An intermediary or device used to obviate direct contact between members of a clandestine organization. (JP 1-02)

-- Also, an intermediary used to obviate direct linkage between either the origin or destination of an intelligence operation or action. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, an individual whose services are used to prevent contact and recognition between specific members of an intelligence service with the purpose of providing compartmentation and security. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, a mechanism or person that acts as a compartment between the members of an operation but which allows them to pass material or messages securely. (CI Centre Glossary)

Cyber. 1) Any process, program, or protocol relating to the use of the Internet or an intranet, automatic data processing or transmission, or telecommunication via the Internet or an intranet; and 2) any matter relating to, or involving the use of, computers or computer networks. (Cybersecurity Act of 2009)

Cyber Attack. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) Also see *cyber espionage, cyber threat*.

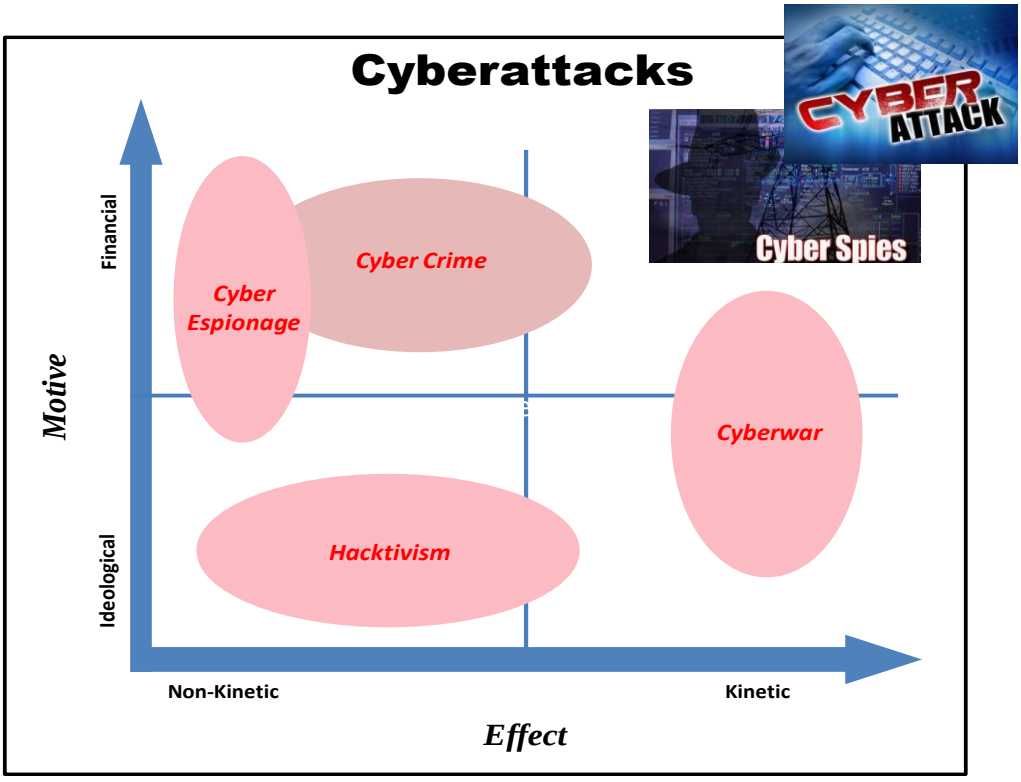
> *Disruptive and destructive cyber attacks are becoming a part of conflict between states, within states, and among nonstate actors. The borderless nature of cyberspace means anyone, anywhere in the world, can use cyber to affect someone else. … The rise of cyber is the most striking development in the post-9/11 national security landscape.*
>
> -- General Martin E. Dempsey (USA), Chairman of the Joint Chiefs of Staff, June 2013
> (Quoted in *Army* Magazine, August 2013, p. 8)
>
> ---
>
> ***Cyber attack** is a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data. It might range from a denial-of-service operation that temporarily prevents access to a website, to an attack on a power turbine that causes physical damage and an outage lasting for days.*
>
> -- DNI, *Worldwide Threat Assessment of the US Intelligence Community*, SSCI, 12 Mar 2013
>
> ---

Existential Cyber Attack *is defined as an attack that is capable of causing sufficient wide scale damage for the government potentially to lose control of the country, including loss or damage to significant portions of military and critical infrastructure: power generation, communications, fuel and transportation, emergency services, financial services, etc.*

-- Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* Jan 2013; copy at: <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

Also see P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs To Know* (2014)

-- Also, Cyberattack: deliberate disruption of a computer system or network and functions delivered or supported by it. (National Research Council - 2009)



Adapted from: Eric Rosenbach and Robert Belk, "U.S. Cybersecurity: The Current Threat and Future Challenges," Nicholas Burns and Jonathon Price, Editors., *Securing Cyberspace: A New Domain for National Security*, 2012, Figure 1, p. 44

Cyber attacks are growing in frequency, scale, complexity and destructiveness.

Cyber attacks are a way of life… *since 2006, cyber incidents against the USG increased 782%* (GPO).

Cyber Counterintelligence. Counterintelligence, by any means, where a significant target or tool of the adversarial activity is a computer, computer network, embedded processor or controller, or the information thereon. (The United States Government-Wide Cyber Counterintelligence Plan - 2009 (U)) Also see *counterintelligence activities in cyberspace; cyberspace.*

* Note: Within DoD the term "cyber counterintelligence " to be withdrawn from JP 1-02; see *Counterintelligence Activities in Cyberspace*.

Cyberspace is a venue.

Cyber Effect: The manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. (PDD-20, US Cyber Operations Policy (U), 16 Oct 2012)

Cyber Electromagnetic Activities (CEMA). Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. (Army FM 3-13, Inform and Influence Activities, Jan 2013)

> CEMA consist of cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (SMO).
>
> See Army FM 3-38, *Cyber Electromagnetic Activities*, 12 Feb 2014.

Cyber Espionage. Refers to intrusions into networks to access sensitive diplomatic, military, or economic information. (DNI, Worldwide Threat Assessment of the US Intelligence Community, SSCI, 12 Mar 2013) Also see *cyber attack, cyber threat*.

-- Also, the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using illegal exploitation methods on internet, networks or individual computers… (Wikipedia at <http://en.wikipedia.org/wiki/Cyber_espionage>; accessed 5 Jan 2010)

> ***"Counterintelligence…is now a concern for every organization that lives on electronic networks and has secrets to keep. Information is liquid and liquid leaks."***
>
> -- Joel Brenner (former NCIX), America *the Vulnerable,: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, 2011, p. 64.

Cyber Exploitation: Penetration of an adversary's computer system or network to seize information (National Research Council, 2009)

> Essentially an intelligence-gathering activity, e.g., Ghostnet, Operation Aurora. Technically, exploits and attack can be similar, i.e., utilize same access vector and manipulate same vulnerability.
>
> ***"Distinction between intelligence collection and damage to systems is a few key strokes"***
>
> -- Richard A. Clarke, Author of *Cyber War*

Cyber Incident. Any attempted or successful access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or an information system, without lawful authority. (NSPD-54 / HSPD-23)

Cyber Intrusion Damage Assessment. A managed, coordinated, and standardized process conducted to determine the impact on future defense programs, defense scientific and research projects, or defense warfighting capabilities resulting from an intrusion into a DIB unclassified computer system or network. (DoDD 5505.13E, DoD Executive Agent for the DoD Cyber Crime Center [DC3], 1 Mar 2010)

Cyber Persona. An identity used in cyberspace to obtain information or influence others, while dissociating the actor's true identity or affiliation. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec10 with change 1 dated 16 Oct 2013)

Cyber Power. The ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power. (Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower and National Security*, Washington, D.C.: National Defense University, 2009)

Cyber power can be used to produce preferred outcomes within cyberspace or it can be use cyber instruments to produce preferred outcomes in other domains outside cyberspace.

See "Cyber Power" by Joseph S. Nye, Harvard Kennedy School, May 2010; available online at: belfercenter.ksg.harvard.edu/files/cyber-power.pdf

Cyber Security (or Cybersecurity). Measures taken to protect a computer network, system, or electronic information storage against unauthorized access or attempted access. (DoDI 5205.13, Defense Industrial Base Cyber Security/Information Assurance Activities, 29 Jan 2010 w/ chg 1 dated 21 Sep 2012) Also see *computer security; information security (INFOSEC).*

-- Also, includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

- Also, the ability to protect, defend, and maintain availability, confidentiality, authentication, and integrity of networks, systems, and the data resident therein. (DoD Strategy for Operating in Cyberspace, May 2011)

-- Also, the ability to protect or defend the use of cyberspace from cyber attacks. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation.

-- National Security Strategy - 2010

"Cybersecurity vulnerabilities challenge governments, businesses, and individuals worldwide. Attacks have been initiated by individuals, as well as countries. Targets have included government networks, military defenses, companies, or political organizations, depending upon whether the attacker was seeking military intelligence, conducting diplomatic or industrial espionage, or intimidating political activists. In addition, national borders mean little or nothing to cyberattackers, and attributing an attack to a specific location can be difficult, which also makes a response problematic."

-- CRS Report, *Cybersecurity: Authoritative Reports and Resources*, 25 Oct 2013
Copy available at: <http://www.fas.org/sgp/crs/misc/R42507.pdf>

_____

"*As long as nations rely on computer networks as a foundation for military and economic power and as long as such computer networks are accessible to the outside, they are at risk."*

-- Rand Report, "Cyberdeterrence and Cyberwar," by Martin C. Libicki (2009)

_____

"*America is being 'invaded,' every hour of every day, by hostile forces using computers…from minor annoyances by young computer hackers to those from sophisticated nations and could cost American lives…the irony is that this new threat stems from the technical sophistication that helps make the US military the strongest in the world."*

-- John Randle, Voice of America, *Future War in Cyberspace*

_____

U.S. military networks *"are constantly under attack. They are probed thousands of times a day. They are scanned millions of times a day. And the frequency and sophistication of attacks are increasing exponentially."*

"The power to disrupt and destroy, once the sole province of nations, now also rests with small groups and individuals, from terrorist groups to organized crime, from hacker activists to teenage hackers, from industrial spies to foreign intelligence services."

-- William Lynn, Deputy Secretary of Defense
(as quoted in "In Cyber War, Most of U.S. Must Defend Itself," by William Matthews, *DefenseNews*, 1 Feb 2010, p. 29)

"Forcing Cybersecurity into a simplified unitary framework limits our choices and underestimates the complexity of the most novel and serious disruptive threat to our national security since the onset of the nuclear age sixty years ago."

-- Michael Chertoff, Former US Secretary of Homeland Security & John M. McConnell, Former DNI
As quoted in *Securing Cyberspace: A new Domain for National Security*, 2012, p. 192

Cyber security within the military is daunting – *"The Department operates over 15,000 networks and 7 million computing devices across hundreds of installations in dozens of countries around the globe."*

-- Zachary J. Lemnios, Assistant Secretary of Defense for Research and Engineering, 20 March 2012
Testimony before the Senate Armed Services Committee hearing on Emerging Threats and Capabilities

---

"In the cyber realm, new exploits can render defenses that seemed effective obsolete in a matter of seconds. Given the speed with which cyber capabilities can be created and the relatively low cost for entry, the potential for possibly far-reaching technological surprise is very high."

-- Dr. James S. Perry, Director of Information Systems Analysis Center at Sandia National Laboratories, 20 March 2012. Testimony before the Senate Armed Services Committee hearing on Emerging Threats and Capabilities

---

"*Repeated cyber intrusions into critical infrastructure demonstrate the need for improved Cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."*

-- EO 13636, *Improving Critical Infrastructure Cybersecurity*, 12 Feb 2013

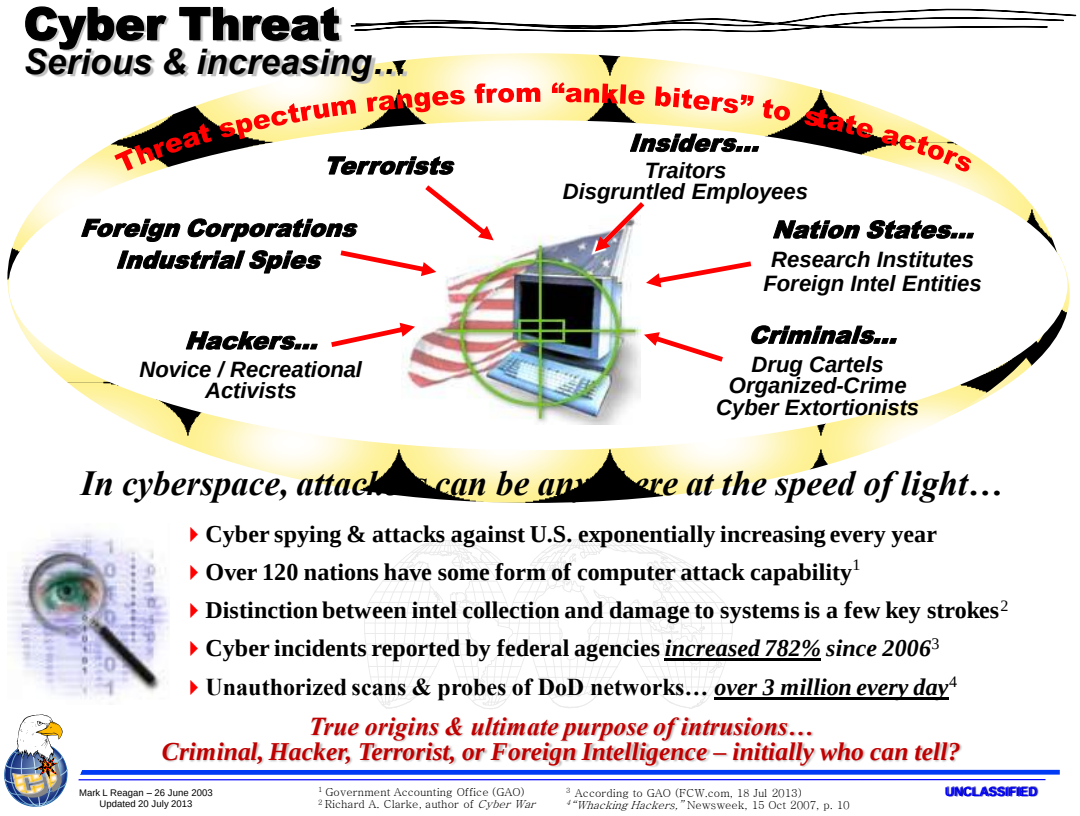
See the "The Comprehensive National Cybersecurity Initiative" at:
<http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>

Also see Committee on National Security Systems, *National Information Assurance (IA) Glossary*, April 2010, <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf>

Also see P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs To Know* (2014)

Cyberattacks are possible only because systems have flaws.

Cyber Threat. The cyber threat is characterized in terms of three classes of increasing sophistication: 1) those practitioners who rely on others to develop the malicious code, 2) those who can develop their own tools to exploit publically known vulnerabilities as well as discovering new vulnerabilities, and 3) those who have significant resources and can dedicate them to creating vulnerabilities in systems. (Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* Jan 2013) Also see *cyber attack*, cyber espionage, *cyber threat investigation.*



Cyber Threat

"In the United States, we define cyber threats in terms of cyber attacks and cyber espionage. A cyber attack is a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data. It might range from a denial-of-service operation that temporarily prevents access to a website, to an attack on a power turbine that causes physical damage and an outage lasting for days. Cyber espionage refers to intrusions into networks to access sensitive diplomatic, military, or economic information."

-- James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Committee on Armed Services, 18 April 2013

The cyber threat the United States faces is increasing in severity and is accessible to a wide range of enemies. *"Most of what we see today is exploitation -- that's theft, stealing secrets, either commercial or military… we know the tools exist to destroy things, to destroy physical property, to destroy networks, to destroy data, maybe even take human lives."*

-- Deputy Defense Secretary William J. Lynn III in a television interview on PBS 14 July 2011

The FBI has noted three primary categories of *cyber threat actors*:

"[1] organized crime groups that are primarily threatening the financial services sector, and they are expanding the scope of their attacks;
[2] state sponsors—foreign governments that are interested in pilfering data, including intellectual property and research and development data from major manufacturers, government agencies, and defense contractors; and
[3] increasingly there are terrorist groups who want to impact this country the same way They did on 9/11 by flying planes into buildings. They are seeking to use the network to challenge the United States by looking at critical infrastructure to disrupt or harm the viability of our way of life."

-- FBI, *The Cyber Threat: Part 1: On the Front Lines With Shawn Henry,* 27 March 2012, http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712/shawn-henry_032712

Foreign intelligence and security services have penetrated numerous computer networks of US Government, business, academic, and private sector entities. Most detected activity has targeted unclassified networks connected to the Internet, but foreign cyber actors are also targeting classified networks.

-- DNI, *Worldwide Threat Assessment of the US Intelligence Community*, SSCI, 12 March 2013, p. 2

[C]omputer network 'exploitation' and 'disruption' activities such as denial-of-service attacks will continue. …the likelihood of a 'destructive' attack that deletes information or renders systems inoperable will increase as malware and attack tradecraft proliferate.

-- DNI, *Worldwide Threat Assessment of the US Intelligence Community*, SSCI, 29 January 2014, p. 1

Cyber Threat Investigation. Any actions taken within the United States, consistent with applicable law and presidential guidance, to determine the identify, location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more cyber threat groups or individuals. (NSPD-54 / HSPD-23)

-- Also, actions taken, consistent with applicable law and Presidential guidance, to determine the identify, location, intent, motivation, capabilities, alliances, funding, or methodologies of one or more FIEs [Foreign Intelligence Entities], that has attempted to penetrate or has, in fact, penetrated a DoD, IC, or DIB [defense industrial base] information system. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010 with change 1 dated 16 Oct 2013)

Attribution is a major problem in the cyber realm

"***Who: Attribution…*** blurry lines between various types of malicious activity in cyberspace may make it difficult for investigators to attribute an incident to a specific individual or organization. Criminal attribution is a key delineating factor between cybercrime and other cyber threats. When investigating a given threat, law enforcement is challenged with tracing the action to its source and determining whether the actor is a criminal or whether the actor may be a terrorist or state actor posing a potentially greater national security threat."

-- CRS Report R42547, *Cybercrime: Conceptual Issues for Congress & U.S. Law Enforcement*, 23 May 2012

"The damage caused by malicious activity in cyberspace is enormous and unrelenting. Every year, cyber attacks inflict vast damage on our Nation's consumers, businesses, and government agencies. This constant cyber assault has resulted in the theft of millions of Americans' identities; exfiltration of billions of dollars of intellectual property; loss of countless American jobs; vulnerability of critical infrastructure to sabotage; and intrusions into sensitive government networks."

-- Senator Sheldon Whitehouse, 14 April 2011

James Clapper, Director of National Intelligence, noted that *"[t]wo of our greatest strategic challenges regarding cyber threats are: (1) the difficulty of providing timely, actionable warning of cyber threats and incidents, such as identifying past or present security breaches, definitively attributing them [emphasis added], and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber attacks; and (2) the highly complex vulnerabilities associated with the IT supply chain for US networks."*

-- Office of the Director of National Intelligence, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence,* 31 Jan 2012, p. 8.

Attribution in cyber is always going to be difficult.
Missiles come with a return address, cyber attacks do not.

-- William Lynn, US Deputy Secrete of Defense
Interview Defense News, 18 July 2011

Cyber Threats. Natural or man-made incidents (intentional or unintentional) that would be detrimental to the cyber domain, or which are dependent on or operate through cyberspace/cyber domain. (Cyber Threats to National Security, Symposium Five, 2011) Also see *cyber threat*.

In the United States, we define cyber threats in terms of cyber attacks and cyber espionage.

-- Hon. James R. Clapper, DNI, Statement for the Record Worldwide Threat assessment of the US Intelligence Community, Senate Committee on Armed Services,18 Apr 2013

Cyber-Terrorism. A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda. (FBI)

-- Also, cyberterrorism: the unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people to further political or social objectives. Actors who engage in these kinds of activities are commonly referred to as cyber terrorists. (Cyber Threats to National Security, Symposium Five, 2011)

Cybercrime. Crime involving use of a computer system or network.

Typically involves data theft (e.g., credit cards, etc.) or transmission (e.g., child porn).

"*Cybercriminals also threaten US economic interests. They are selling tools, via a growing black market, that might enable access to critical infrastructure systems or get into the hands of state and nonstate actors. In addition, a handful of commercial companies sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products. Foreign governments already use some of these tools to target US systems."*

-- Hon. James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Committee on Armed Services, 18 April 2013

Cyberexploitation. Penetration of an adversary's computer system or network to seize information. (National Research Council - 2009)

Essentially an intelligence-gathering activity, e.g., Ghostnet, Operation Aurora.

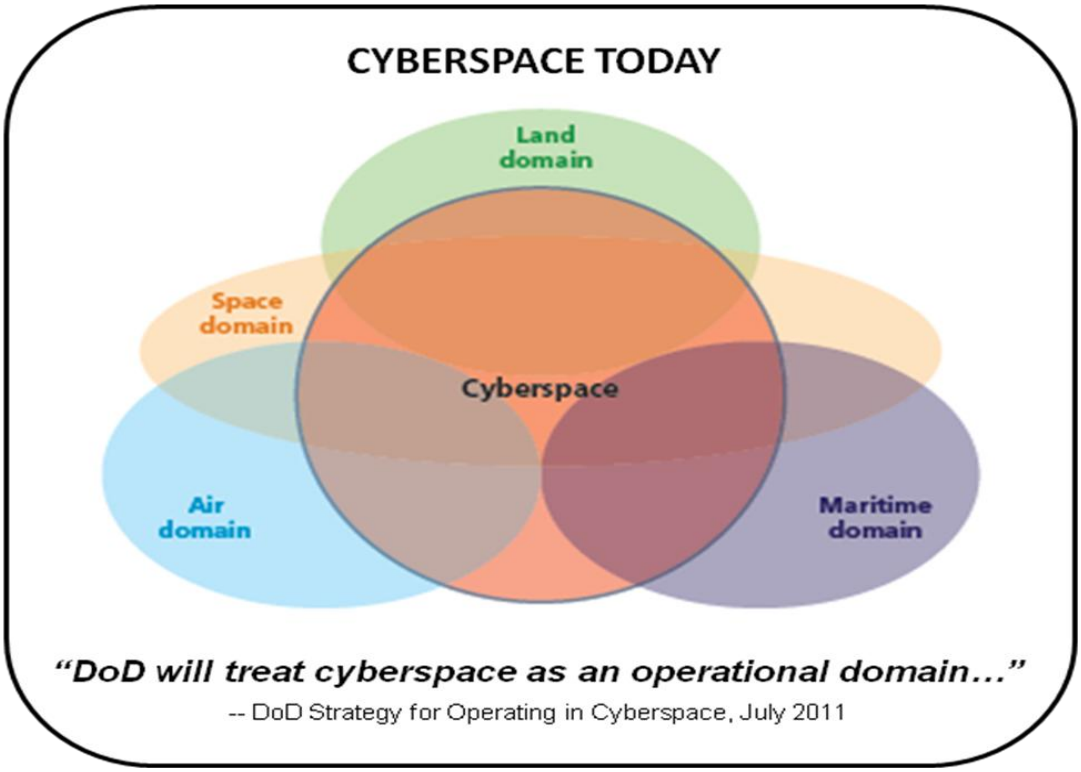
Cyberspace. A global domain within the information environment consisting of the independent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02 and JP 3-12, Cyberspace Operations, 5 Feb 2012) Also see *cyberspace domain*.

-- Also, the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communications systems, networks, and embedded possessors and controllers. (PPD-20, U.S. Cyber Operations Policy (U), 16 Oct 2012)

-- Also, the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded possessors and controllers in critical industries. (NSPD-54 / HSPD-23, 8 Jan 2008)

-- Also, the range of information and resources available through computer networks – especially the Internet. (ODNI Cyberspace Initiative)

-- Also, a global domain within the information environment consisting of the independent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)



-- Adapted from RAND Graphic

In cyberspace, the war has begun…

Cyberspace is a decentralized domain characterized by increasing global connectivity, ubiquity, and mobility, where power can be wielded remotely, instantaneously, inexpensively, and anonymously. This environment presents enormous challenges and unprecedented opportunities…

Cyberspace is a domain that requires man-made technology to enter and exploit. Effects of cyberspace operations can occur simultaneously in many places and they can be precise, broad, enduring and transitory.

Challenges -- Our national security is inextricably linked to the cyberspace domain, where conflict is not limited by geography or time. Cyberspace crosses geographic and jurisdictional boundaries. The expanding use of cyberspace places United States' interests at greater risk from cyber threats and vulnerabilities. Cyber actors can operate globally, within our own borders, and within the borders of our allies and adversaries. The complexity and amount of activity in this evolving domain make it difficult to detect, interdict, and attribute malicious activities.

Threats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies. On the flip side -- cyberspace offers DoD unprecedented opportunities to shape and control the battlespace to achieve national objectives.

Cyberspace will become a main front in both irregular and traditional conflicts. Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In much the same way that airpower transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication. Indeed, adversaries have already taken advantage of computer networks and the power of information technology not only to plan and execute savage acts of terrorism, but also to influence directly the perceptions and will of the U.S. Government and the American population.

-- *The Joint Operating Environment 2010*, US Joint Forces Command

---

"[I]n cyberspace some malicious actors consider that no boundaries exist between military and civilian targets."

-- Congressional Research Service, Report RL32114 (29 Jan 2008)

"…the United States will respond to hostile acts in cyberspace, as we would to any other threat to our country."

-- International Strategy for Cyberspace, May 2011

"Cyberspace is contested every day, every hour, every minute, every second. [The internet] lowers the bar for entry to the espionage game, both for states and for criminal actors. The threat is complex and not easily addressed by just building the security walls higher and higher."

-- Iain Lobban, Chief GCHQ, 13 October 2010

"The myth persists that the United States hasn't been invaded since 1812. I'd like to inform you otherwise. And that is the fact that invasion through cyberspace is now a daily occurrence."

-- Frank Ciffullo, Center for Strategic & International Studies

---

"The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War"

-- Defense Science Board, Jan 2013

For additional information see:

-- DoD website at: <http://www.defense.gov/home/features/2011/0411_cyberstrategy/>
-- *International Strategy for Cyberspace*, May 2011
-- *DoD Strategy for Operating in Cyberspace* (U), May 2011 (classified version)
-- *DoD Strategy for Operating in Cyberspace*, July 2011 (unclassified version)
Copy available at <http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf>
-- ONCIX, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011,* October 2011
-- DSS, *Targeting US Technologies: A Trend Analysis of Reporting from Defense Industry – 2012*
-- Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* Jan 2013
Copy at: <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

Cyberspace Domain. A domain characterized by the use of electronics and electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. (Previously defined in DoDI S-5240.17, CI Collection, 12 Jan 2009)

Cyberspace Operations. The employment of cyber capabilities where the primary purpose is to achieve military objectives in or through cyberspace. (JP 1-02; and JP 3-0, Joint Operations, 11 Aug 2011)

Cybervetting. Checking blogs, social media sites, and other Internet-based sources to identify issues of security concern applicable to people holding or seeking positions of trust. (PERSEREC; accessed 9 Jan 2013)

PERSEREC's initial effort regarding cybervetting entailed working with the national security and law enforcement communities to identify the primary legal, privacy, policy, and procedural considerations that should be taken into account when establishing a cybervetting program. Pilot projects are planned to test the efficacy of cybervetting. In addition, a series of CyberPsychology studies are exploring how certain types of activities in cyber environments, such as Second Life, can spill over into negative affects [sic] on workplace reliability, judgment, and other areas of personnel security concern.

-- PERSEREC at <http://www.dhra.mil/perserec/currentinitiatives.html#Cyber> (accessed 9 Jan 2013)

D ==========

Damage. A loss of friendly effectiveness due to adversary action. Synonymous with harm. (DSS Glossary)

Damage Assessment. [In intelligence usage,] a determination of the effect of a compromise of classified information on national security. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007)

-- Also, the analysis of the impact on national security of a disclosure of classified information to an unauthorized person. (IC Standard 700-1, 4 Apr 2008)

-- Also, systematic analysis that determines the impact of a compromise of classified information on the national security of the United States. (CI Community Lexicon)

-- Also, systematic, comprehensive examination of an intentional and/or inadvertent compromise of classified or sensitive information. (ONCIX, Damage Assessment Guide (U), 21 Mar 2008)

> See ONCIX's *Damage Assessment Guide* - October 2009 (U) for a standardized framework and outline of the processes and procedures involved in national-level damage assessment activity.

Damage to the National Security. Harm to the national defense or foreign relations of the United States from unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information. (EO 13526, Classified National Security Information, 29 Dec 2009)

Danger Signals. Prearranged signals or marks on walls, posts, etc., [used] as a communication system between agents or [case] officers to indicate that the opposition or active enemy is nearby, has been tipped off, or has the area under surveillance. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

Dangle. A person controlled by one intelligence service who is made to appear as a lucrative and exploitable target to an opposing intelligence service. (HDI Lexicon, April 2008) Also see *dangle operation; double agent; penetration; provocation.*

-- Also, an asset placed within the professional or personal view of a FIS [Foreign Intelligence Service] officer or agent with the intention of observing the actions of and possibly being recruited by the FIS. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, counterespionage terminology for the process of presenting an individual to a foreign intelligence service in a manner as to encourage his recruitment as an agent; as "to dangle" or a dangle operation. (CIA in D&D Lexicon, 1 May 2002)

-- Also, an individual who deliberately appears available for recruitment. (Encyclopedia of Espionage, Spies, and Secret Operations, 3rd Edition, 2012)

> ***If you wait for the enemy to come to you, you may not know when he does.***
>
> *…If the fish do not swim into your net, you have to give them a lure, a provocation, something that looks like a juicy worm but that has a hook in it.*
>
> -- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)
>
> ---
>
> *…dangles were a doubled-edged sword, whose specter overshadowed every decision to recruit agents we believed to be real. …Fear of them caused both the KGB and CIA to turn away countless volunteers.*
>
> -- Victor Cherkashin, Former KGB Intelligence Officer and author of *Spy Handler* (2005)

Dangle Operation. An operation in which an enticing intelligence target is dangled in front of an opposition service in hopes they will think him or her a bona fide recruit. The dangle is really a double agent. (Spy Dust) Also see *dangle; double agent penetration; provocation*

Database. *Within DoD: None – term removed from JP 1-02.*

> Previously defined in JP 2-0, Joint Intelligence (22 Jun 2007) as: information that is normally structured and indexed for user access and review. Databases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files.

Data Mining. A program involving pattern-based queries, searches or other analyses of I or more electronic databases, where -- (a) a department or agency of the Federal Government. or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals; (b) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual. or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and (c) the purpose of the queries, searches, or other analyses is not solely- (i) the detection of fraud, waste, or abuse in a Government agency or program; or (ii) the security of a Government computer system. (Data Mining Reporting Act, §804(b)(I)(A))

> *This definition limits covered activities to predictive, pattern-based data mining, which is significant because analysis performed within the ODNI and its constituent elements for counterterrorism and similar purposes is often performed using various types of "link analysis" tools.*
>
> *Unlike "pattern-based" tools, these link analysis tools start with a known or suspected terrorist or other subject of foreign intelligence interest and use various methods to uncover links between that known subject and potential associates or other persons with whom that subject is or has been in contact. The Data Mining Reporting Act does not include such analyses within its definition of "data mining" because such analyses are not "pattern-based."*
>
> -- ODNI 2009 Data Mining Report
>
> ---
>
> *Data mining is finding key pieces of intelligence that may be buried in the mass of data available. Data mining uses automated statistical analysis techniques to search for the specific data parameters that intelligence professionals predetermine will answer their information requirements. Data mining can help organize the mass of collected data.*
>
> -- ADRP 2-0, *Intelligence*, Aug 2012, p. 3-6

DCAT. See *Defense Counterintelligence Anomalies Team*.

DCII. See *Defense Central Index of Investigations*.

DCIP. See *Defense Critical Infrastructure Program*.

DCIP Assessment. A comprehensive assessment of a Defense Critical Asset consisting of an in-depth look based on current DoD DCIP Assessment benchmarks. (CJCSI 3209.01, Defense Critical Infrastructure Program, 9 Jan 2012) Also see *Defense Critical Infrastructure Program.*

DCIP CI Coverage Plan. A formally coordinated, comprehensive plan that outlines the CI support to DCA and Tier 1 TCA protection. A DCIP CI coverage plan is prepared by the critical asset manager and identifies the appropriate support of DoD, non-DoD, and other CI elements necessary to the development and validation of DoD-wide CI support to the DCIP. (DoDI 5240.19, CI Support to DCIP, 31 Jan 2014). Also see *Defense Critical Infrastructure Program.*

> If a "CI Support Plan (CISP)" has been developed for the DCIP organization and meets the requirements of the DCIP CI Coverage Plan IAW DoDI 5240.19 (Table 2) then another plan is not required. For CISPs see DoD Instruction 5240.24, *Counterintelligence Activities Supporting RDA*.

DCIP Threat Assessment. A compilation of strategic intelligence information incorporating multi-faceted threats facing DCAs [Defense Critical Assets] and Tier 1 TCAs [Task Critical Assets]. DCIP threat assessments address threats posed to DCAs from domestic and transnational terrorist elements, foreign intelligence and security services, and weapons of mass destruction. (DoDI 5240.19, CI Support to DCIP, 31 Jan 2014) Also see *Defense Critical Infrastructure Program.*

Dead Drop. A clandestine location for transferring material to or from an agent or asset. (National HUMINT Glossary)

-- Also, a place where a person might leave communications or material in concealment for another person. It serves as a cutout between human elements of a clandestine organization. (AFOSI Instruction 71-101, 6 Jun 2000)

-- Also, a place, unattended by witting individuals, to which communications, materials, or equipment can be left by one individual and from which they can be taken by another individual without either meeting or, ordinarily, seeing one another. Also called a dead letter box, or simply drop. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, a prearranged hidden location used for the clandestine exchange of packages, messages, and payments, which avoids the necessity of an intelligence officer and an agent being present at the same time. (FBI -- Affidavit: USA vs. Robert Philip Hanssen, 16 Feb 2001)

-- Also, a secret location where materials can be left in concealment for another party to retrieve. This eliminates the need for direct contact in hostile situations. (CI Centre Glossary)

-- Also, a preferred means of covert communications in denied areas, separates the agent and handler [case officer] by time, but carries the risk of leaving the package unattended in an environment that could change without warning. (Spycraft, p. 61)

-- Also, pre-cased hiding places used by intelligence services to conduct [clandestine] exchanges with agents. (James M. Olson, Fair *Play: The Moral Dilemmas of Spying*, 2006)

-- Also, a predetermined secret location where [case] officers and agents leave messages and other items for undetected collection by other parties. (*Encyclopedia of the CIA*, 2003)

-- Also, a clandestine communications technique, the dead drop allows agents to exchange messages and other items without the need for a meeting that might attract the attention of hostile surveillance. The dead drop is usually an innocuous, prearranged site where a package or film canister can be secreted temporarily so it can be recovered by the addressee. Ideally, the location is sufficiently innocent to enable both parties to visit it, at different times, without compromising themselves. The use of dead drops is standard tradecraft for espionage professionals, and is usually associated with a remote signaling arrangement so both sides can indicate to the other when a particular drop is ready for servicing. The objective is to obviate the need for personal contact that in denied areas is high risk. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Eliminates the need for direct contact…

In intelligence usage, dead drops are used as a clandestine cut-out to avoid personal meetings which can draw attention to the connection between an intelligence officer/agent handler and an agent/asset. As a rule, a dead drop site is not used more than once.

For a detailed description of dead drops and concealment devices, see *Spycraft*, pp. 388-400.

Debriefing. Systematically covering topics and areas with a voluntary source who consents to a formal interview. (Educing Information - Interrogation: Science and Art, Dec 2006) Also see *strategic debriefing*; *educing information; elicitation; intelligence interrogation; interrogation; interview*.

-- Also, the systematic questioning of individuals to procure information to answer specific collection requirements by direct and indirect questioning techniques. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010; also Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

-- Also, [in detainee operations] the process of using direct questions to elicit intelligence information from a cooperative detainee to satisfy intelligence requirements. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

-- Also, interviewing under other than hostile conditions, of an individual who has completed an intelligence assignment or who has, through observation, participation, or personal knowledge, information of intelligence or counterintelligence value or significance. (AR 381-20, Army CI Program, 25 May 2010)

Counterintelligence debriefings are forms of overt collection entailing the questioning of human sources to satisfy CI requirements.

Debriefings are conducted to obtain CI information acquired by the Component's own employees in the course of their duties. CI debriefings are also used to exploit the opportunity presented by walk-ins and other persons who contact CI elements to provide information of potential CI interest.

-- DoDI S-5240.17, (U) *CI Collection Activities*, 14 Mar 2014 (encl 3, para 2c(1))

Also see Appendix C "Counterintelligence Collection Methods (U)" in JP 2-01.2, *Counterintelligence and Human Intelligence in Joint operations* (U), 16 Mar 2011 w/ chg 1 dated 26 Aug 2011.

Debriefing Operations. Operations conducted to debrief cooperating sources may include refugees, émigrés, displaced persons (DPs), local populace, friendly forces, members of U.S. and foreign governmental and non-governmental organizations, as well as U.S. and foreign personnel employed within the academic, business, or scientific communities. The source may or may not be in custody, and their willingness to cooperate need not be immediate or constant. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Decentralized Execution. Delegation of execution authority to subordinate commanders. (JP 1-02)

Deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006) Also see *counterdeception; deception means; deception in support of OPSEC; denial, military deception.*

-- Also, deliberately manipulating information and perceptions in order to mislead. (Foreign Denial & Deception Committee, 30 Mar 2006)

-- Also, an action intended by an actor to influence the perceptions, decisions, and actions of another. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005)

-- Also, any attempt—by words or actions—intended to distort another person's or group's perception of reality. (Textbook of Political-Military Counterdeception: Basic Principles & Methods, August 2007)

Deception is a fundamental ingredient of military art.
All warfare is based on deception.
-- Sun Tzu (400-320 B.C.)

Deception is the distortion of perceived reality

"Deception is an instrument of policy…. [It] must be orchestrated to succeed."

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

Analysts should routinely consider that their information base is susceptible to deception-- *the distortion of perceived reality.*

Richard Heuer, author of *Psychology of Intelligence Analysis,* notes that analysts often reject the possibility of deception because they see no evidence of it. He then argues that rejection is not justified under these circumstances. If deception is well planned and properly executed, one should not expect to see evidence of it readily at hand. Rejecting a plausible but unproven hypothesis too early tends to bias the subsequent analysis, because one does not look for the evidence that might support it. The possibility of deception should not be rejected until it is disproved or, at least, until a systematic search for evidence has been made and none has been found.

See *Deception 101 –A Primer on Deception* (2004) by Joseph W. Caddell; available online at: <http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=589>

Also see *Textbook of Political-Military Counterdeception: Basic Principles & Methods* (2007) by Barton Whaley, published by the National Defense Intelligence College.

O, what a tangled web we weave,
When first we practise to deceive!

-- Sir Walter Scott, *Marmion* (1808)

MASKIROVKA

According to a declassified 1983 White House National Security Decision Directive --

The Soviet Union… doctrine of "maskirovka" [called] for the use of camouflage, concealment and deception (CC&D) in defense-related programs and in the conduct of military operations. They define maskirovka as a set of measures to deceive, or mislead, the enemy with respect to Soviet national security capabilities, actions, and intentions. These measures include concealment, simulation, diversionary actions and disinformation.

-- National Security Decision Directive 108, *Soviet Camouflage, Concealment and Deception,* 12 Oct 1983 (declassified). Copy available at <http://www.fas.org/irp/offdocs/nsdd/nsdd-108.pdf>

Deception Channel. A means by which controlled information can be reliably transmitted to the target. (CIA in D&D Lexicon, 1 May 2002)

Feeding the enemy self-destructive information is the oldest of arts…. A successful feed should not be considered an operation in and of itself, but rather the fruit of a long fight for control over a channel of information. Therein lies the art.

-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), p. 349

Deception In Support of OPSEC (DISO). A military deception activity that protects friendly operations, personnel, programs, equipment, and other assets from FISS [Foreign Intelligence Security Service] collection. (DoDI S-3604.01, Department of Defense Military Deception, 11 Mar 2013) Also see *deception, military deception*.

The intent of DISO is to create multiple false indicators to confuse FISS, make friendly intentions harder to interpret by FISS, or to limit the ability of FISS to collect accurate intelligence on friendly forces.

DISOs are not targeted against adversary military, paramilitary, or violent extremist organization decision-makers with the intent of eliciting a particular decision or reaction, but are targeted against a FISS or an adversary's intelligence collectors to protect friendly forces by masking, simulating, or dissimulating signatures and observables needed to ascertain friendly capabilities, intent, or vulnerabilities.

Deception Means. Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: 1) physical means -- activities and resources used to convey or deny selected information to a foreign power; 2) technical means -- military material resources and their associated operating techniques used to convey or deny selected information to a foreign power; and 3) administrative means -- resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006)

-- Also, the vehicles or resources for conveying the deception story or deception-related information directly or indirectly to the target. These generally consist of sources accepted by the target as reliable or believable. Deception means have been subdivided into: physical, technical, administrative, and special means. (CIA in D&D Lexicon, 1 May 2002)

Deception Target. The adversary decisionmaker with the authority to make the decision that will achieve the deception objective. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006)

Decipher. Convert enciphered text to plain text by means of a cryptographic system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Declared. An individual or action whose intelligence affiliation is disclosed. (HDI Lexicon, April 2008)

-- Also, an officer, asset, agent, or action whose Agency affiliation is formally identified to a foreign intelligence or security service, government or organization, or other USG entity. (National HUMINT Glossary)

Declassification. The authorized change in the status of information from classified information to unclassified information. (EO 13526, Classified National Security Information, 29 Dec 2009 and DoD IG Evaluation Guide, 22 Jan 2013)

Deconfliction. The process of sharing information regarding collection between multiple agencies to eliminate potential duplication of effort, multiple unintended use of the same source, or circular reporting. (Previously in DoDI S-5240.17, CI Collection, 12 Jan 2009)

Decoy. An imitation in any sense of a person, object, or phenomenon which is intended to deceive enemy surveillance devices or mislead enemy evaluation. (JP 1-02).

Decode. Convert encoded text to plain text by means of a code. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Decrypt. Generic term encompassing decode and decipher. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Deduction. [One of the four basic types of reasoning applied to intelligence analysis,] it is the process of reasoning from general rules to particular cases. Deduction may also involve drawing out or analyzing premises to form a conclusion. (Cited in (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *abduction; induction; scientific method.*

For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003) and *Critical Thinking and Intelligence Analysis* by David Moore, JMIC Press (2006).

Deep Cover. A cover for status designed to withstand close scrutiny by the opposition or through due diligence. (National HUMINT Glossary)

Defection. Conscious abandonment of loyalty, duty, and principle to one's country. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, conscious (mental and/or physical) abandonment of loyalty, allegiance, duty, and principle to one's country. (ICS Glossary)

Defector. A person who has consciously abandoned loyalty to his country and who possess intelligence information of value to another country or countries. (CI Community Lexicon)

-- Also, a person who, for political or other reasons, has repudiated his country and may be in possession of information of interest to the US Government. (ICS Glossary)

-- Also, a person of any nationality, usually from a country whose interests are hostile or inimical to the U.S., who has escaped from the control of his or her country, is unwilling to return to that country, and is of special value to the U.S. Government because: he or she is able to add valuable new or confirmatory information to existing U.S. intelligence knowledge; he or she is, or has been, of operational or political value to a U.S. department or agency; or the defection can be psychologically exploited to the advantage of the U.S. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

"Next to penetrations (moles), defectors are your best weapon against alien intelligence services."

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

An act of treason – a *"defector is an individual who has committed treason, a person who first accepted identification with a regime and then betrayed his allegiance to cooperate with a hostile foreign intelligence service."*

-- Wilhelm Marbes, "Psychology of Treason," in *Studies of Intelligence*, vol. 30, no. 2 (Summer 1986), pp. 1-11. Originally classified "Secret" [declassified].

Defectors *"…certainly the next best thing to penetration. But defector information was finite: it ceased the moment the defector stepped out of his office and crossed to our side."*

-- Richard Helms, *A Look Over My Shoulder: A Life in the Central Intelligence Agency*(2003)

"It's the job of intelligence agencies to distinguish between defectors who claim to have something to say and defectors who are lying and they obviously didn't do their job. The Germans didn't, and we didn't."

-- Richard Perle regarding the Iraqi defector CURVEBALL, 15 Feb 2011

"*Sometimes the bona fides of a defector remain in dispute for many years, as is the case of Yuri Nosenko, who defected from the U.S.S.R. soon after the assignation of President John F. Kennedy in 1963."*

-- Loch K. Johnson and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies* (2008), p.299

Defector in Place. See *recruitment-in-place*.

Defense Attaché. See *Senior Defense Official / Defense Attaché (SDO/DATT).*

Defense Attaché Office (DAO). An organizational element of the U.S. diplomatic mission through which the Defense Attaché System conducts its mission and to which may be attached or assigned such other military detachments or elements as the Secretary of Defense may direct. (DoDI C-5105.32, Defense Attaché System, 18 Mar 2009) Also see *Senior Defense Official / Defense Attaché (SDO/DATT).*

-- Also, a DoD organization established as part of the U.S. diplomatic mission, through which the mission of the Defense Attaché System is accomplished. (DoDI C-5105.81, Implementing Instructions for DoD Operations at U.S. Embassies, 6 Nov 2008)

Defense Central Index of Investigations (DCII). An automated DoD repository that identifies investigations conducted by DoD investigative agencies. DCII does not contain eligibility information. (IC Standard 700-1, 4 Apr 2008)

Effective 26 July 2010, DCII is operated and maintained by the Defense Manpower Data Center (DMDC) on behalf of the DoD components and USD(I). See website at: <https://dcii.dmdc.osd.mil>

Access to DCII is normally limited to DoD and other federal agencies that have adjudicative, investigative and/or counterintelligence missions. Although the DCII database is physically maintained by the DMDC the data it contains is the responsibility of the contributing agencies.

-- Also, a centralized database, organized in a searchable format, of selected unique identifying information and security clearance data utilized by security and investigative agencies in the DoD, as well as selected other Federal agencies, to determine security clearance status and the existence or physical location of criminal and personnel security investigative files. The DCII database is physically maintained by the Defense Manpower Data Center; however, the data that it contains is the responsibility of the contributing agencies. (DoDI 5505.7, Titling & Indexing Subjects of Criminal Investigations in DoD, 27 Jan 2012)

-- Also, an alphabetical index of personal names and impersonal titles that appear as subjects of incidents in investigative documents held by the criminal, counterintelligence, fraud, and personnel security investigative activities of the Defense Investigative Service (DIS), the Defense Criminal Investigative Service (DCIS), and the NSA. DCII records will be checked on all subjects of DOD investigations. (AR 380-67, Personnel Security Program, 24 Jan 2014)

Defense Clandestine Service (DCS). The primary DoD element authorized to conduct clandestine human intelligence (HUMINT) operations is response to high priority national-level intelligence requirements as identified by the USD(I). DCS shall operate worldwide, to include high CI threat and politically sensitive environments. Also see *National Clandestine Service*.

See <http://www.defense.gov/news/newsarticle.aspx?id=116064>

Also see classified SECDEF memorandum, subj: (U) Established of the Defense Clandestine Service, 20 Apr 2012

-- Also, [a DoD organization that] conducts human intelligence (HUMINT) operations to answer national-level defense objectives for the President, the Secretary of Defense, and senior policymakers. The civilian and military workforce of the DCS conducts clandestine and overt intelligence operations in concert with the Central Intelligence Agency, the Federal Bureau of Investigation, and our Military Services to accomplish their mission in defense of the Nation. (www.dia.mil/dcs/; accessed 5 Sep 2013)

Defense Combating Terrorism Center (DCTC). A functional center with the Defense Intelligence Agency focused on terrorism intelligence and related issues within DoD.

Previously known as the Joint Intelligence Task Force for Combating Terrorism (JITF-CT). In the fall of 2012, JITF-CT, the Joint Threat Finance Intelligence Office (JTFI), selected elements from the Defense CI & HUMINT Center, and DIA elements from the Counternarcotics and Western Hemisphere Office (CNW), transitioned into a single center -- *the Defense Combating Terrorism Center (DCTC).*

DCTC is the lead national-level, all-source international terrorism intelligence effort within DoD. It is DoD's all-source national-level intelligence fusion center responsible for enabling DoD counter-terrorism and force protection operations. DCTC analytical assessments address terrorist capabilities, activities and intentions, including terrorist finance activity; see DoDD 2000.12 and DoDI 2000.12.

DIA's Office of Counterintelligence(OCI) focuses on the intelligence apparatus and intelligence activities of international terrorists. In instances where the two missions intersect, DCTC and OCI collaborate and coordinate to ensure that DIA presents a timely, accurate, and consistent picture of the threat to U.S. forces and interests around the world.

Defense Counterintelligence and Human Intelligence Center (DCHC). Previously a center within the Defense Intelligence Agency (DIA) for counterintelligence and human intelligence that was established on 3 August 2008. DCHC was disestablished 28 Jan 2013 by Dir DIA (DIA Vision2020).

Defense Counterintelligence Anomalies Team (DCAT). [DoD CI element that] provides analysis and deconfliction of anomalies and identifies and shares CI insider threat trends with the DoD Components. The DCAT develops, promotes, expands, and improves upon insider threat detection efforts by reaching across organization boundaries and cultivating awareness of anomalies. (DoD Manual 5240.26, CI Insider Threat Program, *draft* 20 Nov 2013) See *anomalies*.

> DoD Components report and handle "anomalies" in accordance with DoDD O-5240.02 (Counterintelligence) and DoDI 5240.26 (Countering Espionage, International Terrorism, and the CI Insider Threat).

Defense Counterintelligence Components. DoD organizations that perform national and DoD counterintelligence and counterintelligence-related functions, including the DoD Counterintelligence Field Activity and the counterintelligence elements of the Military Departments, the Defense Agencies with organic counterintelligence, the Joint Staff, the Office of the Secretary of Defense, and the Combatant Commands. (DoDD 5143.01, USD/I, 23 Nov 2005)

Defense Counterintelligence Enterprise. The collective of DoD organizations authorized to conduct counterintelligence and related activities. See *Defense Counterintelligence Components,*

Defense Counterintelligence Knowledge Base (DCIKB). Serves the Defense CI enterprise as the web-enabled system for collecting observations of CI best practices and lessons learned, disseminating these across DoD CI, conducting triage for further action and facilitating change.

> *DCIKB collects, analyzes, manages, and disseminates knowledge gained through operational experience, exercises, and supporting activities in order to achieve higher levels of performance and to provide information and analysis on emerging issues and trends.*
>
> -- NIPRNet website at: <https//sss.mccll.usmc/dcikb>
>
> -- SIPRNet website at: <www.mccll.usmc.smil.mil/dcikb>

Defense Counterintelligence Manager. The official responsible who provides the centralized management of Defense CI Enterprise-wide activities. (DoDD O-5240.02, CI, 20 Dec 2007 with change 1 dated 30 Dec 2010)

> Director DIA serves as the *Defense CI Manager*, with responsibility to provided for central management of Defense CI Enterprise-wide activities (see O-DoDD 5240.02, para 5.3.1). This role is a corollary to the Director DIA's role as the Defense HUMINT Manager; see *Defense HUMINT Manager*.

Defense Courier Service (DCS). A global courier network for the expeditious, cost-effective, and secure distribution of highly classified and sensitive material.

> For DoD policy see DoDI 5200.33, *Defense Courier Operations (DCO),* 30 Jun 2011.
>
> DCS is under the United States Transportation Command (USTRANSCOM). On 15 November 2005, the Defense Courier Division (TCJ3-C) assumed operational control of worldwide defense courier stations and continues to synchronize the defense courier related activities of the USTRANSCOM staff. See web site at: <http://www.transcom.mil/dcd/> Note: DCS was previously known as the Armed Forces Courier Service (ARFCOS).

Defense Criminal Investigative Service (DCIS). The criminal investigative arm of the Inspector General (IG) of the Department of Defense responsible for investigating: terrorism; technology/munitions theft & diversion; cyber crime; substandard/defective products; and fraud, bribery & corruption. (DCIS – see website at <http://www.dodig.mil/INV/DCIS/index.html>)

Defense Criminal Investigative Organizations (DCIOs). The Defense Criminal Investigative Service, the U.S. Army Criminal Investigation Command, the Naval Criminal Investigation Service, and the Air Force Office of Special Investigations. (DoDI 5505.7, Titling & Indexing Subjects of Criminal Investigations in DoD, 27 Jan 2012)

Defense Critical Asset (DCA). An asset of such extraordinary importance to operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its missions. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *defense critical infrastructure program (DCIP); task critical asset (TCA)*.

Defense Critical Infrastructure (DCI). The composite of DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide. DCI is a combination of task critical assets and defense critical assets. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *defense critical infrastructure program (DCIP).*

-- Also, Department of Defense and non-Department of Defense networked assets and facilities essential to project, support, and sustain military forces and operations worldwide. (JP 3-27, Homeland Defense, 29 Jul 2013)

-- Also, DoD and non-DoD cyber and physical assets and associated infrastructure essential to project and support military forces worldwide. (DoD Strategy for Homeland Defense & Civil Support)

Defense Critical Infrastructure Program (DCIP). A DoD risk management program that seeks to ensure the availability of DCI [Defense Critical Infrastructure]. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *defense critical asset*, *defense critical infrastructure*, *task critical asset*.

> DCIP is an integrated risk management program designed to support DoD mission assurance. The purpose of the DCIP is to ensure the availability of Defense Critical Infrastructure in an all-threat and all-hazard environment.

> Key DCIP references include:
> -- DoD, *Strategy for Defense Critical Infrastructure*, March 2008
> -- DoDD 3020.40, *DoD Policy & Responsibilities for Critical Infrastructure*, 14 Jan 2010 with Chg 2
> -- DoDI 3020.45, *DCIP Management*, 21 Apr 2008
> -- DoDI 3020. 51, *Intelligence Support to DCIP*, 23 Jun 2011
> -- DoDI 5240.19, *CI Support to DCIP*, 31 Jan 2014
> -- DoD Manual 3020.45-M, Vol 3, *DCIP Security Classification Manual*, 15 Feb 2011
> -- CJCSI 3209.01, Defense Critical Infrastructure Program, 9 Jan 2012
> -- USSTRATCOM, *Strategic Mission Assurance Data System (SMADS) User Manual*, Apr 2013
>
> DCIP is a evolving program, see web site at: <http://dcip.dtic.mil/>

Defense Cyber Crime Center (DC3). The Defense Computer Forensics Laboratory and the Defense Computer Investigations Training Program comprise the Defense Cyber Crime Center. The forensics laboratory provides counterintelligence, criminal, and fraud computer-evidence processing, analysis, and diagnosis to DoD investigations. The investigations training program provides training in computer investigations and computer forensics to DoD investigators and examiners. AFOSI is the DoD executive agent for the Center. (DC3 web site)

> *DC3 sets standards for digital evidence processing, analysis, and diagnostics for any DoD investigation that requires computer forensic support to detect, enhance, or recover digital media, including audio and video. The Center assists in criminal, counterintelligence, counterterrorism, and fraud investigations of the Defense Criminal Investigative Organizations (DCIOs) and DoD counterintelligence activities. It also supports safety investigations and Inspector General and commander-directed inquiries.*

DC3 aids in meeting intelligence community document exploitation objectives from a criminal law enforcement forensics and counterintelligence perspective. DC3 provides computer investigation training to forensic examiners, investigators, system administrators, and any other DoD members who must ensure Defense information systems are secure from unauthorized use, criminal and fraudulent activities, and foreign intelligence service exploitation. DC3 remains on the leading edge of computer technologies and techniques through research, development, testing, and evaluation applied to digital evidence processing and computer forensic analysis; and by partnering with governmental, academic, and private industry computer security officials.

-- DC3 web site at <http://www.dc3.mil/dc3/dc3About.php>

Also see DoDD 5505.13E, *DoD Executive Agent for DC3*, 1 Mar 2010

Defense HUMINT Enterprise (DHE). The collective of DoD organizations authorized to conduct HUMINT and related activities under the centralized management of the DHM [Defense HUMINT Manager]. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013 w/ chg 1 dated 13 Jun 2013) Also see *Defense Clandestine Service*.

-- Also, the collective of DoD organizations authorized to conduct HUMINT and related activities. (DoDD S-5200.37, Management & Execution of Defense HUMINT (U), 9 Feb 2009)

Defense HUMINT Executor. The senior DoD intelligence official as designated by the head of each of the DoD components who are authorized to conduct human intelligence and related intelligence activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Defense HUMINT Manager (DHM). The Director DIA, as designated by the USD(I), is the official responsible for the centralized management of the DoD-wide HUMINT Enterprise. (DoDD S-5200.37, Management and Execution of Defense HUMINT (U), 9 Feb 2009)

-- Also, [Dir DIA] serve as the Defense HUMINT Manager (DHM) responsible for centralized management of the DoD-wide HUMINT enterprise, which is based on decentralized execution of HUMINT operations and related activities. (DoDD 5105.21, DIA, 18 Mar 2008)

Defense Industrial Base (DIB). The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. (JP 1-02 and JP 3-27, Homeland Defense, 29 Jul 2013)

DoD is responsible for critical infrastructure protection within the defense industrial base per PDD-21.

-- PDD-21, *Critical Infrastructure Security and Resilience*, 12 Feb 2013

The DIB Sector consists of government and private sector organizations that can support military operations directly; perform R&D; design, manufacture, and integrate systems; and maintain depots and service military weapon systems, subsystems, components, subcomponents, or parts—all of which are intended to satisfy U.S. military national defense requirements.

The government component of the DIB consists of certain laboratories, special-purpose manufacturing facilities, capabilities for production of uniquely military material such as arsenals and ammunition plats, and other services.

The private sector of the DIB consists of hundreds of thousands of independent, competing domestic and foreign companies and supply chains, delivering a vast array of products and services to DoD. DIB defense-related products and services equip, inform, mobilize, deploy, and sustain U.S. military and allied military forces worldwide. The DIB companies also deliver national security products and services to other federal agencies.

-- *Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010, p. 15

Defense Infrastructure Sector (DIS), A virtual association within the DCIP that traverses normal organizational boundaries and encompasses defense networks, assets, and associated dependencies that perform similar functions within the Department of Defense and are essential to the execution of the National Defense Strategy. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

IAW the DoDD 3020.40, the ten (10) *defense infrastructure sectors* are:

DIB Sector. The DoD, U.S. Government (USG), and private sector worldwide industrial complex with capabilities to perform research, development, and design and to produce and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

Financial Services Sector. The DoD, USG, and private sector worldwide network and its supporting infrastructure that meet the financial services needs of the Department of Defense across the range of military operations.

GIG Sector. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. It includes all owned and leased communications (commercial telecommunication infrastructure) and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 11103 of title 40, U.S.C. (Reference (n)).

Health Affairs Sector. The DoD, USG, and private sector worldwide healthcare network and its supporting infrastructure that meet the healthcare needs of DoD personnel across the range of military operations.

Intelligence Sector. Those DoD, USG, and private sector facilities, networks, and systems (assets) located worldwide or extra-terrestrially that conduct and support the collection, production, and dissemination of intelligence, surveillance, and reconnaissance information essential to the execution of the National Military Strategy. These assets encompass human intelligence, geospatial intelligence, measurement and signature intelligence, signals intelligence, open-source intelligence, and technical intelligence; counterintelligence collection, processing, and exploitation means; and all-source analysis and production, including the networks and means over which intelligence information is shared, communicated, and/or disseminated.

Logistics Sector. The DoD, USG, and private sector worldwide facilities, networks, and systems that support the provision of supplies and services to U.S. forces.

Personnel Sector. The DoD, USG, and private sector worldwide network that coordinates and supports personnel and human resource functions of DoD personnel.

Public Works Sector. The DoD, USG, and private sector worldwide network, including the real property inventories (environment, land, buildings, and utilities), that manages the support, generation, production, and transport of commodities (e.g., electric power, oil and natural gas, water and sewer, and emergency services) for and to the Department of Defense.

Space Sector. The DoD, USG, and private sector worldwide network, including both space- and ground-based systems and facilities, that supports launch, operation, maintenance, specialized logistics, and control systems for the space assets relied upon by the Department of Defense.

Transportation Sector. The DoD, USG, and private sector worldwide network that provides military lift support (surface, sea, and air) for U.S. military operations.

Defense Infrastructure Sector Lead Agents (DISLAs). Designated DoD officials and their respective defense sector organizations that perform defense infrastructure sector responsibilities. In coordination with their respective PSAs [Principal Staff Assistants], the DISLAs characterize their defense infrastructure sectors to identify functions, systems, interdependencies, and, ultimately, sector task critical assets that support Combatant Command, Military Department, and Defense Agency missions and sector functions. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Defense Intelligence. Integrated departmental intelligence that covers the broad aspects of national policy and national security and that intelligence relating to capabilities, intentions, and activities of foreign powers, organizations, or persons, including any foreign military or military-related situation or activity which is significant to Defense policy-making or the planning and conduct of military operations and activities. Defense intelligence includes Active and Reserve military, strategic, operational, and tactical intelligence. (DoDD 5143.01, USD/I, 23 Nov 2005)

Defense Intelligence Agency (DIA). A Department of Defense combat support agency and a member of the United States Intelligence Community responsible for providing timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policymakers. DIA is a major producer and manager of foreign military intelligence.

DIA is the nation's premier all-source military intelligence organization, providing the most authoritative assessments of foreign military intentions and capabilities to U.S. military commanders and civilian policymakers.

_____

DIA's core mission resides in four intelligence competencies: all-source analysis, counterintelligence (CI), human intelligence (HUMINT), and measurement and signature intelligence (MASINT).

-- 2012-2017 Defense Intelligence Agency Strategy
Copy available at: <http://www.dia.mil/about/strategic-plan/2012-2017-DIA-Strategic-Plan.pdf>

_____

Director DIA serves as the Defense HUMINT Manager responsible for centralized management of the DoD-wide HUMINT enterprise.

-- DoDI 5105.21, DIA, 18 Par 2008, para 6.2.1, p.5

DIA VISION2020
(IOC 28 Jan 2013)

VISION2020 [is] a transformational effort within DIA that redesigns and will fundamentally reposition the Agency to better address our nation's challenges. […]

VISION2020 aims to build a strong intelligence capability that will integrate and operationalize intelligence to ensure the security of the United States well into the 21st Century.

DIA's new center of gravity will be compromise of four Regional Centers (Asia/Pacific, Europe/Eurasia, Middle East/Africa, and the Americas) and one Functional Center (Defense Combating Terrorism Center DCTC))…

-- LTG Michael T. Flynn (USA), Director DIA

Defense Intelligence Analysis Program (DIAP). The DoD intelligence analysis community's resource allocation and prioritization program. The DIAP establishes the policies, procedures, responsibilities, and levels of analytic effort required to provide timely, objective, and cogent intelligence to warfighters, defense planners, and policymakers. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

-- Also, a DIA developed intelligence analysis production plan to enhance the ability of defense intelligence to focus on critical areas of national security interest, while maintaining a perspective on potential emerging threats. (DIA)

GDIP Directive No. 006, Subject: *Defense Intelligence Analysis Program*, 31 Oct 2005, establishes the policies, procedures, responsibilities, and levels of analytical effort required for Defense intelligence to provide timely, objective, and cogent military intelligence to warfighters, defense planners, and defense and national security policymakers. Program guidance and roles and responsibilities posted on INTELINK at: <http://www.dia.ic.gov/admin/diap/index.htm>.

DIAP organizations are responsible for proactively producing intelligence on topics for which they are assigned responsibility IAW *Defense Intelligence Analysis Program Management Guidance*, 24 Feb 2010. DIA's Office of Counterintelligence is responsible for analyzing foreign intelligence activities and threats to US Defense and Service interests.

Defense Intelligence Components. All DoD organizations that perform national intelligence, Defense Intelligence, and intelligence-related functions, including: the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; the National Security Agency/ Central Security Service; and the intelligence elements of the Active and Reserve component of the Military Departments, including the United States Coast Guard when operating as a service in the United States Navy. (DoDD 5143.01, USD/I, 23 Nov 2005)

Defense Intelligence Enterprise. The Enterprise is comprised of intelligence, CI, and security components of the Joint Staff, Combatant Commands, Military Departments, and other Department elements, as well as those organizations under the authority, direction, and control of the Under Secretary of Defense for Intelligence (USD(I)). (DIA, 2012-2017 Defense Intelligence Agency Strategy)

Defense Intelligence Operations Coordination Center (DIOCC). [Defense-level entity that] integrates and synchronizes military and National Intelligence capabilities. The DIOCC plans, prepares, integrates, directs, manages and synchronizes continuous full-spectrum Defense intelligence operations in support of Combatant Commands. (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007) Also see *Joint Intelligence Operations Center (JIOC).*

> To be disestablished per SECDEF memo, subj: Track Four Efficient Initiatives Decision, 14 Mar 2011 (p.43) which directs the disestablishment the DIOCC and the transfer of its functions to the Joint Staff.

Defense Personnel Security Research Center (PERSEREC). A Department of Defense entity dedicated to improving the effectiveness, efficiency and fairness of the DoD personnel security system.

> PERSEREC was established in response to a recommendation by the DoD Security Review Commission (known as the Stilwell Commission), set up in the wake of the very damaging Walker espionage case, to improve DoD's personnel security system. In its 1985 report, the commission called for a personnel security research center to provide policymakers with an objective basis for policies and processes related to the security clearance system.
>
> PERSEREC report entitled, *Espionage and Other Compromises of National Security: Case Summaries from 1975 to 2008* (11 Aug 2009), provides summaries of 141 publicly reported espionage related cases. These cases demonstrate that loyal and conscientious employees continue to be the target of attempts by agents of foreign intelligence services to recruit them as sources of sensitive defense and intelligence information.
>
> Also see *Changes in Espionage by American: 1947- 2007*, PERSEREC Technical Report 08-5 (March 2008). PERSEREC reports available at: <http://www.dhra.mil/perserec/index.html>

Defense Security Enterprise (DSE). The organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to safeguard DoD personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences. This system of systems comprises personnel, physical, industrial, information, and operations security, as well as SAP security policy, critical program information protection policy, and security training. It addresses, as part of information security, classified information, including sensitive compartmented information, and controlled unclassified information. It aligns with counterintelligence, information assurance, foreign disclosure, security cooperation, technology transfer, export control, cyber security, nuclear physical security, chemical and biological agent security, antiterrorism, force protection, and mission assurance policy and is informed by other security related efforts. (DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012, w/ chg 1 dated 24 Apr 2013)

Defense Security Service (DSS). An agency of the Department of Defense (DoD) located in Quantico, Virginia with field offices throughout the United States. The Under Secretary of Defense for Intelligence provides authority, direction and control over DSS. DSS provides the military services, Defense Agencies, 24 federal agencies and approximately 13,000 cleared contractor facilities with security support services. (DSS Glossary) Also see *industrial security; National Industrial Security Program (NISP).*

DSS is the DoD Cognizant Security Office for industrial security, responsible for the DoD portion of the National Industrial Security Program (NISP) and, by mutual agreement, other U.S. Government departments and agencies; provides security education & training products and services; administers the industrial portion of the DoD Personnel Security Program (PSP); provides authorized counterintelligence services; and also supports DoD efforts to improve security programs and processes.

– DoDD 5105.42, *Defense Security Service*, 3 Aug 2010 (w/ chg 1 dated 31 Mar 2011)

On behalf of the Department of Defense and other U.S. Government Departments and Agencies, the DSS supports national security and the warfighter through our security oversight and education missions. DSS oversees the protection of U.S. and foreign classified information and technologies in the hands of industry under the National Industrial Security Program (NISP).
The NISP applies to all Executive Branch Departments and Agencies and to all cleared contractor facilities located within the United States (Para 1-102, NISPOM).

DSS elements include:

The Center for Development of Security Excellence (CDSE) is located in Linthicum, Md., and provides security education and training to DoD security professionals through formal classroom and distributed learning methodologies (i.e., computer-based, web-based and tele-training).

The Defense Industrial Security Clearance Office (DISCO), located in Fort Meade, Md., processes requests for industrial personnel security investigations and provides eligibility or clearance determinations for cleared industry personnel under the NISP.

See DSS web site at: <http://www.dss.mil/ > (SIPRNet at <https://www.dss.smil.mil>)

DSS has organic counterintelligence support. The DSS CI Directorate's mission is to identify unlawful penetrators of cleared U.S. defense industry and articulate the threat for industry and U.S. government leaders.

The CI Directorate's premier publication, *Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry*, analyzes suspicious contact reports (SCRs) from across the DIB describing suspicious foreign activity targeting U.S. personnel, technologies, and export-controlled products. This publication is available in both an unclassified and classified version. See DSS CI web page at: <http://www.dss.mil/isp/count_intell/index.html>

Timelines –

Jan 1972 – the Defense Investigative Service (DIS)—predecessor to DSS—established to consolidate DoD personnel security investigations (PSIs)
May 1993 – DIS established a counterintelligence office
Nov 1997 – DIS redesignated as the Defense Security Service (DSS) to reflect the agency's broader mission and functions, including industrial security, personnel security, security education and training missions.
Feb 2005 – DSS's personnel security investigations functions transferred to the Office of Personnel Management (OPM)
Dec 2007 – Director DSS named the functional manger for DoD security training

Defense Technology Base. All aspects of basic research plus those portions of applied research and technology development devoted to military systems in the generic sense. Prototyping and test and evaluation of specific technology enabled capabilities to prove the feasibility of a concept are also included. Development and engineering for specific military systems are NOT part of the defense technology base. (DoDI 3100.08, The Technical Cooperation Program (TTCP), 7 Aug 2012)

Defense Unknown Subject Team (DUST). DoD's Enterprise-level focal point and action center to resolve CI leads in which the subject's identity and/or specific affiliation with the DoD is not evident. (DoD FCIP Strategy FY 2013-2017) Also see *Unknown Subject; Unknown Subject Lead*.

-- Also, [DoD element that] serves as the DoD focal point to resolve CI leads in which the subject's identity and specific affiliation with DoD is not evident.

> DoD Components will report unknown subject leads to the DUST in accordance with DoD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence Insider Threat* (Enclosure 3, paragraph 1)

Defensive Counterintelligence Activities. Those counterintelligence activities designed to protect… personnel, operations, technology, and information against collection or exploitation by a foreign intelligence service, as contrasted with offensive counterintelligence activities, which are designed to attack the intelligence services of foreign adversaries by penetrating, collaborating, or conspiring with them to achieve that purpose. (AR 381-20, Army CI Program, 25 May 2010)

Defensive Cyberspace Operations (DCO). Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (JP 1-02 and JP 3-12, Cyberspace Operations, 5 Fen 2013)

Defensive Travel Security Briefing. Formal advisories that alert traveling personnel of the potential for harassment, exploitation, provocation, capture, entrapment, or criminal activity. These briefings, based upon actual experience when available, include recommended courses of action to mitigate adverse security and personal consequences. The briefings also suggest passive and active measures that personnel should take to avoid becoming targets or inadvertent victims in hazardous areas. (DSS Glossary)

Deliberate Compromise. The act, attempt, or contemplation of intentionally conveying classified documents, information, or material to any unauthorized person, including public disclosure, or the intentional misuse or mishandling of classified information, (AR 381-20, Army CI Program, 25 May 2010)

Delimitations Agreement. Common term for the DoD/Department of Justice Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation. (AR 381-20, Army CI Program, 25 May 2010)

Demarche. An official protest delivered through diplomatic channels from one government to another. (Words of Intelligence, 2nd Edition, 20110

Denial. Measures taken to block, prevent, or impair US intelligence collection. (Foreign Denial & Deception Committee, 30 Mar 2006)

-- Also, the attempt to block information that could be used by an opponent to learn some truth. (Roy Godson and James J. Wirtz, "Strategic Denial and Deception," in *Strategic Denial and Deception: The 21st Century Challenge*, eds. Roy Godson and James J. Wirtz, 2002) Also see *deception*.

-- Also, methods used to conceal state and military secrets particularly from foreign intelligence collections. (Joseph W. Caddell; *Deception 101 – A Primer on Deception*, Strategic Studies Institute, US Army War College, 2004)

-- Also, activities and programs designed to eliminate, impair, degrade, or neutralize the effectiveness of intelligence collection within and across any or all collection disciplines, human and technical. (Dr. James B. Bruce, "Denial and Deception in the 21st Century: Adaptation Implications for Western Intelligence," in *Defense Intelligence Journal*, Vol 15, No 2, 2006; pp 13-27)

Denial and Deception – equal parts art and science

Keeping secrets and negating access conceals the truth from an opponent's acquisition. *Denial* hides the real and *deception* portrays the fake.

For additional information see Joint Pub 3-13.4, *Military Deception*, 13 Jul 2006

Denial of intelligence collection is a significant impediment to successful analysis

Denied Area. An area under enemy or unfriendly control in which friendly forces cannot expect to operate successfully within existing operational constraints and force capabilities. (JP 1-02 and JP 3-05, Special Operations, 18 Apr 2011)

-- Also, a country with which the US has no official or formal diplomatic relations, or a country in which the capabilities and focus of the local CI services create an operating environment so hostile as to require non-traditional tradecraft of the highest order. (National HUMINT Glossary)

Denied Area Tradecraft. The specialized clandestine methodology used in handling agents in particularly difficult and hostile environments. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Departmental Intelligence. Intelligence that any department or agency of the Federal Government requires to execute its own mission. (JP 1-02)

Department of Defense Components. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Department of Defense agencies, Department of Defense field activities, and all other organizational entities in the Department of Defense. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Department of Defense Intelligence Information System (DoDIIS). The combination of Department of Defense personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and information to military commanders and national-level decision makers. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, a DIA-led enterprise that manages the intelligence information technology activities of and provides intelligence technology to the Department of Defense, the combatant commands, and other national security entities. (National Intelligence: A Consumer's Guide - 2009)

Department of State / Bureau of Diplomatic Security (DS). The security and law enforcement arm of the U.S. Department of State. DS is responsible for providing a safe and secure environment for the conduct of U.S. foreign policy; it is involved in international investigations, threat analysis, cyber security, counterterrorism, security technology, and protection of people, property, and information. (www.state.gov) Also see *Regional Security Officer*.

Every diplomatic mission in the world operates under a security program designed and maintained by DS. In the United States, diplomatic security personnel protect the Secretary of State and high-ranking foreign dignitaries and officials visiting the United States, investigates passport and visa fraud, and conducts personnel security investigations. Operating from a global platform in 25 U.S. cities and 159 foreign countries, diplomatic security ensures that America can conduct diplomacy safely and securely. DS plays a vital role in protecting U.S. embassies and personnel overseas, securing critical information systems, investigating passport and visa fraud, and fighting the war on terror.

-- Department of State website: <http://state.gov/m/ds/index.htm>

Department of State / Bureau of Intelligence and Research (INR). State's intelligence component that provides analysis of global developments to the State Department and contributes its unique perspectives to the community's National Intelligence Estimates. (WMD Report, 31 Mar 2005)

For additional information: <http://www.state.gov/s/inr/ >

Department of Homeland Security (DHS) / Directorate of Information Analysis and Infrastructure Protection. Monitors, assesses, and integrates terrorist-related information; and assesses and addresses the vulnerabilities of the nation's critical infrastructure. (WMD Report, 31 Mar 2005)

Department of Treasury / Office of Terrorism and Financial Intelligence. Treasury's intelligence component that collects and processes information that bears on U.S. fiscal and monetary policy and threats to U.S. financial intuitions. (WMD Report, 31 Mar 2005)

Dependency. [In critical infrastructure protection usage] a relationship or connection in which one entity is influenced or controlled by another entity. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Derogatory Information. Issue information that adversely reflects on a person's loyalty, reliability and trustworthiness. (IC Standard 700-1, 4 Apr 2008)

Desired Perception. In military deception, what the deception target must believe for it to make the decision that will achieve the deception objective. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006)

Detainee. A term used for any person captured or otherwise detained by an armed force. (JP 1-02)

Within DoD, detainee includes any person captured, detained, or otherwise under the control of DoD personnel (military, civilian, or contract employee). It does not include persons being held primarily for law enforcement purposes except where the United States is the occupying power. As a matter of policy, all detainees will be treated as EPWs until some other legal status is determined by competent authority.

For additional information see JP 3-63, *Detainee Operations*, 30 May 2008.

Detection. 1) In tactical operations, the perception of an object of possible military interest but unconfirmed by recognition; 2) In surveillance, the determination and transmission by a surveillance system that an event has occurred; 3) In arms control, the first step in the process of ascertaining the occurrence of a violation of an arms control agreement; and 4) In chemical, biological, radiological, and nuclear environments, the act of locating chemical, biological, radiological, and nuclear hazards by use of chemical, biological, radiological, and nuclear detectors or monitoring and/or survey teams. (JP 1-02)

Deterrence. The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. (JP 1-02)

Devil's Advocacy. Challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005)

Devil's Advocacy is most effective when used to challenge an analytical consensus or key assumption regarding a critically important intelligence question.

DIAP. Also see *Defense Intelligence Analysis Program (DIAP)*.

Digital and Multimedia (D/MM) Forensics. The application of computer science and investigative procedures involving the examination of D/MM material. D/MM forensics is derived from a combination of definitions as it applies across the spectrum of computer forensics, audio forensics, image analysis, and video analysis. Also see *digital evidence, digital forensics*, and *forensic science*.

D/MM forensic sub-disciplines include:

Computer and Electronic Device Forensics. The scientific examination, analysis, and/or evaluation of digital and electronic materials.

Audio Forensics. The scientific examination, analysis, comparison, and/or evaluation of audio.

Image Analysis. The application of image science and domain expertise to examine and interpret the content of an image and/or the image itself.

Video Analysis. The scientific examination, comparison, and/or evaluation of video.

Digital Evidence. Information of probative value stored or transmitted in binary form. (DoDD 5505.13E, DoD Executive Agent for the DoD Cyber Crime Center, 1 Mar 2010)

-- Also, information stored or transmitted in binary form that may be introduced and relied upon in court. (DoJ, *Electronic Crime Scene Investigation, 2nd Edition: A Guide for First Responders*, Apr 2008)

Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination. Digital evidence:

- Is latent, like fingerprints or DNA evidence.
- Crosses jurisdictional borders quickly and easily.
- Is easily altered, damaged, or destroyed.
- Can be time sensitive.

-- *Electronic Crime Scene Investigation, 2nd Edition,* April 2008. Available online at: www.ncjrs.gov/pdffiles1/nij/219941.pdf

Also see United States Secret Service, *Best Practices for Seizing Electronic Evidence v.3, A Pocket Guide for First Responders*

Digital Forensics. In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony. Beyond traditional legal purposes, the same techniques, scientific rigor, and procedural precision now support the range of military operations and courses of action, e.g., computer network operations as well as CI objectives. (DoDD 5505.13E, DoD Executive Agent for the DoD Cyber Crime Center, 1 Mar 2010) Also see *digital & multimedia forensics, digital evidence*, and *forensic science*.

-- Also, the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. (NIST, Glossary of Key Information Security Terms, May 2013)

Digital Tradecraft. The conduct, topics, or techniques of modern espionage or CI that employ digital or cyber means. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010 with change 1 dated 16 Oct 2013)

-- Also, digital or cyber tactics, techniques, and procedures designed to obscure or frustrate observation by hostile or unfriendly entities. (DoDI S-3325.10, [FOUO title], 6 Jun 2013)

Digraph and/or Trigraph. A two and/or three-letter acronym for the assigned Codeword or nickname. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Diplomatic and/or Consular Facility. Any Foreign Service establishment maintained by the US Department of State abroad. It may be designated a "mission" or "consular office," or given a special designation for particular purposes, such as "United States Liaison Office." A "mission" is designated as an embassy and is maintained in order to conduct normal continuing diplomatic relations between the US Government and other governments. A "consular office" is any consulate general or consulate that may participate in most foreign affairs activities, and varies in size and scope. (JP 1-02)

Diplomatic Establishment. A mission, consulate, embassy, residential compound, or other premises owned or leased and used by a government for official purposes. (Words of Intelligence, 2nd Edition, 2011)

Diplomatic Immunity. A status wherein diplomatic officers accredited to a foreign government as ambassadors, or other public ministers, are immune from the jurisdiction of all courts and tribunals of the receiving states whether criminal or civil. The status of diplomatic immunity protects the bearer from prosecution, civil suit, punishment, or compelled testimony in the country to which he or she is accredited. (Words of Intelligence, 2nd Edition, 2011)

Diplomatic Security. The set of measures enacted to ensure that the diplomatic representatives of a nation-state, kingdom, or other political entity are able to conduct that entity's foreign affairs in a confidential, safe manner. (US State Department) See *Department of State / Bureau of Diplomatic Security*.

> *Security is a basic function of diplomacy, and specific components of diplomatic security include preserving the confidentiality of diplomatic documents and communications, protecting diplomatic personnel, ensuring the integrity of diplomatic personnel through background investigations, and safeguarding diplomatic posts overseas and diplomatic facilities at home.*
>
> -- History of the Bureau of Diplomatic Security of the United States Department of State (October 2011) Copy at <http://www.state.gov/m/ds/rls/rpt/c47602.htm>

Direct Access. Descriptor used for sources with firsthand access to the information provided. (DoDI S-5200.42, Defense HUMINT and Related Intelligence Activities (U), 8 Dec 2009) Also see *indirect access*.

Direct Liaison Authorized (DIRLAUTH). That authority granted by a commander (any level) to a subordinate to directly consult or coordinate an action with a command or agency within or outside of the granting command. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Direct Support (DS). A mission requiring a force to support another specific force and authorizing it to answer directly to the supported force's request for assistance. (JP 1-02)

Direction Finding (DF). A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. (JP 1-02)

Director Defense Intelligence Agency (Dir DIA). Advises the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Combatant Commanders on all matters concerning all-source Defense Intelligence.

> Director DIA serves as the **Defense Counterintelligence Manager** [emphasis added], the Defense HUMINT Manager, the Defense Collection Manager…, and the Commander of the Joint Functional Component Command-Intelligence, Surveillance, and Reconnaissance (JFCC-ISR). See DoDD 5105.21, *DIA*, 18 Mar 2002.

Director of National Intelligence (DNI). Serves as the principal adviser to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security; oversees the 16 federal organizations that make up the intelligence community (IC); and manages the implementation of the National Intelligence Program (NIP). (IRTPA 2004)

> Office of the Director of National Intelligence (ODNI) is charged with: 1) integrating the domestic and foreign dimensions of US intelligence so that there are no gaps in our understanding of threats to our national security; 2) bringing more depth and accuracy to intelligence analysis; and 3) ensuring that US intelligence resources generate future capabilities as well as present results.
>
> DNI created by Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) in December 2004. The Office of the Director of National Intelligence (ODNI) began operations in April 2005. It was created to drive strategic integration, ensure better coordination, and provide oversight & governance of the Intelligence Community (IC).
>
> -- See ODNI Fact Sheet (Oct 2011): <http://www.dni.gov/files/documents/ODNI%20Fact%20Sheet_2011.pdf>

Dirty Bomb. An explosive-driven radiological dispersal device.

> See NRC fact sheet, "Dirty Bombs," May 2007(accessed 27 June 2011); available on line at: <http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs-bg.pdf>
>
> Also see Congressional Research Service (CRS) report R41890, "Dirty Bombs": Technical Background, Attack Prevention and Response, Issues for Congress," 24 June 2011.

Disaffected Person. A person who is alienated or estranged from those in authority or lacks loyalty to the government; a state of mind. (JP 1-02)

Discards. [S]pies supposedly deliberately sacrificed to distract a counterintelligence investigation away from a better target. This is a controversial strategy about which there remains much debate within the intelligence community… (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Discovery. Part of the pre-trial litigation process during which each party requests relevant information and documents from the other side in an attempt to "discover" pertinent facts. Generally discovery devices include depositions, interrogatories, requests for admissions, document production requests and requests for inspection. (<http://www.lectlaw.com/def/d058.htm>; accessed 18 Sep 2012)

Discoverability. Discoverability means users can "discover" selected values (e.g., who, what, where, when), but cannot gain access to the underlying information until the user requesting access is authorized and authenticated. (Markle Task Force, 1 Sep 2009)

> Discoverability is the first step in an effective system for information sharing, offering users the ability to "discover" data that exists elsewhere. Discoverability means users can "discover" selected values (e.g., who, what, where, when), but cannot gain access to the underlying information until the user requesting access is authorized and authenticated. In many ways, knowing where relevant information can be found or who has the information is the essential first step towards information sharing as this makes collaboration and analysis possible. A system of discoverability also avoids the bulk transfers of data required in large centralized databases, improving security and minimizing privacy risks.
>
> See: <http://www.markle.org/sites/default/files/MTFBrief_Discoverability.pdf>

Disguise. Concealment or misrepresentation of the physical characteristics or true nature or identity of a person or object. (CIA in D&D Lexicon, 1 May 2002)

Disinformation. Carefully contrived misinformation prepared by an intelligence or CI service for the purpose of misleading, deluding, disrupting, or undermining confidence in individuals, organizations, or governments. (CI Community Lexicon)

Dissemination. The timely distribution of intelligence products (oral, written, or graphic form) to departmental and agency intelligence Consumer's is a suitable format. (CI Community Glossary)

-- Also, the timely conveyance of intelligence in suitable form to customers. (ICS Glossary)

Dissemination and Integration. In intelligence usage, the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. Also see *intelligence process*. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Divided Loyalties. Broadly defined, individuals with intellectual or emotional commitments to another country through cultural affinity. (PERSEREC Technical Report 02-5, Espionage Against the United States by American Citizens 1947-2001, July 2002) Also see *ideology, MICE*.

DNA. The abbreviation for deoxyribonucleic acid, which is the genetic material present in the cells of all living organisms. DNA is the fundamental building block for an individual's entire genetic makeup. (www.ojp.usdoj.gov; accessed 29 Apr 2013)

> A person's DNA is the same in every cell (with a nucleus). DNA is contained in blood, semen, skin cells, tissue, organs, muscle, brain cells, bone, teeth, hair, saliva, mucus, perspiration, fingernails, urine, feces, etc.

Document and Media Exploitation (DOMEX). The processing, translation, analysis, and dissemination of collected hard copy documents and electronic media, which are under U.S. Government's physical control and are not publicly available; excludes: handling of documents and media during collection, initial review, and inventory process; and documents and media withheld from the IC DOMEX dissemination system in accordance with DNI-sanctioned agreements and policies to protect sources and methods. (ICD 302, Document and Media Exploitation, 6 Jul 2007) Also see *Document Exploitation* (*DOCEX), Harmony,* and *National Media Exploitation Center (NMEC)*.

-- Also, the processing, translation, analysis, and dissemination of collected hard-copy documents and electronic media that are under U.S. Government physical control and are not publicly available. In the Department of Defense this includes the handling of documents and media during their collection, initial review, inventory, and input to a database. (DoDD 3300.03, DoD DOMEX, 11 Jan 2011)

-- Also, the handling and exploitation of documents and/or media for intelligence purposes. (HDI Lexicon, April 2008)

> The National Media Exploitation Center (NMEC) is responsible for ensuring the rapid collection, processing, exploitation, dissemination and sharing of all acquired and seized media throughout the intelligence, counterintelligence, military and law enforcement communities. See ICD 302, copy available online at <http://www.fas.org/irp/dni/icd/icd-302.pdf>
>
> Director DIA is the IC Executive Agent for NMEC (DoDD 3300.03, *DoD DOMEX*, 11 Jan 2011)

Document Exploitation (DOCEX). The systematic extraction of information from all media formats is response to collection requirements. (Term previously defined in Army FM 2-0, Intelligence, May 2004) Also see *Document and Media Exploitation (DOMEX); Harmony;* and *NMEC.*

Doctrine. Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. (JP 1-02)

> *"Doctrine evolves from theory and concepts based on values, beliefs, historical perspective, experience, and research."*
>
> -- AR 600-100, *Army Leadership*, 8 Mar 2007

-- Also, *Joint Doctrine*: fundamental principles that guide the employment of US military forces in coordinated action toward a common objective. Joint doctrine contained in joint publications also includes terms, tactics, techniques, and procedures. It is authoritative but requires judgment in application. (JP 1-02)

DoD CI Campaign (previously referred to as "*DoD CI Strategic Campaign).* See the FOUO definition in O-DoDD 5240.02, Counterintelligence, 20 Dec 2007, with change 1 dated 30 Dec 2010; available on SIPRNet at <http://www.dtic.smil.mil/whs/directives/corres/pdf/524002p.pdf>

> DoD CI Campaigns drive and shape Defense CI engagement against critical foreign intelligence threats globally to achieve strategic outcomes; these CI Campaigns are managed by DIA's Office of Counterintelligence (OCI-1).

DoD Criminal Investigative Organizations. The term refers collectively to the United States Army Criminal Investigation Command, Naval Criminal Investigative Service, U.S. Air Force Office of Special Investigations, and Defense Criminal Investigative Service, Office of the IG DoD. (DoDD 5525.07)

DoD Functional Manager for Security Training. Director Defense Security Service (DSS).

DoD Law Enforcement Organizations. Organizations, agencies, entities, and offices of the Military Departments and Defense Agencies and the DoD Inspector General that perform a law enforcement function for those departments and agencies and are manned by DoD LEOs [Law Enforcement Officers]. (DoDI 2000.26, Suspicious Activity Reporting, 1 Nov 2011)

DoD Personnel Travel Clearance. Travel clearance for DoD and DoD-sponsored personnel performing official temporary travel abroad. The three types of clearance are country clearance, theater clearance, and special area clearance. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

DoD Strategic CI Campaign. See FOUO definition in O-DoDD 5240.02, CI, 20 Dec 2007.

DoD Unknown Subject. The subject of a DoD CI investigation whose identity has not been determined. (DoDI 5240.04, CI Investigations, 2 February 2009 with change 1 dated 15 Oct 2013) Also see *Defense Unknown Subject Team; Unknown Subject*.

> An "unknown subject" is commonly referred to as an "UNSUB."
>
> DIA's Office of Counterintelligence (OCI-2) serves as the focal point and central repository for DoD unknown subject CI leads, reports and information.

Domestic Activities. Activities within the United States that do not involve a significant connection with a foreign power, organization, or person. (AR 381-20, Army CI Program. 25 May 2010)

Domestic Intelligence. Intelligence relating to activities or conditions within the United States that threaten internal security and that might require the employment of troops; and intelligence relating to activities of individuals or agencies potentially or actually dangerous to the security of the Department of Defense. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011)

Domestic Terrorism. Terrorism perpetrated by the citizens of one country against persons in that country. This includes acts against citizens of a second country when they are in the host country, and not the principal or intended target. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013)

-- Also, Americans attacking Americans based on U.S.-based extremist ideologies. (FBI)

-- Also, domestic terrorists: people who commit crimes within the homeland and draw inspiration from U.S.-based extremist ideologies and movements. (CRS Report R42536, The Domestic Terrorist Threat: Background and Issues for Congress, 15 May 2012)

One particularly insidious concern that touches all forms of domestic extremism is the lone offender—a single individual driven to hateful attacks based on a particular set of beliefs without a larger group's knowledge or support. In some cases, these lone offenders may have tried to join a group but were kicked out for being too radical or simply left the group because they felt it wasn't extreme or violent enough. We believe most domestic attacks are carried out by lone offenders to promote their own grievances and agendas.

-- FBI at <http://www.fbi.gov/news/stories/2009/september/domterror_090709> (accessed 18 Dec 2012)

The Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) do not officially list domestic terrorist organizations, but they have openly delineated domestic terrorist "threats." These include individuals who commit crimes in the name of ideologies supporting animal rights, environmental rights, anarchism, white supremacy, anti-government ideals, black separatism, and anti-abortion beliefs.

-- CRS Report R42536, *The Domestic Terrorist Threat: Background and Issues for Congress*, 15 May 2012

Dossier. A file consisting of information concerning an individual. (National HUMINT Glossary)

Double Agent. Agent in contact with two opposing intelligence services, only one of which is aware of the double contact or quasi-intelligence services. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *dangle; dangle operation; provocation*.

No term is more misused by amateurs and greenhorns than "double agent."

-- William R. Johnson, Former Army Intelligence and CIA

In its simplest form, a double agent works for two intelligence services at the same time, with only one of the services understanding this.

-- Stuart A. Herrington, *Traitors Among Us: Inside the Spy Catcher's World* (1999), p. 132

The double agent is the most characteristic tool of counterespionage operations, and he comes in many guises.

-- Allan W. Dulles, The Craft of Intelligence (2006), p. 123

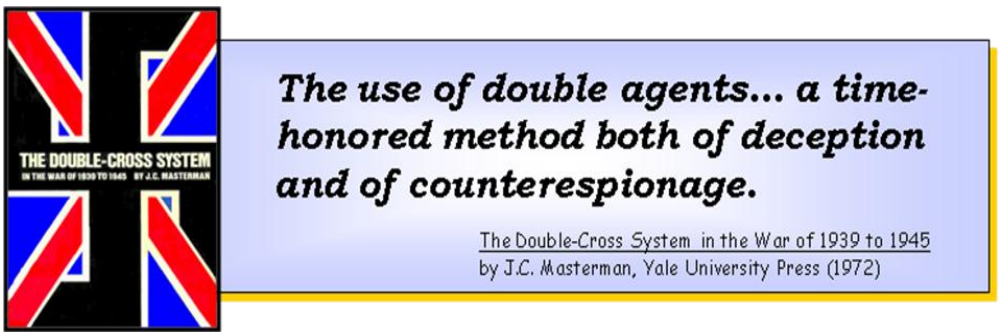
The first purpose of any double agent program is to engage the enemy. …The basic use of double agents is to keep contact with the enemy. What you use that contact for depends on the state of your CI program at any moment. But without contact, there isn't much you can do.

A double agent operation is a channel in which information moves in both directions. On each end of the channel is an intelligence or counterintelligence service. The intelligence service seeks to ensure that the flow of material through the channel is beneficial to itself. The CI service seeks to ensure that the flow of material is detrimental to its opponent.

-- William R. Johnson (Former CIA Officer)

The caviar of the intelligence business.

-- James M. Olson, Former Chief of CIA Counterintelligence



-- Also, an agent who is cooperating with an intelligence service of one government on behalf of and under the control of an intelligence or security service of another government, and is manipulated by one to the detriment of the other. (Glossary of Intelligence Terms and Definitions, IC Staff, 1978)

-- Also, a person pretending to work as a spy for one government while actually working as [an asset] for another government. (WMD Report, 31 Mar 2005)

-- Also, an agent working for two opposing agencies; he is loyal to one while betraying the other. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

-- Also, *double agents* – individuals under the control of one intelligence agency who offer their services to an opposing intelligence agency. ("Double Agent Operations," *Espionage*, Naval Investigative Service Command; nd, circa 1989)

-- Also, a clandestine operative who works for two opposing espionage organizations but who is loyal to one of the organizations and betrays the other. (*Encyclopedia of the CIA*, 2003)

-- Also, a person who engages in clandestine activity for two intelligence or security services (or more in joint operations), who provides information about one or about each to the other, and who wittingly withholds significant information from one on the instructions of the other or is unwittingly manipulated by one so that significant facts are withheld from the adversary. (John P. Dimmer - 1962; see below)

A World of Stratagems

"To tackle enemy espionage (whoever the enemy may turn out to be) it is therefore of paramount importance to keep a firm hold on the enemy's own system of agents and informers. Knowledge of his methods, knowledge of his intentions, and knowledge of the personnel of his organization are all vitally necessary. Surely all these objects are the best attained by the maintenance of double agents! The confession of faith is consequently a simple one. It amounts to this: that ***in peace as well as in war a carefully cultivated double agent system is the safest and surest weapon of counterespionage*** *[emphasis added], and the one most easily adaptable to changing conditions, changing problems, and even changing enemies."*

-- J.C. Masterman, *The Double-Cross System* (1972)

The term "double agents" as used during OSS operations in WWII: *"…captured agents who would be persuaded to continue their activities for the enemy, ostensibly in good faith but acting at the direction of X-2 [OSS Counterintelligence]…."* Also *"the case of an agent recruited by X-2 [OSS CI] and infiltrated into enemy territory to induce the enemy to employ him as an agent and return him to Allied territory."*

-- Kermit Roosevelt, *War Report of the OSS* (1976)

"The fact that doubles have an agent relationship with both sides distinguishes them from penetrations, who normally are placed with the target service in a staff or officer capacity…. The double agent is one of the most demanding and complex counterintelligence activities in which an intelligence service can engage. Directing even one double agent is a time-consuming and tricky undertaking that should be attempted only by a service having both competence and sophistication."

-- John P. Dimmer, CIA (1962)

"One side has a agent whom it deliberately tries to work in as an agent on the other side, of course without the other knowing anything about it… the most advanced and dangerous kind of work an agent can do, both for the agent himself and for the two parties."

-- Colonel Stig Erik Constans Wennerström, Swedish Air Force
Spy for the GRU -- convicted of treason in 1964

Note: For a full account of the Wennerström affair see *An Agent in Place* by Thomas Whiteside (1966), republished in 1983 in Ballantine Intelligence Library

---

Double Agents *"can serve as excellent channels through which misleading information can flow to the enemy. So double agents serve both as collectors of positive intelligence and channels for deception."*

-- Church Committee (Senate Report 94-755 , 26 April 1976)

A condoned channel of communication with the enemy

For additional open source information regarding double agents see:

William R. Johnson, *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer,* Georgetown University Press *(*2009); pp. 91-153.

Federal Government Security Clearance Programs, Report # 99-166, Hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, US Senate, April 1985, specifically testimony on pp. 63-103 regarding two Army CI controlled double agent operations: 1) Chief Warrant Officer Jamos Szmolka against the Hungarian Intelligence Service in 1977-1981; and 2) Sergeant "Smith" against the KGB for over 10 years starting in the early 1970's.

"Double Agent Operations*," Espionage*, Naval Investigative Service Command (nd, circa 1989); pp. 24-33.

John P. Dimmer (aka F.M. Begum), "Observations on the Double Agent," *Studies in Intelligence*, V6: 11, pp 57-72 (1962); declassified, originally classified Secret. Available online at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol6no1/html/v06i1a05p_0001.htm>

J.C. Masterman, *The Double-Cross System* (1972). Double agent operations against the Germans in World War II. Nazi agents in Britain were captured or turned themselves in and were then used by the British to broadcast mainly disinformation to their Nazi controllers.

John Barron, *Operation Solo: The FBI's Man in the Kremlin* (1996). Operation Solo tells the remarkable and true story of FBI run double agent Morris Childs, code named "Agent 58", who, for twenty-seven years, provided the FBI with the Kremlin's innermost secrets during fifty-two clandestine missions to the Soviet Union, China, and Eastern Europe.

David Wise, *Cassidy's Run* (2000). True-life story of US Army Sgt. Joseph Cassidy who successfully pretended to be a traitor to his country. In the eyes of his Soviet handlers, he was a mole planted deep inside DoD. This US Army/FBI double agent operation – code named Operation SHOCKER -- flushed out 10 Soviet spies including a Russian sleeper agent in the Bronx and revealed the lengths to which Soviet intelligence would go to penetrate DoD.

Andrew Tully, *Inside the FBI* (1980). Chapter 5 "Spies for Sale" (pp. 70-81) tells the story of a joint Naval Investigative Service and FBI double agent operation [Operation LEMONAID] targeting the Russian Intelligence Service resulting in the arrest of three Russians working out of the United Nations for espionage on 20 May 1978. Also see Jeremy J. Leggatt, "Art Lindberg's Walk in the Cold," *Reader's Digest*, June 1980.

Downgrade. To determine that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a lower degree. (JP 1-02)

Doxing. [Cyber usage] Publicly releasing a person's identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

Dry Clean. [Tradecraft jargon] Actions taken to determine if one is under surveillance. (Spy Book)

Dry Cleaning. [Tradecraft jargon] Any technique used to elude surveillance. A usual precaution used by intelligence personnel when actively engaged in an operation. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, any technique used to detect surveillance; a usual precaution engaged in by intelligence personnel when actively engaged in an operation. (FBI FCI Terms)

Dynamic Threat Assessment (DTA). An intelligence assessment developed by the Defense Intelligence Agency that details the threat, capabilities, and intentions of adversaries in each of the priority plans in the Joint Strategic Capabilities Plan. (JP 2-0, Joint Intelligence, 22 Oct 2013)

> The DTA is used by the Combatant Commanders and COCOM planning staffs to conduct Mission Analysis for Step 1 - Strategic Guidance under Adaptive Planning and Execution (APEX).

Dual Agent. *Within DoD, term rescinded by JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011.*

> Previously defined in JP 1-02 as "one who is simultaneously and independently employed by two or more intelligence agencies, covering targets for both."

Dual Citizen. Any person who is simultaneously a citizen of more than one country. (DSS Glossary)

Dual-use. Technology and articles that are potentially used either for commercial/civilian purposes or for military, defense, or defense-related purposes. (DoDI 2040.02, International Transfers of Technology, Articles, and Services, 10 Jul 2008) See *critical technology*.

DUST. See *Defense Unknown Subject Team*.

E ==========

Economic Espionage. The knowing misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent. Misappropriation includes, but is not limited to, stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to obtain trade secrets without authorization. (Economic Espionage Act of 1996, PL 104-294)

Economic Espionage… is a fact of life

I think you have to separate very clearly what are the fields which are covered by the alliance and the fields which are not covered by an alliance. It's clear that when you are allies, you have certain sectors, I'm speaking of the armaments. I'm thinking of diplomatic matters where normally you should not try to gather intelligence. But in all of the other fields, being allied does not prevent the states from being competitors. Even during the Cold War, the economic competition existed. Now the competition between the states is moving from the political-military level to the economic and technological level. ***In economics, we are competitors, not allies.*** *I think that even during the Cold War getting intelligence on economic, technological, and industrial matters from a country with which you are allies is not incompatible with the fact that you are allies.*

-- Pierre Marion, Former Director of French Intelligence (DGSE)
as quoted in *Friendly Spies* by Peter Schweizer (1993)

Section 101(a) of the Economic Espionage Act of 1996 criminalizes economic espionage.
See <http://www.gpo.gov/fdsys/pkg/PLAW-104publ294/content-detail.html>
Also see <http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage>

The **Economic Espionage Act (EEA) of 1996** (18 USC §§ 1831-1839) is concerned in particular with economic espionage and foreign activities to acquire US trade secrets. In this context, trade secrets are all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether stored or unstored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing, if the owner (the person or entity in whom or in which rightful legal or equitable title to, or license in, is reposed) has taken reasonable measures to keep such information secret and the information derives independent economic value, actual, or potential from not being generally known to, and not being readily ascertainable through, proper means by the public. Activities to acquire these secrets include the criminal offenses: economic espionage and industrial espionage.

The Office of the National Counterintelligence Executive submits an annual report to Congress on the threat to the United States from foreign economic collection and industrial espionage; see annual reports at: <http://www.ncix.gov/publications/reports/fecie_all/index.html>

"US intelligence officials put the cost of lost sales due to illicit appropriation of technology and business ideas at between $US100 billion and $US250 billion a year."

-- *Financial Times*, January 2011

Educing Information (EI). The full range of approaches to obtain useful information from sources. EI includes elicitation, debriefing, and interrogation. (*Educing Information – Interrogation: Science and Art*, Dec 2006) Also see *debriefing; elicitation; interrogation; interview*.

The 2006 Intelligence Science Board report *Educing Information – Interrogation: Science and Art* is available online at <http://www.ndic.edu/press/3866.htm>

Effect. 1) The physical or behavioral state of a system that results from an action, a set of actions, or another effect; 2) The result, outcome, or consequence of an action; 3) A change to a condition, behavior, or degree of freedom. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Effects-Based Operations (EBO). [Non-doctrinal term] A process for obtaining a **desired strategic outcome** [emphasis added] or *effect* on the enemy. (JFCOM Glossary at www.jfcom.mil/about/glossary.htm)

> Effects Bases Operations: *Coordinated sets of actions directed at shaping the behavior of friends, foes, and neutrals in peace, crisis, and war.*
>
> *The concept of EBO focuses "coordinated sets of actions" on objectives defined in terms of human behaviors in multiple dimensions and on multiple levels, and measures their success in terms of the behavior produced…. Effects cannot be isolated. All effects, at each level and in each arena, are interrelated and are cumulative over time. And lastly, effects are both physical and psychological in nature.*
>
> -- Edward A. Smith, *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War* (2002)

eGuardian. The FBI's unclassified, law enforcement-centric threat reporting system. It provides a means to disseminate SARs dealing with information regarding a potential threat or suspicious activity rapidly throughout the national law enforcement community. (DoDI 2000.26, Suspicious Activity Reporting, 1 Nov 2011) See *suspicious activity report*.

> All reports in the eGuardian system Shared Data Repository are viewable through Guardian, the FBI's classified threat reporting system. DoD personnel assigned to Joint Terrorism Task Forces (JTTFs) and the National Joint Terrorism Task Force (NJTTF) have access to Guardian.
>
> For additional information see: <http://foia.fbi.gov/eguardian_threat.htm>

Electronic Intelligence (ELINT). Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JP 1-02 and JP 3-13.1, Electronic Warfare, 25 Jan 2007) Also see *electronic warfare; foreign instrumentation signals intelligence; signals intelligence.*

> ELINT is a sub-category of signals intelligence (SIGINT) that engages in dealing with information derived primarily from electronic signals that do not contain speech or text (which are considered Communications Intelligence aka COMINT). Two major branches of ELINT are Technical ELINT (TechELINT) and Operational ELINT (OpELINT) described as follows:
>
> -- TechELINT describes the signal structure, emission characteristics, modes of operation, emitter functions, and weapons systems associations of such emitters as radars, beacons, jammers, and navigational signals. A main purpose of TechELINT is to obtain signal parameters which can define the capabilities and the role that the emitter plays in the larger system, such as a ground radar locating aircraft, and thus lead to the design of radar detection, countermeasure, or counterweapons equipment.
>
> -- OpELINT concentrates on locating specific ELINT targets and determining the operational patterns of the systems; these results are commonly called Electronic Order of Battle (EOB).
>
> For additional information see: Richard L. Bernard, *Electronic Intelligence (ELINT) at NSA*, 2009. On line at: <http://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/elint.pdf>
>
> Also see additional background information at: <www.fas.org/irp/nsa/almanac-elint.pdf>

Electronic Surveillance. The acquisition of a nonpublic communication by electronic means without the consent of a person who is party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication. (DoD 5240.1-R, Dec 1982) Also see *surveillance; foreign intelligence surveillance act (FISA).*

> Governed by the Foreign Intelligence Surveillance Act (FISA) of 1978 (50 USC §1805).
>
> For DoD CI see Chap 5. Proc 5 – Electronic Surveillance, DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, 7 Dec 1982

The Electronic Communications Privacy Act of 1986 (ECPA) prohibits unauthorized electronic eavesdropping**.** ECPA consists of three parts. The first, often referred to as Title III, outlaws wiretapping and electronic eavesdropping, except as otherwise provided. The second, the Stored Communications Act, governs the privacy of, and government access to, the content of electronic communications and to related records. The third outlaws the use and installation of pen registers and of trap and trace devices, unless judicially approved for law enforcement or intelligence gathering purposes.

-- Also, the use of electronic devices to monitor or record conversations, activities, sound, or electronic impulses. (Army FM 2-22.2, Counterintelligence, Oct 2009)

-- Also, (ELSUR) under Title III and FISA is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

Electronic Tracking Device. Direction finder including electronic tracking devices, such as, radio frequency beacons and transmitters, vehicle locator units, and the various devices that use a Global Positioning System [GPS] or other satellite system for monitoring non-communication activity. (FBI Domestic Investigations and Operations Guide, 16 Dec 2008)

Electronic Warfare (EW). Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support. (JP 1-02 and JP 3-13.1, Electronic Warfare, 25 Jan 2007)

Electronics Security. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar. (JP 1-02 and JP 3-13.1, Electronic Warfare, 25 Jan 2007)

Elements of Espionage. The fundamentals components in which an intelligence service conducts espionage… some or all of the following elements are present in every espionage operation: 1) contact & communication; 2) collection; 3) motive / reward; 4 travel; and 5) tradecraft. (*Espionage 101: Elements of Espionage*, US Army AFCITC Course Handout, 3 Dec 1996, authored by CW4 Constance Y. Huff, USA) Also see *Espionage; Espionage Act; Espionage Against the United States.*

Espionage *investigative elements* are different than the *prosecutorial elements* (which are addressed in Title 18 USC, §§ 792-798 and Article 106, UCMJ).

Elicitation. In intelligence usage, the acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *educing information; debriefing; interrogation; interview.*

-- Also, engaging with a source in such a manner that he or she reveals information without being aware of giving away anything of value. (Educing Information – Interrogation: Science and Art, Dec 2006)

-- Also, the strategic use of conversation to extract information from people without giving them the feeling they are being interrogated. (FBI)

-- Also, the use of generalized questions to ascertain someone's knowledge on a particular topic. (Army FM 2-22.2, Counterintelligence, Oct 2009

A casual conversation with a hidden agenda

The subtle extraction of information during an apparently "normal" and "innocent" conversation. A supplemental technique used during interviews, debriefings and interrogations.

Elicitation is the practice of obtaining information about a topic from conversations, preferably without the source knowing what is happening.

-- Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (2004), p. 72

Elicitation, that is to say, like a lot of other tradecraft techniques, has its Scylla and Charybdis. On one hand, the cautious seeker risks concealing his purpose in such general questions or remarks that he evokes nothing of value. On the other hand, if the questions are excessively direct, the contact may quickly suspect he is being interrogated for intelligence purposes and bring the interview to an abrupt and unpleasant end.

-- George G. Bull, "The Elicitation Interview," *Studies in Intelligence*, vol. 14 no. 2 (Fall 1970), pp. 115-22. Originally classified "Secret" [declassified].

Elicitation is a technique used to discreetly gather information. It is a conversation with a specific purpose: collect information that is not readily available and do so without raising suspicion that specific facts are being sought. It is usually non-threatening, easy to disguise, deniable, and effective. The conversation can be in person, over the phone, or in writing. Conducted by a skilled collector, elicitation will appear to be normal social or professional conversation. A person may never realize she was the target of elicitation or that she provided meaningful information.

-- *Elicitation Techniques*, FBI (accessed 20 Aug 2012)
See pdf available at: <http://www.fbi.gov/about-us/investigate/counterintelligence/elicitation-brochure>

Emanation Security. Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information systems. Synonymous with Transient Electromagnetic Pulse Emanation Standard (TEMPEST). (DSS Glossary) Also see *TEMPEST.*

Emerging Warning Concerns. Newly identified issues relevant to national security of sufficient significance to warrant temporary attention by the Defense Intelligence Enterprise. An emerging warning issue may be redefined as an enduring warning issue based on national security priorities and operational plans. (DoDD 3115.16, The Defense Warning Network,5 Dec 2013)

Émigré. A person who lawfully departed his or her country with the intention of resettlement elsewhere. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, a person who departs from his country for any lawful reason with the intention of permanently resettling elsewhere. (ICS Glossary)

Emission Security. The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptoequipment and telecommunications systems. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010). Also see also *communications security*.

Equipment Exploitation Operations. Intelligence exploitation operations of all types foreign and non-foreign material which may have military application or answer a collection requirement. This material includes material found on a detainee or on the battlefield (Captured Enemy Equipment (CEE)), or purchased through either open or clandestine means (Foreign Military Acquisition). (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Enabling Activities. [In CI and HUMINT usage] Any activity that supports Defense CI and HUMINT operations, functions, and missions, including source validation, collection management, collection requirements management, cover, cover support, information systems, production management, source communications, targeting, and training. (DoDI O-5100.93, Defense CI & HUMINT Center, 13 Aug 2010)

Encipher. To convert plain text into unintelligible form by means of a cipher system. (JP 1-02)

-- Also, convert plain text to cipher text by means of a cryptographic system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Encode. Convert plain text to cipher text by means of a code. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Encrypt. Generic term encompassing encipher and encode. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Encryption. The process of changing plaintext into ciphertext for the purpose of security or privacy. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

End State. Set of required conditions that defines achievement of the commander's objectives. (JP 1-02)

Enduring Warning Issue. A significant national security issue, usually linked to an operation plan or concept plan, that is well defined and are longstanding potential threats to the interests of the U.S. and its allies. (DoDD 3115.16, The Defense Warning Network,5 Dec 2013)

Enemy Combatant (EC). A person engaged in hostilities against the United States or its coalition partners during an armed conflict. (DoDD 2310.01E and JP 3-56, Detainee Operations, 6 Feb 2008)

Esoteric Communications. Public statements whose surface meaning (manifest content) does not reveal the real purpose, meaning, or significance (latent content) of the author. (Army Techniques Publication 2-22.9, Open-Source Intelligence, 10 Jul 2012)

Espionage. Intelligence activity directed towards the acquisition of information through clandestine means. (NSCID 5 and DCID 5/1) Also see *Elements of Espionage*; *Espionage Act*; *Espionage Against the United States*.

> **"*The object of secret intelligence activity [espionage] is to obtain by secret means information which cannot otherwise be secured and which is not elsewhere available.*"**
> -- Kermit Roosevelt, *War Report of the OSS* (1976)

> "*In espionage, two factors are constant. Intelligence officers recruit foreign nationals who can provide classified information on their governments' plans and intentions, and the counterintelligence services of those countries try to thwart these operations.*"
> -- Brian P. Fairchild (CIA Case Officer for 20 years), *"Human Intelligence, Operational Security and the CIA's Directorate of Operations."* Statement before the Joint Economic Committee, United States Congress 20 May 1998

-- Also, 1) Intelligence activity directed toward the acquisition [of] information through clandestine means and proscribed by the laws of the country against which it is committed; 2) Overt, cover, or clandestine activity designed to obtain information relating to the national defense with an intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation. (CI Community Lexicon)

-- Also, Clandestine intelligence activity. This term is often interchanged with "clandestine collection." (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- Also, 1) The art of spying; 2) The act of seeking information for one government that the other government wishes to keep secret. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

> Espionage is the clandestine collection of information by people either in a position of trust for the targeted entity, or with access to people with such access. The process of recruiting such individuals and supporting their operations is the HUMINT discipline of *agent handling*.

_____

"Espionage—the use of spies or secret agents to steal information from enemies, adversaries, or competitors—is one of the oldest forms of intelligence gathering."

-- Arthur S. Hulnick, "Espionage: Does It Have a Future in the 21st Century?" *The Brown Journal of World Affairs;* XI: 1 (2004)

_____

"Espionage is distinguished from other forms of intelligence gathering by its clandestinity and its 'illegal means' of acquisition."

-- Frederick P. Hitz, Former Inspector General of the CIA (1990-1998)

_____

"Espionage is the theft of information in contravention of another nation's laws by a person known as an 'agent.' This act of theft may be direct, as in the secret copying of a classified document, or the indirect, as in hiding of an eavesdropping device, or merely oral, but is done by an agent and it breaks either a foreign law or the internal regulation of an alien organization. Espionage is not the confidential purchase of information where mere embarrassment, rather than illegality, is risked. It is not the flattery, bribery, or coercion of a person to influence his actions within legal limits. It is not 'a scuttling, violence-prone business. . . incompatible with democracy.' But rather a silent, surreptitious, violence-shunning business serving the nation."

-- William R. Johnson, "Clandestinity and Current Intelligence," *Studies in Intelligence*, vol. 20, no. 3 (Fall 1976), pp. 15-69. Originally classified "Secret / No Foreign Dissem" [declassified].

Espionage, since it is based on human vulnerability, can penetrate even the most heavily guarded repositories of national secrets.

-- Also, [*Crime of Espionage*] the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Espionage is a national security crime, specifically a violation of Title 18 USC, §§ 792-798 and Article 106, Uniform Code of Military Justice (UCMJ).

See article *"Espionage: The American Judicial Response. An in Depth Analysis of the Espionage Laws and Related Statues"* by Harold W. Bank (45 pages).
Copy at <http://www.wcl.american.edu/journal/lawrev/21/bank.pdf.> (accessed 31 Oct 2012)

_____

"The man engaged in espionage on behalf of his own country is committing a patriotic act. The man who gives away or sells his own country's secrets is committing treason."

-- Allen W. Dulles, *The Craft of Intelligence* (2006), p. 179

_____

"Espionage is a crime almost devoid of evidence…"

-- Peter Wright (Former Asst Director MI5), *Spycatcher* (1987)

_____

"*The act of espionage is unlike any other criminal act in that it leaves no traces. Indeed, unless the agent is caught, the government office that has been penetrated is usually unaware that any crime has taken place. The actual detection of espionage is a very specialized task…."*

-- Miles Copeland, *Without Cloak or Dagger* (1974), p. 160

_____

"*...[E]spionage in it's own way is a very unique crime: There are no smoking guns, no battered victims, rarely do we have any forensic evidence, no bait money, no exploding dye packs, no bank surveillance films. Espionage, in many cases, leaves no footprints."*

-- William H. Webster, Director FBI (12/10/85)

_____

"Because it leaves no footprints, espionage is one of the more difficult crimes to uncover. Yet the business of catching spies affects profoundly the American way of life. If done well, it protects our freedoms by keeping us strong. If done poorly, it can impinge on our liberties just as surely as a takeover by a foreign power."

-- Ronald Kessler, *Spy vs. Spy* (1988), p. 8

"... the essence of espionage, even the most innocuous sort, is betrayal of trust. One might almost say that is the defining element, because without it, there is no espionage."

-- Aldrich Ames, CIA Traitor & Convicted Spy
as quoted in as quoted in *Confessions of a Spy* by Pete Earley

---

"Espionage is a crime of double-edged secrecy. Spies, well experienced in clandestine procedures and operating not as individuals but as agents of a nation, are hard to detect by traditional police work. And the loot that they seek is not the kind of evidence that can be labeled Exhibit A in the courtroom. …And there is still another kind of secret that a trail reveals: the failings of the secret-holder's own security safeguards"

-- Thomas B. Allen and Norman Polmar, *Merchants of Treason: America's Secret for Sale* (1988), p. 163

"No matter how overwhelming the evidence can be, prosecuting espionage cases is never easy."

-- John L. Martin, Retired Chief Counterespionage Section, US Department of Justice

Espionage Act. The Espionage Act of 1917 (18 USC § 792 et seq.) is a U.S. federal law passed in June 1917, shortly after the U.S. entry into World War I. It prohibited any attempt to interfere with military operations, to support U.S. enemies during wartime, to promote insubordination in the military, or to interfere with military recruitment. The law was further strengthen by the *Espionage and Sabotage Act of 1954*, which authorized the death penalty or life imprisonment for espionage or sabotage in peacetime as well as during wartime. The Act requires agents of foreign governments to register with the U.S. Government. It also suspended the statue of limitations for treason. In 1958, the scope of the act was broaden to cover Americans engaged in espionage against the U.S. while overseas. Also see *espionage.*

Statues now governing espionage date from the first effort to protect the governments' secrets in the Defense Secrets Act of 1911. The Espionage Act of 1917 adopted the approach take in 1911, incorporating many of its key phrases. Most of the 1917 act in turn has been incorporated without many revisions into 18 U.S. Code 793, the core statute for dealing with espionage. The last revisions in wording made to section 793 were in 1950 with the Internal Security Act; also in that act 18 U.S. Code 794 was added.

-- PERSEREC Technical Report 08-05, *Changes in Espionage by Americans: 1947-2007*, March 2008.

The Federal Espionage Laws codified in Title 18 Section 793 and 794 US Code along with other related crimes date back to the terrorist attack of 1916 on Black Tom Island carried out by the German IIIb intelligence service. This event had such an impact on the nation that proposals were made to court martial civilians since there were no viable laws to deal with espionage at the time.

The result was the 1917 Espionage Law of which codified a very restricted definition of the crime of Espionage. As you know espionage has four elements:

- *Unauthorized transmittal*
- *of national defense information*
- *to a foreign power or agent*
- *with the intent to harm the US or aid that foreign power.*

As a result of a German espionage case in the early 1940s, that was appealed, and precedence was established that the national defense security information transmitted in an espionage case had to be protected information. Accordingly, it is essential to prove in an espionage prosecution that the information affected the military defense of the United States and was protected information not in the public domain at the time it was transmitted.

-- Prepared Statement of David G. Major, President CI Centre, before the US House of Representatives, Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security "Enforcement of Federal Espionage Laws" Hearing, 29 January 2008

Prominent among the statutory offenses enacted by Congress and relating to matters of national security are the espionage laws found in title 18, sections 791 through 798.' The activities covered therein by these sections go far beyond those limited to any dictionary definition or popular concept of the term "espionage."

The obtaining of national defense information for the benefit or use of foreign nations or its subsequent transmittal is the primary target of the espionage laws. However, equally as criminal is the conspiracy and attempt to do any of the above as well as the receiving or obtaining of national defense information with reason to believe that such information was to be used in violation of the espionage laws. In addition, the willful refusal to turn over national defense information upon proper demand by lawful authority and the loss or compromise of national defense information through gross negligence is also included in the statutory proscription. The penalties prescribed for violation of the espionage laws are severe.

-- Commission on Government Security – 1957, p. 617

Espionage Indicators. Warning signs that an insider may be working for or is susceptible to control by a Foreign Intelligence Entity (FIE). These warning signs are the result of an insider's actions, activities, and behaviors that may be indicative of potential espionage-related activity. Also see *indicator*.

-- Also, Potential Espionage Indicators: Activities, behavior or circumstances that may, unless satisfactorily explained, be indicative of potential espionage activity by an individual who may be acting as a witting espionage agent or spy. (DSS CI Report, Potential Espionage Indicators in Personnel Security Investigations, undated, circa early 2000)

Mere exhibition of an espionage indicator does not necessarily indicate spying or a Foreign Intelligence Entity (FIE) connection; individuals may exhibit PEI for a variety of legitimate reasons. Presence of PEI, especially multiple PEI, warrants further CI action.

In CI usage, ***Indicators are different from anomalies.*** Espionage indicators are manifested in an insider's actions, activities, and behaviors whereas anomalies surface as a result of FIE actions and activities [see *anomalies, anomalous activity, anomaly*].

-- Indicator: an individual's action, activity or behavior
-- Anomaly: foreign power activity or knowledge

Potential Espionage Indicators alone do not presuppose that an individual is necessarily working on behalf of a FIE… additional CI follow-up is required.

DoD Directive 5240.06, *Counterintelligence Awareness and Reporting*, 17 May 2011, lists reportable contacts , activities, indicators, and behaviors associated with foreign intelligence activities (FIEs), a term that includes international terrorists; for specifics see Tables 1-3 at Enclosure 4.

Essential Elements of Information (EEI). The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Essential Elements of Friendly Information (EEFI). Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. (Previously in JP 2-01, Joint and National Intelligence Support to Military Operations)

Essential Task. A specified or implied task that an organization must perform to accomplish the mission that is typically included in the mission statement. (JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *implied task; specified task*.

Estimative Intelligence. Intelligence that identifies, describes, and forecasts adversary capabilities and the implications for planning and executing military operations. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Evaluation. In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. (JP 1-02)

Evaluation and Feedback. In intelligence usage, continuous assessment of intelligence operations throughout the intelligence process to ensure that the commander's intelligence requirements are being met. (JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Evidence. Testimony, writings, material object, or other things presented to the senses that are offered to prove the existence or nonexistence of a fact.

"***No matter how overwhelming the evidence can be, prosecuting espionage cases is never easy."***

-- John L. Martin, Retired Chief of Internal Security at the Department of Justice

In legal proceedings there are several different types: 1) in terms of their relationship to the crime, they are known as "direct" or "circumstantial," and 2) in terms of their relationship to the world at large, they are known as "testimonial" or "physical."

TESTIMONIAL: statements or the spoken word from the victim(s) or witness(es).

PHYSICAL: includes such things as hairs, fibers, latent fingerprints, and biological material. Physical evidence is objective and when documented, collected, and preserved properly may be the only definitive way to reliably place or link someone to a crime scene. This is why Physical evidence is known as the "silent witness."

Physical evidence has the potential to play a critical role in the overall investigation and resolution of a suspected criminal act.

-- US Department of Justice,
Crime Scene Investigation: A Guide for Law Enforcement, January 2000

-- Also, anything that helps to ascertain the truth of a matter, or gives proof of a fact. Evidence may be physical or testimonial. (AR 195-5, Evidence Procedures, 25 Jun 2007)

-- Also, the legal data that conclusions or judgments may be based on. It is the documentary or verbal statements and material objects admissible as testimony in a court of law. Evidence is the means by which any alleged matter of fact is proven or disproved. Evidence includes all matters, except comment or argument, legally submitted to a court. Evidence is the source from which a court-martial or jury must form its conclusions as to the guilt or innocence of an accused. *Testimonial evidence*, e.g., sworn statements of eyewitness accounts and admissions of guilt, is obtained through communication with people. *Physical evidence*, e.g., identified weapons and fingerprints, is obtained by searching crime scenes, tracing leads, and developing technical data. Investigators must always be evidence conscious. Both physical and testimonial evidence are vital to the successful prosecution of an investigation. (Army FM 3-19.13, Law Enforcement Investigations, Jan 2005)

Evidence is the source from which a court-martial or jury must form its conclusions as to the guilt or innocence of an accused. Evidence is the means by which any alleged matter of fact is proven or disproved. Evidence includes all matters, except comment or argument, legally submitted to a court.

-- Army FM 3-19.13, *Law Enforcement Investigations*, Jan 2005, p. 1-8

-- Also, evidence in its broadest sense, refers to anything that is used to determine or demonstrate the truth of an assertion; the term has specialized meanings when used with respect to specific fields, such as criminal investigations and legal discourse. …Legal evidence concerns the tight rules governing the presentation of facts that tend to prove or disprove the point at issue. …Testimony (which tells) and exhibits (which show) are the two main categories of evidence presented at a trial or hearing. (Wikipedia; accessed 1 Aug 2007)

The law of evidence governs the use of testimony (e.g., oral or written statements, such as an affidavit) and exhibits (e.g., physical objects) or other documentary material which is admissible (i.e., allowed to be considered by the trier of fact, such as a jury) in a judicial or administrative proceeding (e.g., a court of law). Evidence must be acquired/received, processed, safeguarded and disposed of properly.

Military Rules of Evidence are Part III of the *Manual for Courts-Martial*; Appendix 22 of the MCM is Analysis of the Military Rules of Evidence.

Also see "Evidence" in Chapter 8 of Army FM 2-22.2, *Counterintelligence*, October 2009, pp. 8-5 through 8-8.

_____

*"Espionage is a crime **almost** devoid of evidence…"*
-- Peter Wright, *Spycatcher* (1987)

_____

"*While espionage may be **ALMOST** devoid of evidence, it is **NOT VOID** of evidence."*
-- *ESPIONAGE 101: Elements of Espionage* by CW4 Connie Huff (USA), 3 Dec 1996

Evidence Identifiers. Tape, labels, containers, and string tags used to identify the evidence, the person collecting the evidence, the date the evidence was gathered, basic criminal offense information, and a brief description of the pertinent evidence. (Crime Scene Investigation: A Guide for Law Enforcement, Sep 2013)

Execute Order (EXORD). 1) An order issued by the Chairman of the Joint Chiefs of Staff, by the authority and at the direction of the Secretary of the Defense, to implement a decision by the President or SECDEF to initiate military operations; 2) An order to initiate military operations as directed. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Execution Planning. The Adaptive Planning and Execution System translation of an approved course of action into an executable plan of action through the preparation of a complete operation plan or operation order. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Executive Agent (EA) [within DoD]. A term used to indicate a delegation of authority by the Secretary of Defense or Deputy Secretary of Defense to a subordinate to act on behalf of the Secretary of Defense. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Exfiltration. The removal of personnel or units from areas under enemy control by stealth, deception, surprise, or clandestine means. (JP 1-02)

-- Also, a clandestine rescue operation designed to get a defector, refugee, or operative and his or her family out of harm's way. (CI Centre Glossary)

-- Also, a clandestine operation undertaken to remove an individual from a denied area. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

-- Also, the surreptitious extraction of operatives in the field. (*Encyclopedia of the CIA*, 2003)

-- Also, an operation to get an individual secretly and illegally [in violation of a foreign country's law] out of a hostile area. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

> Examples include the escapes of KGB officer Oleg Gordievsky from the Soviet Union in 1985, orchestrated by MI6, and KGB officer Victor Sheymov, his wife, and daughter from the Soviet Union in 1980, carried out by the CIA.

Expanded-scope Screening [Polygraph]. (ESS) An examination that includes the questions from a CSP polygraph and questions related to falsification of security forms, involvement with illegal drugs, and criminal activity. Previously known as full-scope polygraph. (DoDI 5210.91, PCA Procedures, 12 Aug 2010 with change 1 dated 15 Oct 2013)

Exploitation. The process of obtaining information from any source and taking advantage of it. (DoDD 5205.02E, DoD OPSEC Program, 20 Jun 2012)

-- Also, the process of obtaining intelligence information from any source and taking advantage of it for intelligence purposes. (ODNI, U.S. National Intelligence – An Overview 2011)

Export Enforcement Coordination Center (E2C2). The primary forum within the federal government for executive departments and agencies to coordinate and enhance their export control enforcement efforts. The Center maximizes information sharing, consistent with national security and applicable laws. This helps partner agencies detect, prevent, disrupt, investigate and prosecute violations of U.S. export control laws. (www.ice.gov)

> Executive Order 13558 created the Export Enforcement Coordination Center. E2C2 provides a venue through which to deconflict technology transfer investigations,
>
> For additional information see <http://www.ice.gov/export-enforcement-coordination-center/>

Extremist Activity. As used in this regulation, an activity that involves the use of unlawful violence or the threat of unlawful violence directed against the Army, DOD, or the United States based on political, ideological, or religious tenets, principals, or beliefs. (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010)

Eyewash. [Tradecraft jargon] False entries made in files, usually to protect the security of a source, often indicating that a particular target has rejected a pitch, when in fact the offer was accepted. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

F ==========

Fabricator. An individual or group who, usually without genuine resources, invents or inflates information for personal or political gain or political purposes. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, an agent who furnishes false information for financial gain. (A Spy's Journey)

False Flag. Development or execution of any imitative or operation under false national sponsorship or credentials (aka "false colors"). The Russian term is foreign flag. (CIA in D&D Lexicon, 1 May 2002) Also see *false-flag approach* and *false-flag recruitment*

-- Also, occurs when an individual is recruited believing he or she is cooperating with an intelligence service of a specific country. In actuality, he or she has been deceived and is cooperating with an intelligence service of another country. (AFOSI Manual 71-119, CI Investigations, 27 Oct 2009)

-- Also, the technique for misrepresenting an individual's country of origin is a risky but well-established tactic adopted by all counterintelligence agencies in the absence of other, safer alternatives. Invariably, the strategy is one of last resort when a suspect is known to have engaged in espionage, but is thought to be currently inactive. The offer to be reengaged as a spy may be accepted and result in sufficient evidence to secure a conviction, or may prompt an incriminating action. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

-- Also, approach by a hostile intelligence officer who misrepresents himself or herself as a citizen of a friendly country or organization. The person who is approached may give up sensitive information believing that it is going to an ally, not a hostile power. (Spy Book)

-- Also, the use of a third country's nationality to effect the recruitment of an agent so they do not know an activity's true country of origin. (A Spy's Journey)

False-Flag Approach. An intelligence officer or agent who represents themselves as a person of another nationality in order to foster trust and lessen suspicion about the contact. (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010) Also see *false flag; false-flag recruitment*.

False-Flag Recruitment. A situation that occurs when an individual is recruited believing that he/she is cooperating with an intelligence eservice of a specific country, when in actually he/she has been deceived and is cooperating with an intelligence service of another country. (CI Community Lexicon) Also see *false-flag; false-flag approach*.

> *"…'false flag' recruitment—when an intelligence service recruits a target while pretending to represent another nation—a common piece of tradecraft. When you finally recruit the target, he believes he is providing information to some other nation. The Israelis have often used this technique by impersonating CIA officers when trying to recruit Arabs."*
> -- Duane R. Clarridge, *A Spy For All Seasons: My Life in the CIA* (1997), p. 97

-- Also, an individual recruited believing he/she is cooperating with an intelligence service of a specific country when, in reality, the individual has been deceived and is working on behalf of an intelligence service of another country. (ICS Glossary & AR 381-47, OFCO, 17 Mar 2006)

-- Also, recruitment of an individual under the guise of working for one entity when actually working for another entity. (HDI Lexicon, April 2008)

> Can also be used as a CI investigative technique to determine whether a suspected spy intends to or has committed espionage or other national security crimes against the United States; in this type of false flag a U.S. CI or law enforcement officer poses as an intelligence operative of a foreign power in an undercover operation. The FBI has successfully used this type of false flag operation in several espionage cases, e.g., see United States of America *v.* Stewart Davis Nozette (U.S. District Court for the District of Columbia, case number: 09-0565M)

Faraday Bag. Specialty collection bags for electronic parts with lining to protect the contents from electromagnetic forces. (Crime Scene Investigation: A Guide for Law Enforcement, Sep 2013)

FIE. See *Foreign Intelligence Entity*.

FISS. See *Foreign Intelligence and Security Service*.

Federal Bureau of Investigation (FBI). The primary investigative arm of the US Department of Justice (DoJ) with jurisdiction over violations of more than 200 categories of federal law and also a statutory member of the US Intelligence Community. The FBI's mission is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners. (www.fbi.gov)

> "*The FBI is unique in having a dual responsibility—to prevent harm to national security as a member of the U.S. Intelligence Community and to enforce federal laws as part of the Department of Justice. The Bureau reports to both the Attorney General and the Director of National Intelligence."*
>
> -- FBI, *Today's FBI – Facts and Figures 2010-2011*
>
> _____
>
> The FBI has authority to investigate threats to the national security pursuant to Presidential Executive Orders, Attorney General authorities, and various statutory sources. Per EO 12333 (US Intelligence Activities) the FBI coordinates the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States.
>
> _____
>
> "*We always thought of the FBI highly. We viewed it, this organization, as a formidable one. In the intelligence business, it's better to overestimate than underestimate, we never just thought of the FBI as incompetent or weak organization. It was an adversary, a formidable adversary, truly."*
>
> -- Oleg Kalugin, Retired KGB General (served in Washington DC and Former Chief of Line KR)

Federal Grand Jury (FGJ). An independent panel charged with determining whether there is probable cause to believe one or more persons committed a particular federal offense. If the FGJ believes probable cause exists, it will vote a "true bill" and the person will be indicted. An indictment is the most typical way a person is charged with a felony in federal court. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

Federal Polygraph Examiner. Military, civilian, or contractor personnel authorized to conduct polygraph examinations on behalf of a federal agency. (DoD 5210.48, Polygraph and Credibility Assessment Program, 25 Jan 2007 with change 2 dated 15 Nov 2013)

Federally Funded Research and Development Center (FFRDC). Research and development-performing organizations that are exclusively to substantially financed by the Federal Government and are supported by the Federal Government either to meet a particular research and development objective or, in some instances, to provide major facilities at either universities or corporate or contractor locations for applied research to development purpose. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

Feed Material. Information that is usually true but unimportant given to an individual to pass to another intelligence service to maintain or enhance his value to that service. Sometimes called build-up material. (FBI FCI Terms)

Feedback. Information or intelligence provided to deception planners as to the progress of a deception operation and, ultimately, its success or failure. (CIA in D&D Lexicon, 1 May 2002)

Fifth Columnist. A subversive who acts out of secret sympathy for an enemy of his or her own country. (*Encyclopedia of the CIA*, 2003)

-- Also, people who clandestinely undermine a larger group such as a nation from within. A fifth column can be a group of secret sympathizers of an enemy that are involved in sabotage within military defense lines, or a country's borders. A key tactic of the fifth column is the secret introduction of supporters into the whole fabric of the entity under attack. (Wikipedia; accessed 9 August 2012)

The term was coined in 1936, during the Spanish Civil War. It was said then that the Spanish rebels had four columns of troops marching on the city of Madrid—and an additional "fifth column" of sympathizers within the city itself. Ready to take up arms at a moments' notice.

-- *Encyclopedia of the CIA* (2003)

In the United States at the end of the 1930s, as involvement in the European war seemed ever more likely, those who feared the possibility of betrayal from within used the newly coined term "fifth column" as a shorthand for sedition and disloyalty.

-- Wikipedia; accessed 9 August 2012

The fifth column is *"that portion of our population which is ready to give assistance or encouragement in any form to invading or opposing ideologies."*

-- Attorney General Robert H. Jackson, 1940
(later Associate Justice of the United States Supreme Court, 1941–1954)

The Communist Party of the United States is a fifth column if there ever was one.

-- J. Edgar Hoover, Director Federal Bureau of Investigation
Testimony before Committee on Un-American Activities,
U. S. House of Representatives, circa 1948

Financial Crimes Enforcement Network (FinCEN). An element of the Department of Treasury with the mission to safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering and other illicit activity. FinCEN administers the Bank Secrecy Act; supports law enforcement, intelligence, and regulatory agencies through sharing and analysis of financial intelligence; builds global cooperation with counterpart financial intelligence units; and networks people, ideas, and information. (website: <http://www.fincen.gov>)

FinCEN exercises regulatory functions primarily under the Currency and Financial Transactions Reporting Act of 1970, as amended by Title III of the USA PATRIOT Act of 2001 and other legislation, which legislative framework is commonly referred to as the "Bank Secrecy Act" (BSA).

The BSA is the nation's first and most comprehensive Federal anti-money laundering and counter-terrorism financing (AML/CFT) statute. In brief, the BSA authorizes the Secretary of the Treasury to issue regulations requiring banks and other financial institutions to take a number of precautions against financial crime, including the establishment of AML programs and the filing of reports that have been determined to have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings, and certain intelligence and counter-terrorism matters.

Financial Record. An original, its copy, or information known to have been derived from the original record held by a financial institution that pertains to a customer's relationship with the financial institution. (DoDI 5400.15, Guidance on Obtaining Information from Financial Institutions, 2 Dec 2004 w/ chg 3 Jul 2007)

Finding. A written legal determination made by the President of the United States authorizing a particular covert action important to US national security, in compliance with the Foreign Assistance Act of 1961, as amended by the 1971 Hughes-Ryan Amendment. (National HUMINT Glossary) Also see *covert action*.

The President shall approve all covert action Findings in writing. Under Section 662 of the Foreign Assistance Act of 1961, as amended, all covert actions undertaken… must be authorized by a Presidential Finding that each such operation is important to US national security.

-- National Security Decision Directive Number 159, 18 Jan 1985 (originally TS-Sensitive, declassified)

According to the Congressional Research Service, the reference to a **"presidential finding"** took on its current popular meaning when Congress adopted the Hughes-Ryan amendment to the Foreign Assistance Act in 1974. Section 662 of the statute prohibits the expenditure of appropriated funds by or on behalf of the CIA for covert actions "unless and until the President finds that each such operation is important to the national security of the United States and reports, in a timely fashion, a description and scope of such operation to the appropriate committees of Congress."

The requirements of this provision subsequently went through a series of transformations, the vestiges of which were recently codified in the Intelligence Authorization Act, FY1991, which still requires a written presidential finding satisfying certain conditions set forth in the statute for covert actions to occur. Such presidential findings, which are classified, are to be "reported to the intelligence committees as soon as possible" after being approved "and before the initiation of the covert action authorized by the finding." These findings are not published in the Federal Register or reproduced in CFR Title 3 compilations.

Firewall. A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy. . (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

FIVE EYES (FVEY). Australia, Canada, New Zealand, United Kingdom and the United States. (CAPCO and DoDI C-5240.08, CI Security Classification Guide, 28 Nov 2011)

Five Ws (also known as the Five Ws and one H). The formula for getting the "full" story on something. The maxim of the Five Ws (and one H) is that in order for a report to be considered complete it must answer a checklist of six questions, each of which comprises an interrogative word: Who, What, When, Where, Why, and How? (Wikipedia; accessed 20 Feb 2009)

Flag Officer. A term applied to an officer holding the rank of general, lieutenant general, major general, or brigadier general in the US Army, Air Force or Marine Corps or admiral, vice admiral, or rear admiral in the US Navy or Coast Guard. (JP 1-02)

Flaps and Seals. [Intelligence parlance for] the clandestine opening, reading, and resealing of either envelopes or packages without the recipient's knowledge. (Spycraft)

For or On Behalf of a Foreign Power. The determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in (a) control or policy direction; (b) financial or material support; or (c) leadership, assignments, or discipline. (AFOSI Manual 71-119, CI Investigations, 27 Oct 2009)

Force Multiplier. A capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

Force Protection (FP). Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information . (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Force Protection Detachment (FPD). A CI element that provides CI support to transiting and assigned ships, personnel, and aircraft in regions of elevated threat. (DoDD O-5240.02, Counterintelligence, 20 Dec 2007 with change 1 dated 30 Dec 2010; also JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ change 1 dated 26 Aug 2011)

The primary focus of FPDs is to provide current and actionable force protection information to the commander of "in transit" resources. FPDs were created in the aftermath of the USS Cole (DDG 67) bombing in the Port of Aden, Yemen on 12 October 2000.

_____

Service counterintelligence programs are integral to force protection and must be adequately manned and funded to meet the dynamic demands of supporting in-transit forces.

-- Finding 20, *DoD USS Cole Commission Report*, 8 Jan 2001 (p. 97); p. 7 in the unclassified version.

_____

The FPD primary mission is to detect and warn of threats to DoD personnel and resources in-transit at overseas locations without a permanent DoD CI presence. … FPDs shall maintain liaison contact with host nation officials to assess an operational picture of the local intelligence, terrorist, and criminal threat.

-- DoDI 5240.22, *CI Support to Force Protection,* 24 Sep 2009, pp. 7-8 (encl 3, para 5)

_____

The principal responsibility of the FPD is to provide FP [force protection] services to DoD personnel, aircraft, ships and resources, as well as coordinate component FP activities. The FPD detects and warns of threats to DoD military and civilian assets in-transit at overseas locations that do not possess a permanent DoD CI presence.

-- Erika Triscari, "Force Protection Detachments, the Force Multiplier," *The Guardian*, April 2006, pp. 6-9.

Force Protection Response Group (FPRG). For specifics see DoDI S-5240.15, FPRG (U), 20 Aug 2010.

Foreign Agents Registration Act (FARA). A disclosure statute, enacted in 1938, that requires persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities. Disclosure of the required information facilitates evaluation by the government and the American people of the statements and activities of such persons in light of their function as foreign agents. (22 USC §611)

See more on the FARA at DoJ website: <http://www.fara.gov>

The FARA Registration Unit of the Counterespionage Section in the National Security Division (NSD), Department of Justice (DoJ) is responsible for the administration and enforcement of the Act. See DoJ website at <http://www.usdoj.gov/criminal/fara/index.html>

Foreign Collection Threat. Opportunity for a foreign entity or cooperating DoD personnel (an insider) to overtly, covertly or clandestinely collect information about RDA programs, technologies, system capabilities and employment methods that may enable an adversary to copy, counter, or defeat6 a capability, or inhibit, exploit, or sabotage a defense system. Within the context of [DoDI O-5240.24], the term collectively refers to threats posed by or form an insider, cyber exploitation, supply chain manipulation, an FIE [foreign intelligence entity], a foreign company, international transfers or exports of technology, and disposal of export-controlled technology. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

Foreign Computer Intrusion. The use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more U.S.-based computers. (AG Guidelines for Domestic FBI Operations, 29 Sep 2008)

Foreign Contact. Contact with any person or entity that is not a U.S. Person. (IC Standard 700-1, 4 Apr 2008)

Foreign Connection. A U.S. person has a foreign connection when a reasonable belief exists that the U.S. person is or has been in contact with, or has attempted to contact, a foreign person or representative of a foreign power for purposes harmful to U.S. national security interests; or when a reasonable belief exists that the U.S. person is acting or encouraging others to act in furtherance of the goals or objectives of a foreign person or power for purposes harmful to U.S. national security interests. (DoDD 5148.11, ATSD/IO, 24 Apr 2013)

-- Also, a foreign connection is established by a reasonable belief that a U.S. person is or has been in contact with, or has attempted to contact, a foreign person or a representative of a foreign power, or a reasonable belief that a U.S. person is acting or encouraging others to act to further the goals or objectives of a foreign person or foreign power. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013)

Foreign Counterintelligence Program (FCIP). Military component of the National Intelligence Program (NIP) that conducts counterintelligence activities in support of the Department of Defense. Also see *National Intelligence Program (NIP).*

> Within the National Intelligence Program (NIP) the two key national-level DoD intelligence programs are the General Defense Intelligence Program (GDIP) and the FCIP.
> -- Adapted from Dan Elkins, *Financial Management of Intelligence Resources: A Primer* (3rd Edition), May 1992

Foreign Cultural Analysis. Analysis of information on the demographics, norms, values, institutions, and artifacts of a population used to assist in anticipating the actions of that population within the operating environment. (DoDD 3600.01, Information Operations, 14 Aug 2006 with chg 1, 23 May 2011)

Foreign Denial & Deception. Foreign capabilities and techniques designed to conceal, manipulate, deny, deceive, influence, induct uncertainty, and generate gaps in U.S. intelligence capabilities and/or conceal intentions. Also see *denial; deception, military deception*.

> ***Aggressive foreign D&D efforts erode our intelligence advantage***
>
> Foreign knowledge and understanding of US intelligence capabilities are significant and growing problems across all intelligence disciplines and represent serious challenges to US national Security.
>
> ***"America's toughest adversaries know a great deal about our intelligence system and are becoming better at hiding their intentions and capabilities."***
>
> -- *The National Intelligence Strategy*, October 2005, p.9

Foreign Denial & Deception Committee (FDDC). An interagency intelligence committee that operates under the auspices of the National Intelligence Council (see ICD 204).

Foreign Instrumentation Signals Intelligence (FISINT). Technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012) Also see *signals intelligence (SIGINT).*

> In the early 1980s the term TELINT (telemetry intelligence) was broadened to include other key signals that also describe missile/space events and was renamed Foreign Instrumentation Signals Intelligence (FISINT).

Foreign Intelligence (FI). Information relating to capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence, except for information on international terrorist activities. (National Security Act §3(2), 50 USC §401a) Also see *positive intelligence*.

-- Also, information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities. (EO 12333 as amended and JP 2-0, Joint Intelligence, 22 Oct 2013)

> FI collection disciplines include: human intelligence (HUMINT); signals intelligence (SIGINT); geospatial intelligence (GEOINT), including imagery intelligence (IMINT); and measurement & signatures intelligence (MASINT).
>
> FI does not include counterintelligence. FI is one of the two components of intelligence, the other is counterintelligence (CI) per Executive Order 12333 *US Intelligence Activities* as amended and the National Security Act of 1947 as amended.

Foreign Intelligence Agent. A person other than a foreign intelligence officer, who is engaged in intelligence activities or sabotage for on the behalf of a foreign power, or international terrorist activity, or who knowingly conspires with or aids and abets such a person in these activities. (CI Community Lexicon) Also see *agent;* and *agent net.*

Foreign Intelligence and Security Service (FISS). An organization of a foreign country capable of executing all or part of the intelligence cycle. Note: sometimes referred to as FIS (Foreign Intelligence Service). Also see *foreign intelligence entity*.

-- Also, a foreign government's intelligence and security organization. (DoD FCIP Strategy FY 2013-2017)

Foreign Intelligence Collection Threat. The potential of a foreign power, organization, or person to overtly or covertly collect information about U.S. acquisition program technologies, capabilities, and methods of employment that could be used to develop a similar weapon system or countermeasures to the U.S. system or related operations. (DoD 5200.1-M, Acquisition Systems Protection Program, March 1994)

Foreign Intelligence Entity (FIE). Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service [FISS] and international terrorist organizations. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; DoDD 5240.06, CIAR, 17 May 2011 with change 1 dated 30 May 2013; and DoDI S-5240.17, CI Collection Activities, 14 Mar 2014)

> FIE is a more encompassing term, which includes but not limited to Foreign Intelligence and Security Services (FISS), as well as Foreign Intelligence Services (FIS).

-- Also, any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, blocks or impairs U.S. intelligence collection, influences U.S. policy, or disrupts U.S. systems and programs. This term includes a foreign intelligence and security service and international terrorists. (DoDI 5240.26, Countering Espionage, International Terrorism, and Counterintelligence Insider Threat, 4 May 2012 with change 1 dated 15 Oct 2013)

-- Also, any known or suspected foreign organization, person, or group (public, private, governmental) that conducts intelligence activities to acquire U.S. information, blocks or impairs US intelligence collection, influence US policy, or disrupts US systems and programs. This term includes foreign intelligence and security services and international terrorists. (DoDI S-5240.23, CI Activities in Cyberspace, 13 Dec 2010 with change 1 dated 16 Oct 2013) *Note: this definition is slightly different than the one above.*

-- Also, any foreign organization, person, or group (public, private, governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service as defined in Joint Publication 1-02. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

-- Also, known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and service services and international terrorists. (ICD 750, Counterintelligence Programs, 5 Jul 2013)

Foreign Intelligence Information. 1) Information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against— (a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or 2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—(a) the national defense or the security of the United States; or (b) the conduct of the foreign affairs of the United States. (Foreign Intelligence Surveillance Act of 1978; Public Law 95–511, 25 October 1978) Also see *Foreign Intelligence Surveillance Act (FISA).*

Foreign Intelligence Liaison. Activities or relationships between elements of the United States Government and elements of foreign governments or international organizations on matters involving foreign intelligence, counterintelligence, or clandestine intelligence activity.

Foreign Intelligence Officer. A member of a foreign intelligence service. (CI Community Lexicon) [Also referred to as an IO (intelligence officer)]. Also see *agent handler.*

Foreign Intelligence Service (FIS). An organization of a foreign country capable of executing all or part of the intelligence cycle. (CI Community Lexicon) Also see *Foreign Intelligence and Security Service, Foreign Intelligence Entity.*

Foreign Intelligence Entity (FIE) is a more all encompassing term which includes but is not limited to FIS.

_____

The importance of intelligence services in the fortune of nations can't be overstated…. The existence or absence of a well-working spy network on the territory of a potential enemy may well spell the difference between victory and defeat.

-- Alexander Orlov in *Handbook of Intelligence and Guerrilla Warfare* (1963)

Foreign Intelligence Surveillance Act (FISA). [50 USC §1801 / Public Law 95-111] …the legal authority authorizing and regulating electronic surveillance within the United States for foreign intelligence or counterintelligence purposes and physicals searches within the United States for foreign intelligence purposes. The act sets out the application, order, and report process to be followed. (CI Community Lexicon) Also see *Foreign Intelligence Surveillance Court*.

Primary purpose must be collection of foreign intelligence information.

FISA prescribes procedures for the physical & electronic surveillance and collection of "foreign intelligence information" between or among "foreign powers". Subchapters of FISA provide for: electronic surveillance; physical searches; pen registers and trap & trace devices for Foreign Intelligence (FI) purposes; and access to certain business records for FI purposes. FISA does not apply to U.S. counterintelligence activities overseas.

-- FISA, codified in 50 U.S.C. §1801, et seq was amended by the FISA Amendments Act of 2008.

The Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, 92 Stat. 1783 (25 Oct 1978), 50 USC §§ 1801 et seq., provides a statutory framework for gathering **foreign intelligence information** through the use of electronic surveillance, physical searches, and pen registers or trap and trace devices, and access to business records and other tangible things, the 1978 Act dealt only with electronic surveillance.

The provisions passed almost 30 years ago became Title I of FISA. As originally enacted, the measure provided a statutory framework for collection of **foreign intelligence information** through the use of electronic surveillance of communications of foreign powers or agents of foreign powers, as those terms were defined in the act. The act has been amended repeatedly in the intervening years in an effort to address changing circumstances. Then, as now, the Congress sought to strike a balance between national security interests and civil liberties.

FISA consists of seven parts. The first authorizes electronic surveillance in foreign intelligence investigations. The second authorizes physical searches in foreign intelligence cases. The third permits the use and installation of pen registers and trap and trace devices in the context of a foreign intelligence investigation. The fourth affords intelligence officials access to business records and other tangible items. The fifth directs the Attorney General to report to Congress on the specifics of the exercise of FISA authority. The sixth, scheduled to expire on 30 December 2012, permits the acquisition of the communications of targeted overseas individuals and entities. The seventh creates a safe harbor from civil liability for those who assist or have assisted in the collection of information relating to the activities of foreign powers and their agents.

Electronic surveillance can provide vital information needed to identify those who are acting or preparing to act against U.S. interests for the benefit of foreign powers, including those engaged in espionage, sabotage, or terrorist acts or who otherwise pose a threat to the nation or its citizens, and to uncover their plans or activities. This information may not be readily uncovered by other investigative means. Thus, surveillance can provide a valuable tool for protecting the security of the nation and its citizens.

-- CRS Report RL34279: *Foreign Intelligence Surveillance Act: An Overview of Selected Issues*, 7 Jul 2008
Copy available on line at: <http://www.fas.org/sgp/crs/intel/RL34279.pdf>

Note: Under 50 USC §1801(e)(1), ***foreign intelligence information*** is information that relates to U.S. ability to protect against: 1) possible hostile acts of a foreign power or agent of a foreign power; 2) sabotage or terrorism by a foreign power or agent, and: 3) . clandestine intelligence activities by a foreign power or agent. Foreign intelligence information includes information with respect to a foreign power or foreign territory that relates to the national defense, national security, or conduct of foreign affairs of the United States.

Probable cause under FISA: *"Ordinarily, probable cause speaks to the probability of the existence of a certain fact, e.g., probable cause to believe a crime has been, is, or is about to be committed and that the search will result in the discovery of evidence or contraband. FISA authorizes issuance of a surveillance or search order predicated upon the probability of a possibility; the probability to believe that the foreign target of the order may engage in spying, or the probability to believe that the American target of the order may engage in criminal spying activities, 50 U.S.C. 1805(a)(3)(A), 1824(a)(3)(A), 1801(b)(1)(B), (b)(2)(A).3 But it is the predicate not the standard that is changed. The probable cause standard is the same in FISA as in a criminal context: would a prudent individual believe that a fact is probably true. It is the focus that is different. Would a prudent individual believe that spying may occur."*

-- CRS Memorandum (American Law Division), 30 Jan 2006

Misc. FISA References& Background

Foreign Intelligence Surveillance of 1978, 50 USC §1801 (Public Law 95-111)

Presidential Directive/NSC-19, Electronic Surveillance Abroad and Physical Searches for Foreign Intelligence Purposes, 25 Aug 1977 [declassified]; amended by POTUS via 24 Aug 1979 White House Memo [declassified]

Executive Order 12139, FISA, 23 May 1979

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (PL 110-261), 10 Jul 2008

Executive Order 12949, Foreign Intelligence Searches, 9 Feb 1995

A thorough constitutional justification of FISA can be found in *United States v. Duggan* (743 F.2d 59[2d Cir. 1984]) where both Fourth and Fifth Amendment challenges to this kind of electronic surveillance were addressed by the court.

US Senate. *The Foreign Intelligence Surveillance Act of 1978: The First Five Years*, Report 98-660, 98th Congress, 2nd Session, Washington, DC, 1984.

CRS Report R42725, *Reauthorization of the FISA Amendment s Act*, 2 Jan 2013; copy available at: <http://www.fas.org/sgp/crs/intel/R42725.pdf>

For additional FISA background see FAS website at: <http://www.fas.org/irp/agency/doj/fisa/>

Foreign Intelligence Surveillance Court (FISC) [often referred to as the "FISA Court"]. A U.S. federal court established in 1978 when Congress enacted the *Foreign Intelligence Surveillance Act* (FISA)--codified, as amended, at 50 USC §§ 1801-1885c. The Court entertains applications submitted by the U.S. Government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes.

Most of the Court's work is conducted ex parte as required by statute, and due to the need to protect classified national security information. The FISC sits in Washington D.C. and is composed of eleven federal district court judges who are designated by the Chief Justice of the United States.

Each judge serves for a maximum of seven years and their terms are staggered to ensure continuity on the Court. By statute, the judges must be drawn from at least seven of the United States judicial circuits, and three of the judges must reside within 20 miles of the District of Columbia. No judge may be appointed to this court more than once, and no judge may be appointed to both the Court of Review and the FISC. FISC Judges typically sit for one week at a time, on a rotating basis.

For additional information, see the FISC web site at: <http://www.fisc.uscourts.gov/>
-- FISC Rules of Procedures at: <http://www.fisc.uscourts.gov/rules-procedure>
-- FISC Public Findings at: <http://www.fisc.uscourts.gov/public-filings>

Foreign Intelligence Threat. The all-source intelligence threat posed by foreign intelligence entities to US interests.

Foreign Intelligence Threats

[T]he leading state intelligence threats to US interests in 2014 will continue to be Russia and China, based on their capabilities, intent, and broad operational scope. Sophisticated foreign intelligence entities will continue to employ human and cyber means to collect national security information.

-- Hon. James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, SSCI, 29 January 2014

_____

Foreign intelligence services, along with terrorist groups, transnational criminal organizations, and other nonstate actors, are targeting and acquiring our national security information, undermining our economic and technological advantages, and seeking to influence our national policies and processes covertly. These foreign intelligence efforts employ traditional methods of espionage and, with growing frequency, innovative technical means. Among significant foreign threats, ***Russia*** *and* ***China*** *remain the most capable and persistent intelligence threats and are aggressive practitioners of economic espionage against the United States.* ***Countering such foreign intelligence threats is a top priority for the Intelligence Community for the year ahead*** *[emphasis added].*

-- Hon. James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Committee on Armed Services, 18 April 2013, p. 8

Foreign Liaison Officer (FLO). A foreign government military member or civilian employee who is authorized by his or her government to act as an official representative of that government in its dealings with the DoD and Military Services in connection with programs, projects, or agreements of mutual interest to DoD and the foreign government. (adapted from AR 380-10, 22 Jun 2005)

Three types of FLOs:

1) A *Security Assistance FLO* is a foreign government representative who is assigned to a DoD element or contractor facility pursuant to a requirement that is described in an FMS LOA;

2) An *Operational FLO* is a foreign government representative who is assigned to a DoD element pursuant to a documented requirement to coordinate operational matters, such as combined planning or training and education; and

3) A *National Representative FLO* is a foreign government representative who is assigned to his or her national embassy or legation in Washington, DC (for example, an attaché), to conduct liaison activities with DoD / Military Services.

Foreign Material. Any item of foreign origin including physical possession of, or access to, an item of foreign material or technology. (DIAM 58-4, Foreign Material Program, 22 Feb 2002)

Foreign Material Acquisition (FMA). FMP [Foreign Material Program] activities that include gaining physical possession, or access to, an item of foreign material or technology. (DoDD S-3325.01E, Foreign Material Program (U), 30 Dec 2011)

Foreign Material Exploitation (FME). FMP [Foreign Material Program] activities that include analysis, testing, evaluation, and documentation of the S&TI [Scientific & Technical Intelligence] characteristics of an item of foreign material. (DoDD S-3325.01E, Foreign Material Program (U), 30 Dec 2011)

Foreign Military Intelligence Collection Activities (FORMICA). Entails the overt debriefing, by trained HUMINT personnel, of all U.S. persons employed by the Department of Defense who have access to information of potential national security value. (DoDI C-5205.01, FORMICA (U), 22 Jan 2009; also JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Foreign National. Any person other than a US citizen, US permanent or temporary legal resident alien, or person in US custody. (JP 1-02)

-- Also, any person who is not a citizen of the U.S. (IC Standard 700-1, 4 Apr 2008)

Foreign Ownership, Control or Influence (FOCI). A U.S. company is considered under foreign ownership, control, or influence whenever a foreign interest has the power, direct or indirect, whether or not exercised and whether or not exercisable through ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information and/or special nuclear material or may affect adversely the performance of classified matters. (ISC 2008-700-1, 4 Apr 2008)

> Within DoD, see DTM 09-019, *Policy Guidance for FOCI*, 2 Sep 2009 (with chg 6 dated 9 Jan 2014)

Foreign Power. Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities. (DoD 5240.1-R, Dec 1982)

-- Also, foreign power means: (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation thereof; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments. (50 USC § 1801a). Also see *Agent of a Foreign Power.*

Foreign Service National (FSN). Foreign nationals who provide clerical, administrative, technical, fiscal, and other support at foreign service posts abroad and are not citizens of the United States. The term includes third country nationals who are individuals employed by a US mission abroad and are neither a citizen of the US nor of the country to which assigned for duty. (JP 1-02 and JP 3-68, Noncombatant Evacuation Operations, 23 Dec 2010)

Foreign Terrorist Tracking Task Force (FTTTF). A specialized task force that was created pursuant to Homeland Security Presidential Directive No. 2 and was consolidated into the FBI pursuant to the Attorney General's directive in August 2002. The FTTTF uses innovative analytical techniques and technologies that help keep foreign terrorists and their supporters out of the United States or lead to their location, detention, prosecution, or removal. The participants include DoD, Department of Homeland Security's bureaus of Immigration and Customs Enforcement (ICE) and Customs and Border Protection, State Department, Social Security Administration, Office of Personnel Management, Department of Energy, and CIA. (FBI website: <http://www.fbi.gov/congress/congress06/mueller120606.htm>)

Foreign Visits System (FVS). Automated system operated by the Office of the Under Secretary of Defense (Policy) that provides staffing and database support for processing requests for visits by foreign nationals to DoD activities and defense contractors. FVS consists of an unclassified segment that allows the online submission of visit requests from embassies in Washington, DC, and, in some cases, directly from foreign governments overseas. FVS also has a classified segment that provides staffing, decision-making support, and database capabilities to the military departments and DIA.

Forensics. [In computer / cyber usage] The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) Also see *forensic science*.

Forensic Copy. An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Forensic Science (often shortened to forensics). The application of multidisciplinary scientific processes to establish facts. (DoDD 5205.15E, DoD Forensic Enterprise, 16 Apr 2011) Also see *digital & multimedia forensics, digital evidence*, and *digital forensics*.

> The Secretary of the Army is the DoD Executive Agent (EA) for Forensics, specifically for those forensic disciplines relating to deoxyribonucleic acid (DNA), serology, firearms and tool marks, latent prints, questioned documents, drug chemistry, and trace materials, as well as forensics relating to forensic medicine disciplines such as forensic pathology, forensic anthropology, forensic toxicology, and DNA analysis to identify human remains.
>
> The Secretary of the Air Force is the DoD EA for Digital and Multimedia (D/MM) Forensics, specifically for those forensics disciplines relating to computer and electronic device forensics, audio forensics, image analysis, and video analysis.

Forensic-Enabled Intelligence (FEI). The intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest. (JP 2-0, Joint Intelligence, 22 Oct 2013.

FORMICA. See *Foreign Military Intelligence Collection Activities*.

FOUR EYES (ACGU). Australia, Canada, United Kingdom, and the United States. (CAPCO)

Front. [In intelligence usage] a legitimate operation created by an intelligence organization as a cover for its operatives. (*Encyclopedia of the CIA*, 2003)

-- Also, Front Company [in law enforcement/criminal investigation usage] a company or business entity that is established, used, or co-opted for an illicit purpose; wherein the management, control, influence or criminal activities are being directed by a hidden or disguised individual or group. (Colin A. May, M.S., CFE, U.S. Department of Commerce, Sep 2010)

> For additional information see Colin A. May, "Front Companies: Challenges and Tools in Criminal Investigations," *IALEIA Journal*, Vol. 19, No. 1, pp. 101-120, September 2010. The *IALEIA Journal* is published by the International Association of Law Enforcement Intelligence Analysts, Inc.,
>
> > According to Colin May (in his article cited above, p. 102),*"many people use the phrase 'front company' when they are really describing the front company's distant cousin—the Shell Company. The Financial Crimes Enforcement Network… defines shell companies as 'limited liability companies and other business entities with no significant assets or ongoing business activities.' The shell simply is a paper company; they have also been called "International Business Corporations (IBCs)" or 'shelf companies,' since in some off-shore jurisdictions, the incorporators already have created the companies and simply pull them off the shelf to change the beneficial owner. The difference cannot be overstated…."*
> >
> > *"Front companies conduct actual business—shells do not.* [Shells] *are simply paper companies. Front companies have tangible operations, although they may be illicit or illegitimate, they are definite business transactions. The main difference that many investigators and intelligence analysts seem to miss is the 'action' piece in a front company—and that, of course, is highly dependent on the criminal's intended purpose for the front company. A shell, used by a criminal, disguises their involvement in the business, but the shell has no actual operations, whereas the front company does."*
>
> Also see Defense Security Service (DSS) article "Front Companies: Who is the End User?" at: <http://www.dss.mil/isp/count_intell/front_comp_who_user.html>

Full Field Counterintelligence Investigation. An investigation which is conducted when there are specific and articulable facts giving reason to believe that a person over whom Army counterintelligence has jurisdiction may be involved in acts that may constitute threats to national security. (AR 381-20, Army CI Program, 25 May 2010) See *CI Investigation*.

> Within the FBI referred to as "Full Investigation" which may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or collect foreign intelligence. These cases may be opened if there is an "articulable basis" of possible criminal or national threat activity.
>
> The Investigation of threats to the national security can be investigated under FBI's criminal investigation authority or its authority to investigate threats to the national security. A Full Investigation solely for the collection of positive foreign intelligence extends the sphere of the FBI's information gathering activities beyond federal crimes and threats to the national security and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States' foreign affairs.
>
> -- FBI's Domestic Investigation and Operations Guide (redacted copy), 15 Oct 2011

Full-Spectrum Counterintelligence Activities. Full array of CI activities – both offensive & defensive – that can be applied in executing CI effects-based operations to achieve strategic outcomes in peacetime, crisis, war and post conflict activities (e.g., stabilization operations/reconstruction efforts). These activities support national security objectives, as well as defense decision-makers and the Combatant Commanders.

Functional Component Command. A command normally, but not necessarily, composed of forces of two or more Military Departments which may be established across the range of military operations to perform particular operational missions that may be of short duration or may extend over a period of time. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Functional Managers. Executive Order 12333 designates three Functional Managers: Director CIA for human intelligence (HUMINT), Director NSA for signals intelligence (SIGINT), and Director NGA for geospatial intelligence (GEOINT), (EO 12333, para 1.3 (b)(12)(A)(i-iiii)) See ICD 113, *Functional Managers*.

> Pursuant to EO 12333, Functional Managers report to the DNI concerning the extent of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; setting training and tradecraft standards; and ensuring coordination within and across intelligence disciplines and IC elements and with related non-intelligence activities.
>
> Functional Managers may also advise on resource management; policies and procedures; collection capabilities and gaps; intelligence processing and dissemination; technical architectures; and other issues or activities, as applicable.
>
> Note: The National Counterintelligence Executive (NCIX) is the Mission Manager for CI.

Functional Support [Analytical Product]. A type of CI analytical product that supports the specific needs of a Defense CI Component. A functional support product is related to the CI functions of collection, investigation, OFCO {Offensive Counterintelligence Operation], and functional services as described in DoDI 5240.16. The depth and comprehensiveness varies depending on the requestor's requirements. An investment in analytical effort may be significant. The production timeline ranges from hours to weeks, but can vary widely depending on the function the analysis supports. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013) Also see *Counterintelligence Analytical Product*.

Functional Support Plan (FSP). Annexes to the National Intelligence Support Plan (NISP) [that] describe how service intelligence centers and Combat Support Agencies support COCOM plans. (Adaptive Planning Roadmap II, 5 Mar 2008) Also see *Counterintelligence Functional Support Plan (CI FSP).*

> Director DoD Counterintelligence Field Activity (CIFA)* will *"fully integrate CI into the intelligence campaign planning process by developing and updating the CI functional support plans."*
> -- DUSD (CI&S) memo, subj: Counterintelligence Support to COCOMs, 29 Dec 2006
> * Note: CIFA's mission and functions transitioned into DIA effective 3 August 2008.

Fusion. In intelligence usage, the process of managing information to conduct all-source analysis and derive a complete assessment of activity. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, consolidating, combining, and correlating information together. (ADRP 2-0, Intelligence, Aug 2012)

Fusion Center. A State and major urban area focal point for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government, SLTT, and private sector partners. (Source: DHS in the National Infrastructure Protection Plan 2013)

G ==========

Gap. See *intelligence gap*.

GAMA (G). Unclassified term used to describe a type of sensitive compartmentalized information (SCI). (Words of Intelligence, 2nd Edition, 2011)

General Defense Intelligence Program (GDIP). An integrated Defense Intelligence capability that includes DIA, the Service technical production centers, and special collection activities. The GDIP integrates and produces National Intelligence for Defense and national Consumer's. It represents the national Defense Intelligence priorities for operational customers, national and Defense-wide collection management, All-Source Analysis, HUMINT, MASINT, IT, and Special Activities. The GDIP is an integrated capability, and the Director, DIA, serves as the Program Manager. The GDIP is part of the NIP, as defined in EO 12333. The GDIP may include other NIP activities as agreed between the Secretary of Defense and the DNI. (DoDI 5105.21, DIA, 18 Mar 2008) Also see *National Intelligence Program*.

> The GDIP is the broadest-based NIP program within the Department Of Defense and the military services. This program funds all national-level military intelligence units and activities that involve something other than cryptology, counterintelligence, and certain types of specialized reconnaissance, The GDIP funds intelligence production, collection, and infrastructure, which includes all defense intelligence production, all national-level DoD Human Source Intelligence (HUMINT), etc.
>
> -- Adapted from Dan Elkins, *Financial Management of Intelligence Resources: A Primer* (3rd Edition), May 1982, pp. 13-14

General Military Intelligence (GMI). Intelligence concerning the military capabilities of foreign countries or organizations, or topics affecting potential United States or multinational military operations. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *intelligence; military intelligence*.

General Support (GS). That support which is given to the supported force as a whole and not to any particular subdivision thereof. (JP 1-02) Also see *direct support*.

Geospatial Information. Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products. (JP 2-03, GEOINT Support to Joint Operations, 22 Mar 2007)

> See Congressional Research Report (CRS) R41825 (18 May 2011) for an unclassified primer on geospatial data & geographic information systems: <http://www.fas.org/sgp/crs/misc/R41825.pdf>

Geospatial Information and Services (GI&S). The collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the Earth's surface. Geospatial services include tools that enable users to access and manipulate data, and also include instruction, training, laboratory support, and guidance for the use of geospatial data. (DoDD 5105.60, NGA, 29 Jul 2009 and JP 2-03, GEOINT Support to Joint Operations, 22 Mar 2007)

Geospatial Intelligence (GEOINT). The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. (ICD 1, 1 May 2006; also JP 1-02 and JP 2-03, GEOINT Support to Joint Operations, 22 Mar 2007)

-- Also, intelligence derived from the exploitation of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. (ODNI, U.S. National Intelligence – An Overview 2011)

The Intelligence Community refers to the use and analysis of geospatial information to assess geographically referenced activities on Earth as geospatial intelligence (GEOINT). It is everything you can see or know about the earth. GEOINT consists of: Imagery - a likeness of any natural or man-made feature, as well as its location; Imagery Intelligence (IMINT) – information derived through interpreting imagery; and Geospatial Information – information that identifies a natural or constructed feature on Earth by its geographic location and other characteristics.

-- www.cia.gov (accessed 30 Nov 2010)

GEOINT collection encompasses all aspects of: literal, infrared (IR), and synthetic aperture radar (SAR) imagery; overhead persistent infrared capabilities; and geospatial information and services. GEOINT includes the exploitation and analysis of electro-optical, IR, and radar imagery; and of geospatial, spectral, laser, IR, radiometric, SAR phase history, polarimetric, spatial, and temporal data. It employs all ancillary data, signature information, and fused data products, as necessary. Integrated GEOINT products may also include data and information from collateral sources.

-- DoDD 5105.60, *NGA*, 29 Jul 2009

GEOINT is typically gathered from commercial satellites, government satellites, reconnaissance aircraft, or by other means such as maps, commercial databases, census information, GPS waypoints, utility schematics, or any discrete data that have locations on earth. This data is utilized to support our national security, which includes everything from assisting soldiers on the battlefield to assisting humanitarian and disaster relief efforts.

-- www.intelligence.gov (accessed 13 Aug 2012)

Ghost Surveillance. Extremely discreet and seemingly omnipresent surveillance, working mostly out of the view of the target. (CI Centre Glossary) Also see *surveillance*.

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010)

Global Force Management (GFM). The ability to align force apportionment, assignment, and allocation methodologies in support of the National Defense Strategy and joint force availability requirements; present comprehensive insights into global availability and operational readiness of U.S. military forces; globally source joint force requirements; and provide senior decision-makers a vehicle to quickly and accurately assess the impact and risk of proposed allocation, assignment, and apportionment changes. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Global Positioning System (GPS). A satellite-based radio navigation system operated by the Department of Defense to provide all military, civil, and commercial users with precise positioning, navigation, and timing. Also called GPS. (JP 1-02 and JP 3-14, Space Operations, 6 Jan 2009)

Goldwater-Nichols Act (GNA). The Goldwater-Nichols Department of Defense Reorganization Act of 1986 (PL 99-433), sponsored by Sen. Barry Goldwater and Rep. Bill Nichols, was a major reorganization of U.S. defense institutions and processes. Operational authority was centralized through the Chairman of the Joint Chiefs of Staff as opposed to the service chiefs. The Chairman was designated as the principal military advisor to the President, National Security Council, and Secretary of Defense. The act

established the position of vice-chairman and streamlined the operational chain of command from the President to the Secretary of Defense to the Unified Commanders.

For additional information see <http://www.ndu.edu/library/goldnich/goldnich.html>
Copy of PL 99-443 at <http://www.au.af.mil/au/awc/awcgate/congress/title_10.htm>

Gray Literature (aka Grey Literature). Material not well covered by conventional book trade channels. Gray literature is intrinsically more difficult to identify, acquire, process, access, and otherwise handle than conventional literature. Examples include but are not limited to conference papers, trade literature, electronic bulletin boards, and foreign government reports. The information that grey literature contains is not available in any kind of source. (Words of Intelligence, 2nd Edition, 2011)

Gray List. Contains the identities and locations of those personalities whose inclinations and attitudes toward the political and military objectives of the United States are obscure. Regardless of their political inclinations or attitudes, personalities may be listed on gray lists when they are known to possess information or particular skills required by US forces. They may be individuals whose political motivations require further exploration before they can be utilized effectively by US forces. (CI Community Lexicon) Also see *Black List; White List.*

-- Also, a list of those foreign personalities of operational interest whose inclinations and attitudes toward the political and military objectives of the United Sates are unknown. (HDI Lexicon, April 2008)

Regardless of their leanings, personalities may be on gray lists when known to possess information or particular skills required by friendly forces. They may be individuals whose political motivations require further exploration before they can be used effectively. Examples of individuals who may be included in this category are:

1) Potential or actual defectors from the hostile cause whose credibility has not been established.
2) Individuals who have resisted, or are believed to have resisted the enemy government and who may be willing to cooperate with friendly forces, but whose credibility has not been established.
3) Nuclear, biological, chemical and other scientists and technicians suspected of having been engaged in enemy weapons of mass destruction and other programs against their will.

-- USMC, MCWP 2-6 (previously 2-14), Counterintelligence, 5 Sep 2000

Graymail. Threat by a defendant in a trail to expose intelligence activities or other classified information if prosecuted. (Spy Book) Also see *Classified Information Procedures Act (CIPA).*

"Graymail" colloquially refers to situations where a defendant may seek to introduce tangentially related classified information solely to force the prosecution to dismiss the charges against him.

A criminal prosecution involving classified information may cause tension between the government's interest in protecting classified information and the criminal defendant's right to a constitutionally valid trial. In some cases, a defendant may threaten to disclose classified information in an effort to gain leverage.

Concerns about this practice, referred to as "graymail," led the 96th Congress to enact the *Classified Information Procedures Act* (CIPA) to provide uniform procedures for prosecutions involving classified information.

Green Door. Slang term for the metaphorical locked door behind which intelligence personnel are said to hide their codeword secrets and important information not shared with consumers who need and should get it. (Words of Intelligence, 2nd Edition, 2001)

Groupthink. A decision-making flaw that occurs when a group does not consider alternatives and desires unanimity at the expense of quality decisions. Groupthink can lead to seeking out few alternative solutions because there is an illusion of group invulnerability ("we all can't be wrong'). Some symptoms of groupthink are the absence of critical discussion of information, a sharing of stereotypes to guide decisions, a strong moral climate, and the suppression of true feelings among the participants in the group. (Words of Intelligence, 2nd Edition, 2011)

GRU. *Glavnoye Razvedyvatel'noye Upravlenie* (Chief Intelligence Directorate of the General Staff); aka Russian Military Intelligence.

Russian military intelligence has a spy network abroad that is believed by espionage experts to be several times bigger than that of Russia's Foreign Intelligence Service.

-- Reuters, 24 Apr 2009

Also see Viktor Suvorov's (alias for GRU defector Vladimir Bogdanovich Rezun) books: *Aquarium* (Аквариум), 1985 and *Inside Soviet Military Intelligence*, 1984.

Guerrilla Force. A group of irregular, predominantly indigenous personnel organized along military lines to conduct military and paramilitary operations in enemy-held, hostile, or denied territory. (JP 1-02 and JP 3-05, Special Operations, 18 Apr 2011)

H ==========

Hacker. Unauthorized user who attempts to or gains access to an information system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a person who creates and modifies computer software and hardware, including computer programming, administration, and security-related items. This can be done for either negative or positive reasons. Criminal hackers create malware in order to commit crimes. (McAfee.com; accessed 15 Nov 2010)

> In computer security usage, a term used for a person who accesses a computer system by circumventing its security system.

Hacktivism. The nonviolent use of ambiguous digital tools in pursuit of political ends; these tools include website defacements, redirects, denial-of-service attacks, information theft, website parodies, virtual sit-ins, virtual sabotage, and software development. (<en.wikipedia.org/wiki/Hacktivists>; accessed 2 Apr 2009) Also see *hacktivists*.

> Hacktivism is the use of cyber instruments for political or ideological purposes.
>
> Hacktivism is a controversial term. Some argue it was coined to describe how electronic direct action might work toward social change by combining programming skills with critical thinking. Others use it as practically synonymous with malicious, destructive acts that undermine the security of the Internet as a technical, economic, and political platform**.**
>
> The term "hackitivism" first appeared in 1998, when members of a hacker group called the Cult of the Dead Cow used it as they chatted online about hacking and political liberation while discussing ideas to work with Chinese hackers following the Tiananmen Square protests.
>
> For additional information see McAfee White Paper, "Cybercrime and Hacktivism" (undated), available online at: <www.mcafee.com/us/resources/white-papers/wp-cybercrime-hactivism.pdf>

Hacktivists. Individuals who hack or attack Web sites and computer systems to communicate an ideological, social, or political message and further their cause. (FBI, Nov 2012) Also see *hacktivism*.

> *Hacktivists continue to target a wide range of companies and organizations in denial-of-service attacks…. Most hacktivists use short-term denial-of-service operations or expose personally identifiable information held by target companies, as forms of political protest. However, a more radical group might form to inflict more systemic impacts—such as disrupting financial networks—or accidentally trigger unintended consequences that could be misinterpreted as a state-sponsored attack.*
>
> -- DNI, *Worldwide Threat Assessment of the US Intelligence Community*, SSCI, 12 March 2013

Handler. An intelligence officer or co-opted worker directly responsible for the operational activities of an agent; also agent handler or case officer. (CI Community Lexicon) Also see *agent handler; case officer.*

-- Also, an intelligence collector directly responsible for the operational activities of an agent, source, or asset. (HDI Lexicon, April 2008)

Hard Target. A person, nation, group, or technical system often hostile to the US or heavily protected, with a well-honed counterintelligence capability that presents a potential threat to the US or its interests, and provides significant difficulty for agent infiltration or penetration. (National HUMINT Glossary)

Harmony. The Intelligence Community's centralized database for foreign military, technical and open-source documents and their translations. Harmony is managed by the US Army's National Ground Intelligence Center (NGIC). Also see *DOMEX; DOCEX*.

Hawala. The word comes originally from the Arabic language and means transfer or remittance. (US Department of Treasury)

> *Hawala provides a fast and cost-effective method for worldwide remittance of money or value, particularly for persons who may be outside the reach of the traditional financial sector. In some nations hawala is illegal, in others the activity is considered a part of the "gray" economy. It is therefore difficult to accurately measure the total volume of financial activity associated with the system, however, it is estimated that the figures are in the tens of billions of dollars, at a minimum. Officials in Pakistan, for example, estimate that more than $7 billion flow into the nation through hawala channels each year. Other Alternative Remittance or Informal Value Transfer Systems include "hundi," "fei ch 'ien," "chit system," "poey kuan" and the black market peso exchange.*
>
> -- US Department of Treasury web site, accessed 19 Nov 2012 <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/Hawala-and-Alternatives.aspx>

Hazard or Hazardous Condition. [In TSCM] a condition, either technical or physical, that could permit the exfiltration and exploitation of information. (DoDI 5240.05, TSCM, 3 Apr 2014)

Hazards. [In critical infrastructure protection usage] non-hostile incidents such as accidents, natural forces, and technological failure that cause loss or damage to infrastructure assets. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Hello Number. Tradecraft jargon for a cutout telephone where the speaker does not identify himself or his/her location. This procedure is used by proprietaries, devised facilities or cover offices of clandestine intelligence agencies for certain types of contacts with agents or affiliated personnel, usually in an emergency, and only information given by the caller over the phone is a codeword or danger signal to be relayed to the appropriate case officer for immediate call-back or other pre-arranged action. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Heuristics. Normal, intuitive mental shortcuts for processing information. They can be effective aids for problem-solving, but can lead to biases and thus to analytic errors.

High-Payoff Target (HPT). A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets that must be acquired and successfully attacked for the success of the friendly commander's mission. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007) Also see *high-value target; target.*

High-Risk Personnel (HRP). Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

High-Value Detainee Interrogation Group (HIG). The interagency body under the administrative control of the Federal Bureau of Investigation that was established to assemble and dispatch mobile interrogation teams to interrogate high-value detainees. (DoDD 3115.13, DoD Support to the High-Value Detainee Interrogation Group, 9 Dec 2010 w/ chg 1 dated 15 Nov 2013)

-- Also, an interagency body that collects intelligence from key terror suspects to prevent attacks against the United States and its allies. (www.fbi.gov) Also see *National Security Branch*.

> *In response to Task Force recommendations from Executive Order 13491, Ensuring Lawful Interrogations, the High-Value Detainee Interrogation Group was created in 2009 to coordinate law enforcement, military, and intelligence efforts in interrogating key terror suspects. The HIG is housed in the FBI's NSB [National Security Branch], and staffed with members from various IC [Intelligence Community] agencies.*
>
> -- FBI web site at <http://www.fbi.gov/about-us/nsb/national-security-branch-brochure>

High-Value Target (HVT). A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007) Also see *high-payoff target* and *target.*

HOCNet. HUMINT Operational Communication Network (HOCNet) provides information technology, communications, and desktop services for DoD HUMINT needs. (National Intelligence: A Consumer's Guide - 2009)

Homegrown Violent Extremist (HVE). A person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization. (FBI & DHS, cited in CRS Report R42536, 15 May 2012)

> *"HVEs are growing threat to the DoD, as evidenced by numerous disrupted plots targeting DoD facilities, installations, and personnel since 2009. The majority of HVE plots are unsophisticated, use readily available weapons, and target nearby facilities. While they are less likely to generate spectacular, mass casualty attacks than transnational terror groups, HVE attacks are considerably more difficult for law enforcement and intelligence agencies to detect and disrupt."*
>
> -- LTG Michael Flynn, Director, DIA, Annual Threat Assessment [Unclassified], Statement before the Senate Armed Services Committee, 18 April 2013, p.10

Homegrown Terrorist. As defined by the Congressional Research Service, homegrown describes terrorist activity or plots perpetrated within the United States or abroad by American citizens, legal permanent residents, or visitors radicalized largely within the United States. (CRS Report R41416, 23 Jan 2013)

> *American Jihadist Terrorism: Combating a Complex Threat*, CRS Report R41416, 23 Jan 2013 available online at: <http://www.fas.org/sgp/crs/terror/R41416.pdf>
>
> _____
>
> *The term "homegrown terrorism" means the use, planned use, or threatened use, of force or violence by a group or individual born, raised, or based and operating primarily within the United States or any possession of the United States to intimidate or coerce the United States government, the civilian population of the United States, or any segment thereof, in furtherance of political or social objectives.*
>
> -- House Bill 1955, 110th Congress, 24 Oct 2007
>
> _____
>
> *[T]he long war on terrorism is far from over. Most disturbingly, an increasing number of Islamist-inspired terrorist attacks are originating within America's borders. The rise of homegrown extremism is the next front in the fight against terrorism and should be taken seriously by the Administration.*
>
> -- The Heritage Foundation, Special Report No. 137, *60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism*, 22 July 2013

Homeland. The physical region that includes the continental United States, Alaska, Hawaii, United States territories, and surrounding territorial waters and airspace. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

Homeland Defense (HD). The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression, or other threats as directed by the President. (JP 1-02 and JP 3-27, Homeland Defense, 29 Jul 2013)

Homeland Security (HS). A concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur. (JP 3-27, Homeland Defense, 29 Jul 2013)

-- Also, a concerted national effort to prevent terrorist attacks within the United Sates, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (National Strategy for Homeland Security, Oct 2007).

-- Also, describes the intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, law enforcement, customs, border control, and immigration. (Quadrennial Homeland Security Review Report, Feb 2010)

-- Also, defensive efforts to counter terrorist threats. (National Strategy for Counterterrorism, 2011)

In the years since 9/11, homeland security has become commonly and broadly known as both a term and as a Federal department.

Homeland security is a concerted effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive. Ultimately, homeland security is about effectively managing risks to the Nation's security.

-- Quadrennial Homeland Security Review Report, Feb 2010

The *Quadrennial Homeland Security Review Report* (Feb 2010) is available online at: <http://www.dhs.gov/xabout/gc_1208534155450.shtm>

According a Jan 2013 Congressional Research Service (CRS) report, the U.S. government does not have a single definition for "homeland security." Currently, different strategic documents and mission statements offer varying missions that are derived from different homeland security definitions. The concept of homeland security has evolved over the last decade.

-- See CRS Report R42462, 8 Jan 2013 (accessed 9 Jan 2013)
copy available at: <http://www.fas.org/sgp/crs/homesec/R42462.pdf>

Homeland Security Information. Any information possessed by a Federal, State, or local agency that: a) relates to the threat of terrorist activity; b) relates to the ability to prevent, interdict, or disrupt terrorist activity; c) would improve the identification or investigation of a suspected terrorist organization; or d) would improve the response to a terrorist act. (Homeland Security Act, § 891)

Honey Pot. A trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource of value to attackers. (JP 1-02 and JP 3-13.4, Military Deception)

-- Also, a system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, in computer terminology, a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network but which is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource that would be of value to attackers. (Wikipedia; accessed 18 Jan 2011)

Honey Trap. The term universally applied to operations undertaken to ensnare an unwary target in a compromising sexual encounter that may leave the victim vulnerable to blackmail that might result in espionage. (*Historical Dictionary of Cold War Counterintelligence*, 2007) .

-- Also, slang for use of men or women in sexual situations to intimidate or snare others. …[U]se of sex to trap or blackmail an individual…. (Spy Book)

-- Also, an often-used espionage technique wherein a person is deliberately targeted for sexual entrapment. (*Encyclopedia of the CIA*, 2003)

> *Pravda* (the Russian news organization) reported on the use of sexual blackmail by the KGB (Soviet Foreign Intelligence Service), see "KGB Sex Espionage," *Pravda*, 7 Aug 2002.
>
> _____
>
> Honey Trap -- *a strategy regularly adopted by the KGB's Second Chief Directorate which routinely attempted to entrap Western businessmen, foreign diplomats, and other visitors in Moscow, the techniques included the deployment of attractive women, known as "Swallows," and men, referred to as "Romeos," who homed in on vulnerable women, often lonely secretaries with access to classified information.*
>
> -- Nigel West, *Historical Dictionary of Cold War Counterintelligence*, 2007, p. 155
>
> _____
>
> The use of sex is *"a common practice among intelligence services all over the world. This is a tough dirty business. We have used that technique against the Soviets. They have used it against us."*
>
> -- Former Assistant FBI Director William C. Sullivan
> Testimony before the Church Committee, United States Senate, 1 November 1975

Horizontal Identification. [Proposed DoD definition] consistent determination of CPI across two or more RDA programs as a result of a former CPI identification process. (*Draft* 5200.39 CPI Identification and Protection within RDA Programs)

Horizontal Integration. Processes and capabilities to acquire, synchronize, correlate, and deliver National Security Community data with responsiveness to ensure success across all policy and operational missions. (CJCSI 3340.02, Horizontal Integration of Warfighter Intelligence, 23 Dec 2005)

Horizontal Protection. The process which ensures that critical program information (CPI) associated with two or more acquisition programs is protected to the same degree by all responsible DoD agencies. (AR 381-20, Army CI Program, 25 May 2010) Also see *critical program information*.

-- Also, [proposed DoD definition] application of a consistent level of protection to similar CPI associated with more than one RDA program, including inherited CPI. (*Draft* DoDI 5200.39, CPI Identification and Protection within RDA Programs)

Horizontal Protection Analysis. The process that determines if critical Defense technologies, to include CPI [critical program information], associated with more than one RDA [research, development & acquisition] program are protected to the same degree by all involved DoD activities. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008 with change 1 dated 28 Dec 2010)

> Horizontal protection within DoD is focused on ensuring that research, development and acquisition (RDA) information associated with more than one research and technology activity or acquisition program is protected to the same degree by all DoD activities, or is adequately protected based on the impact of an aggregation of the correlated information.

Host Country. A nation which permits, either by written agreement or official invitation, government representatives and/or agencies of another nation to operate, under specified conditions, within its borders. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 chg 1 dated 26 Aug 2011)

Host Nation (HN). A nation that receives the forces and/or supplies of allied nations, coalition partners, and/or NATO organizations to be located on, to operate in, or to transit through its territory. (JP 1-02)

Host-Nation Support (HNS). Civil and/or military assistance rendered by a nation to foreign forces within its territory during peacetime, crises or emergencies, or war based on agreements mutually concluded between nations. (JP 1-02 and JP 4-0, Joint Logistics, 18 Jul 2008)

Hostage Rescue (HR). A personnel recovery method used to recover isolated personnel who are specifically designated as hostages. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

Hostile Act. An attack or other use of force against the United States, United States forces, or other designated persons or property to preclude or impede the mission and/or duties of United States forces, including the recovery of United States personnel or vital United States Government property. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

Hostile Environment. Operational environment in which hostile forces have control as well as the intent and capability to effectively oppose or react to the operations a unit intends to conduct. (JP 1-02)

Hostile Intent. The threat of imminent use of force against the United States, United States forces, or other designated persons or property. (JP 1-02 and JP 3-01, Countering Air and Missile Threats, 23 Mar 2012)

HotR. DoD acronym for HUMINT On-Line Tasking and Reporting System. HotR is a web-based software application that supports DoD HUMINT, as well as DoD Counterintelligence.

House Permanent Select Committee on Intelligence (HPSCI). A committee of the US House of Representatives, established by House Resolution 658 on July 14, 1977. It is the primary committee in the U.S. House of Representatives charged with the oversight of the US Intelligence Community and intelligence-related activities of all other government organizations. Also see *Senate Select Committee on Intelligence.*

> The 1980 Intelligence Oversight Act charged the Senate Select Committee on Intelligence and HPSCI with authorizing the programs of US intelligence agencies and overseeing their activities.
>
> *It is IC policy that IC elements shall, in a timely manner, keep the Congressional intelligence committees fully informed, in writing, of all significant anticipated intelligence activities, significant intelligence failures, significant intelligence activities, and illegal activities.*
>
> -- ICD 112, *Congressional Notification*, 16 Nov 2011

Human Derived Information (HDI). Activities related to the conduct of the collection of intelligence information by or through humans. It includes the following forms of information: FI, CI, Force Protection, Research and Technology Protection, and Law Enforcement. (SECNAVINST S3821.1, 19 Nov 2008)

Human Domain. The presence, activities, social structure or organization, networks and relationships, motivation, intent, vulnerabilities and capabilities of individuals or groups.

> *The human domain encompasses the totality of the physical, cultural, and social environments that influence human behavior. Success in the human domain will depend upon understanding the human terrain and establishing trust with those humans who occupy that space.*
>
> -- Navy Adm. William H. McRaven, Commander, US Special Operations Command, 5 June 2013
>
> ---
>
> *The Human Domain, or Human Dimension, which is a vital and integral part of ABI [Activity Based Intelligence], is defined as the presence, activities (including transactions - both physical and virtual), culture, social structure/organization, networks and relationships, motivation, intent, vulnerabilities, and capabilities of humans (single or groups) across all domains of the operational environment (Space, Air, Maritime, Ground, and Cyber).*
>
> -- Mark Phillips, "A Brief Overview of Activity Based Intelligence and Human Domain Analytics," (Sep 2012); copy at: <http://trajectorymagazine.com/images/winter2012/A_Brief_Overview_of_ABI.pdf>

Human Enabled Information (HEI). Activities designed to spot, assess and develop platforms which facilitate information collection and other assigned operations. (SECNAVINST S3821.1, 19 Nov 2008)

Human Factors. The physical, cultural, psychological, and behavioral attributes of an individual or group that influence perceptions, understanding, and interactions. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *human domain*.

Human Intelligence (HUMINT). A category of intelligence derived from information collected and provided by human sources [includes HUMINT enabling]. (ICD 1, 1 May 2006; JP 1-02; JP 2-0, Joint Intelligence, 22 Oct 2013; and DoDD S-5200.37, Management and Execution of Defense HUMINT, 9 Feb 2009)

-- Also, a category of intelligence derived from information collected by USG civilian employees or military personnel. Who are trained and certified HUMINT collectors, and assigned to an organization with the mission and authority to collect foreign intelligence from human sources in response to validated intelligence requirements. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, intelligence derived from information collected and provided by human sources. This intelligence includes overt data collected by personnel in diplomatic and consular posts, as well as otherwise unobtainable information collected via clandestine sources of information, debriefings of foreign nationals and U.S. citizens who travel abroad, official contacts with foreign governments, and direct observation. (National Intelligence: A Consumer's Guide - 2009)

-- Also, [from CIA perspective] vital information from human sources acquired by Core Collectors of the National Clandestine Service in response to national intelligence requirements. (www.cia.gov, posted 23 Mar 2009) Also see *national clandestine service*.

-- Also, the collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities. (Army FM 2-0, Intelligence 23 Mar 2010 and FM 2-22.2, CI, Oct 2009)

-- Also, consists of information obtained from individuals who know or have access to sensitive foreign information that has implications for U.S. security interests. (WMD Report, 31 Mar 2005)

-- Also, a category of intelligence, that which is reported by a government information collector, who has obtained it either directly or indirectly from a human source. (IC21, HPSCI Staff Study, 9 Apr 1996)

HUMINT collection is a science and an art.
-- Army FM 2-22.3, *Human Intelligence Collector Operations*

HUMINT – espionage – is the heart of the spy business

Core Mission: Collect foreign intelligence through human sources to fill critical intelligence gaps.

Human Intelligence (HUMINT) is intelligence derived from human beings who may act as both sources and collectors, and where the human is the primary collection instrument. It is a foreign intelligence (FI) collection discipline. HUMINT collectors focus on acquiring information from individuals with access to vital intelligence on the full range of national security issues.

There are two basic types of HUMINT: overt and clandestine. Overt HUMINT methods include, but are not limited to, debriefing, interrogation, elicitation, and observation. Clandestine HUMINT, sometimes referred to as Clan HUMINT, involves intelligence activity using human sources directed towards the acquisition of information through clandestine means, i.e., *espionage*.

"*In overt collection, the collector meets openly with sources as a declared U.S. Government representative. …Clandestine collection is conducted in secret. …After the source is recruited, contact is usually strictly controlled in an effort to elude discovery. The recruitment of a clandestine human source can take months or years, but the leak of a source's information may immediately eliminate access to that source."*

-- U.S. National Intelligence – An Overview 2011, p, 54

The Director CIA serves as the ***National HUMINT Manager*** for the Intelligence Community (IC) with the authority to coordinate, deconflict, and evaluate HUMINT operations across the IC; authorities for clandestine HUMINT delegated to the Director of the National Clandestine Service (NCS); see ICD 300 and ICD 304.

The Director DIA serves as the ***Defense HUMINT Manager*** responsible for providing centralized management of DoD HUMINT.

U.S. FI collection priorities are driven by the National Intelligence Priorities Framework (NIPF); see NSPD 26 and ICD 204. For DoD HUMINT policy see DoDD S-5200.37, *Management and Execution of Defense Human Intelligence (HUMINT) (U)*, 9 Feb 2009 with chg 2.

Foreign intelligence entities worldwide, as well as a variety of non-state actors, commercial enterprises, and regional organizations) use clandestine human intelligence collection to "acquire information" (aka conduct espionage). Typically intelligence entities rely upon specially trained or designated employees, often referred to as "case officers" or "agent handlers" (aka operations officers within CIA) to spot, access, develop, and recruit agents who can provide information that is not publicly available.

Within CIA, Operations Officers (OOs) are certified Core Collectors who collect human intelligence of concern to the U.S. President, policymakers, and military by recruiting and handling clandestine human sources in a secure manner. OOs clandestinely spot, assess, develop, recruit and handle human sources with access to vital intelligence.

-- See <https://www.cia.gov/offices-of-cia/clandestine-service/careers/careers-operations-officer.html>

Human-Source Intelligence (HUMINT). The oldest method for collecting information, this is intelligence derived from human sources. Collection includes clandestine acquisition of photography, documents, and other material; overt collection by personnel in diplomatic and consular posts; debriefing of foreign nationals and US citizens who travel abroad; and official contacts with foreign governments. To the public, HUMINT is synonymous with espionage and clandestine activities. However, most of it is accumulated by overt collectors such as diplomats and military attaches.

The CIA, working closely with the Office of the Director of National Intelligence (ODNI) established the National Clandestine Service (NCS) to improve HUMINT throughout the IC. The NCS serves as the national authority for coordination, de-confliction, and evaluation of clandestine HUMINT operations, both abroad and inside the United States. While the ODNI establishes policy related to clandestine HUMINT, the NCS executes and implements that policy across the Intelligence Community (IC).

-- <http://www.intelligence.gov/about-the-intelligence-community/how-intelligence-works/data-gathering.html>

Human Intelligence is derived from the analysis of foreign positive information collected by a trained HUMINT Collector from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human contacts and informants as a tool, and a variety of collection methods to gather information that satisfies the commander's critical information requirements (CCIR) and cues other collection resources.

-- Colonel Jerry W. Jones (USA Retired), "CI and HUMINT or HUMINT and CI or CI/HUMINT or TAC HUMINT," *Military Intelligence Professional Bulletin*, vol. 28, no. 2 (April 2002), p 29.

HUMINT is the oldest collection discipline and a key contributor to the all-source picture of the battlefield. HUMINT is the intelligence, to include adversary intentions, derived from information collected from people and related documents. It uses human sources acquired both passively and actively to gather information to answer intelligence requirements and to cross-cue other intelligence disciplines. HUMINT is produced from the collection on a wide range of requirements with the purpose of identifying adversary capabilities and intentions.

-- U.S. Army ST 2-22.7, Tactical Human Intelligence and Counterintelligence Operations, April 2002, p. 7-4.

The U.S. will continue to need the capabilities to collect HUMINT, especially as a major insight into intentions and plans of hostile states or groups, and to carry out covert action.

-- IC 21: HPSCI Staff Study, 9 Apr 1996 (Finding, p.18)

As George Kisevalter, a CIA case officer who handled defector Col. Oleg Penkovsky, stressed, HUMINT was as much an art as a science, and that "common sense, and the ability to analyze charter quickly and decisively, were the intelligence officer's greatest assets." So too, the mastery of intelligence tradecraft is imperative for success.

-- Julie Anderson, "The HUMINT Offensive from Putin's Chekist State," *International Journal of Intelligence and Counterintelligence*, Vol 20 No 2 (Summer 2007), p. 274

Note: Mr. Kisevalter handled both Major Pyotr Popov, the first Soviet GRU officer run by the CIA, as well as Colonel Oleg Penkovsky. See Clarence Ashley. *CIA SpyMaster* (2004) for the inside story on a CIA legend. .

Counterintelligence (CI) is often mistaken as part of or a subset of HUMINT. Although HUMINT and CI are partners in the Human Domain -- both are intelligence activities that operate in the human domain -- ***they are distinctly different…different missions, different authorities, each focused on different content, as well as outcomes.*** FI collection values the information above all, whereas CI insists on acting on that information--*a totally different operational dynamic*. See *counterintelligence*.

Human Intelligence Collector. See *HUMINT Collector.*

Human Intelligence Source. People who provide intelligence directly; individuals associated with organizations (such as foreign government entities and intelligence services) who willingly share intelligence information with the United States; individuals and organizations who facilitate the placement or service of technical collection means that could not succeed without their support; and foreign citizens who are identified as of an intelligence interest to the United States with a reasonable expectation that they will provide information or services in the future. Information that may reveal the identities of people upon whom the United States relies for information, access to information, or cooperation leading to obtaining information is considered to potentially reveal human intelligence sources. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012) Also see *Human Source, Source*.

Human Source. A person who wittingly or unwittingly conveys by any means information of potential intelligence value. (ICS Glossary) Also see *Human Intelligence Source*; *Source.*

-- Also, a person from whom information can be obtained. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

"Every person—friendly, hostile, or neutral—is a potential source of information. The HUMINT information collection system uses various methods to collect information from a number of sources."

-- U.S. Army ST 2-22.7, *Tactical Human Intelligence and Counterintelligence Operations*, Apr 2002

"[H]uman sources collect the smallest volume of intelligence but generally it is the most difficult to obtain and the most useful when we do get it. It is in this area that the best information is acquired on the all-important subject of intentions."

-- General Veron Walters (Former DCI), *Silent Missions* (1978)

Human Source Contact Operations (SCO). HUMINT collection activity directed toward the establishment of human sources who have agreed to meet and cooperate with HUMINT collectors for the purpose of providing information. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

> *SCO sources include: one-time contacts, continuous contacts, and formal contacts from debriefings, liaison, and contact operations. The basic goal of all levels of contact is to collect information in response to collection tasking.*
>
> -- Army FM 2-22.3, *Human Intelligence Collector Operations* (2006)

Human-Source Intelligence. Intelligence obtained from human sources. See *Human Intelligence*.

Human Terrain Analysis. A multidisciplinary approach to describe and predict geospatial and temporal patterns of human behavior by analyzing the attributes, actions, reactions, and interactions of groups or individuals in the context of their environment. (DoDD 3600.01, Information Operations, 14 Aug 2006 with chg 1, 23 May 2011)

HUMINT. See *Human Intelligence*.

HUMINT Collection Activities. Categories include: tactical questioning; screening, interrogation; debriefing; liaison; human source contact operations (SCOs), documents exploitation (DOCEX); and captured enemy equipment (CEE) operations. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

> DoDD S-5200.37 provides overarching policy for all Defense HUMINT collection operations. Also see: DHE-M 3301.001, Vol I, *Collection Requirements, Reporting, and Evaluation Procedures* (U); DHE-M 3301.002, Vol II, *Collection Operations* (U); and Army FM 2-22.3, *Human Intelligence Collector Operations.*

HUMINT Collection Requirement (HCR). A long-term, DoD validated HUMINT collection requirement which supports DoD or IC operational planning, policy- and decision making, intelligence production, and intelligence databases. (DHE-M 3301.001, DIA HUMINT Manual, Vol I, 30 Jan 2009 w/ chg 2)

HUMINT Collection Methods. There are two HUMINT collection methods authorized for use within DoD: overt and clandestine. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

HUMINT Collection Requirement (HCR). A long-term DoD-wide HUMINT collection requirement which supports DoD operational planning, policy- and decision-making, intelligence production, and intelligence databases. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

HUMINT Collection Team (HCT). Element that collects information from human sources. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

HUMINT Collector. A person who is specifically trained and certified for, tasked with, and engages in the collection of information from HUMINT sources for the purposes of answering intelligence information requirements. (DHE-M 3301.001, Vol I: Collection Requirement, Reporting, and Evaluation Procedures, 30 Jan 2009, w/ chg 2 dated 1 Feb 2012)

-- Also, a person who is specifically trained and certified for, tasked with, and engages in the collection of information from individuals (HUMINT sources) for the purpose of answering intelligence information requirements. (Army FM 2-22.3, HUMINT Collector Operations, Sep 2006)

> Within DoD, appropriately trained and certified individuals are the only personnel authorized to conduct HUMINT operations beyond tactical questioning.

HUMINT Enabling. An operational support function in which non-HUMINT intelligence collection operations are facilitated by HUMINT collection platforms.

HUMINT Operations. Intelligence activities, including military source operations, the primary purpose of which is to obtain foreign intelligence information collected and provided by human sources. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013, with chg 1 dated 13 Jun 2013) Also see *human intelligence*.

> DoD HUMINT operations are conducted in response to DoD or national requirements based on the needs of the originator.

HUMINT Operations Cell (HOC). Assigned under the J/G2X to track all HUMINT activities in the area of intelligence responsibility. It provides technical support to all HUMINT collection operations and deconflicts HUMINT collection operations in the AO. (Term previously defined in Army FM 2-0, Intelligence, May 2004)

> For additional information on the HOC see: JP 2-01.2, *CI & HUMINT in Joint Operations (U)*, 16 Mar 2011 (w/ chg 1 dated 26 Aug 2011), p. II-8 (para 3c).

HUMINT Source. A person from which services or intelligence information are obtained. The source may possess either first or second-hand knowledge normally obtained through sight or hearing and may be witting or unwitting. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010) Also see *human source; source*.

-- Also, a person from whom information can be obtained. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

HUMINT Support Element (HSE). A DIA representative or staff element assigned to support a COCOM. An HSE provides liaison and assists the COCOM with HUMINT planning, coordination, collection management, training, and operations. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

HUMINT Targeting. The integration of all-source intelligence and systemic analytic methodologies to identify and develop relevant HUMINT leads in direct support of HUMINT collection operations. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

HUMINT Tasks. Include but not limited to: conducting source operations; liaising with host nation officials and allied counterparts; eliciting information from select sources; debriefing US and allied forces and civilian personnel including refugees, displaced persons, third-country nationals, and local inhabitants; interrogating enemy prisoners of war and other detainees; and initially exploiting documents, media, and material. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

HUMINT Training. Instruction and applied exercises for acquiring and retaining skills and knowledge required in the acquisition of foreign intelligence derived from the collection discipline that uses human beings as both sources and collectors. (DoDI 3305.15, DoD HUMINT Training, 25 Feb 2008)

HUMINT Training Joint Center of Excellence (HT-JCOE). An advanced joint HUMINT training activity that supports HUMINT activities within the DCHE [Defense CI and HUMINT Enterprise]. The HT-JCOE is comprised of HT-JCOE West and HT-JCOE East. The HT-JCOE West operates with the Department of the Army. The JT-JCOE East operates within the [Defense Intelligence Agency]. (DoDI O-5109.95, HT-JCOE, 18 Apr 2012)

Hybrid Threats. Hybrid threats refer to the ability of adversaries—lone attackers, criminal, transnational terrorist organizations, even nation-states—to employ combinations of tactics, technologies, and capabilities to gin an asymmetric advantage. (Quadrennial Homeland Security Review Report, Feb 2010)

-- Also, the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects. (ADRP 3-0, Unified Land Operations, May 2012)

Hyperspectral Imagery (HSI). Term used to describe the imagery derived from subdividing the electromagnetic spectrum into very narrow bandwidths. These narrow bandwidths may be combined with or subtracted from each other in various ways to form images useful in precise terrain or target analysis. (JP 1-02 and JP 2-03, Geospatial Intelligence Support to Joint Operations, 31 Oct 2012).

I ==========

i-Space (Integrated Space): a U.S. Intelligence Community (IC) social networking and collaboration service hosted on JWICS; intended to foster and facilitate collaboration between IC members. Previously known as "A-Space," the transformation to i-Space broadens membership from analyst only to virtually any intelligence professional with access and a mission need. (Intellipedia, accessed 1 Nov 2013)

ICE-mail. Email between organizations over JWICS network. Also referred to as ICE-mail or JWICS email. (National Intelligence: A Consumer's Guide - 2009)

ICON. See *Investigations, Collections and Operations Nexus*.

Identity. The distinguishing characteristics or personality of an individual or facility. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

Identity Intelligence (I2). The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Ideology. Commitment to a competing political or economic system such as Communism. (PERSEREC 1992) Also see divided *loyalties, MICE*.

IDSRS. See *Integrated Defense Source Registry System*.

Illegal. An officer, employee, or agent of an intelligence organization who is dispatched abroad and who has no overt relationship with the intelligence service with which he/she is connected or with the government operations that intelligence service. Term is derived from the fact that the individual is in the host country illegally. (CI Community Lexicon)

-- Also, an intelligence officer or a recruited agent who operates in a foreign country in the guise of a private person, and is often present under false identity. (FBI -- Affidavit: USA vs. Robert Philip Hanssen, 16 Feb 2001)

-- Also*, Illegal Intelligence Officers (IIO)* – individuals who enter a country either by circumventing border controls or by using false documentation. False documents permit the IIO to remain within the country for a long time while being able to withstand extensive background checks and leave the country with minimum official scrutiny. The very nature of the IIO's covert activity makes it extremely difficult for counterintelligence agencies to identify or accurately assess their total strength and potential impact on national security. (AFOSI Manual 71-144, Vol 5, CI Program, 15 May 2009)

"Illegals" have no "easily" detectable contacts with their parent intelligence service. They pose as legitimate residents of the target country and operate without benefits of diplomatic cover.

"In intelligence parlance, an 'illegal' is a spy operating without benefit of diplomatic cover. If caught, an illegal can be prosecuted, imprisoned, or even executed; by contrast, a diplomat can only be declared persona non grata and expelled by the host country."

-- David Wise, *Tiger Trap: America's Secret War with China* (2011), p. 208

"*The illegal is a highly trained specialist in espionage tradecraft. He may be a [foreign] national and/or a professional intelligence officer dispatched to the United States under a false identity."*
-- FBI as cited in Senate Report # 94-755 (aka Church Committee Report), Book I, 26 April 1976, p.164

"*Illegal agents—that is, operatives for whom an alias identity has been systemically developed which enables them to live in the United States as America citizens or resident aliens without our knowledge of their true origins."*
-- Rockefeller Committee Report, June 1975, p. 8

Illegal Net. An intelligence gathering unit operating under the control of an illegal residency. (AFOSI Manual 71-142, OFCO, 9 Jun 2000 and FBI FCI Terms)

Operation GHOST STORIES -- FBI investigation of a network of Russian sleeper agents under non-official cover in the United States. July 2010, the FBI arrest of 10 Russian "illegals" which provided a chilling reminder that espionage on U.S. soil did not disappear when the Cold War ended. The FBI case against the Russian Intelligence operatives went on for more than a decade.

The FBI released dozens of still images, surveillance video clips, and documents related to the investigation, see <http://www.fbi.gov/news/stories/2011/october/russian_103111/russian_103111>

Illegal Residency. An intelligence apparatus established in a foreign country and composed of one or more intelligence officers, which has no apparent connection with the sponsoring intelligence organization or with the government of the country operating the intelligence organization. (ICS Glossary)

Illegal Support Officer. An intelligence officer assigned to a legal residency whose primary function is to support illegal agents by supplying anything needed. A secondary function is the gathering of information and documents that will serve as guidance and models for documentation of future illegal agents. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Imagery. A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations). (JP 1-02 and JP 2-03, GEOINT Support to Joint Operations, 22 Mar 2007)

-- Also, representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Imagery Exploitation. The cycle of processing, using, interpreting, mensuration and/or manipulating imagery, and any assembly or consolidation of the results for dissemination. (JP 1-02.and JP 2-03, GEOINT Support to Joint Operations, 31 Oct 2012)

Imagery Intelligence (IMINT). The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. (JP 1-02 and JP 2-03, GEOINT Support to Joint Operations, 31 Oct 2012) Also see *geospatial intelligence*.

-- Also, IMINT is derived from the exploitation of imagery collected by visual photography, infrared sensors, lasers, multispectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media. (Army FM 2-0, Intelligence, 23 Mar 2010)

-- Also, intelligence that includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. (ODNI, U.S. National Intelligence – An Overview 2011)

> *Imagery Intelligence (IMINT): The National Geospatial-Intelligence Agency (NGA) manages all IMINT activities, both classified and unclassified, within the US Government . This includes requirements, collection, processing, exploitation, dissemination, archiving, and retrieval.*
>
> -- www.intelligence.gov (accessed 13 Aug 2012)
>
> _____
>
> There are two general types of imagery collection platforms:
> + Satellites—compromised of national technical means [NTM] and commercial platforms.
> + Airborne Systems—compromised of national, commercial, theater, and tactical.
>
> There are two general types of imagery sensors:
> + Electro-optical: panchromatic (visible); infrared; special (multispectral & hyperspectral); and polarmetric.
> + Radar: synthetic aperture radar systems that collect and display data either as representations of fixed targets or as moving target indicators.
>
> -- Army FM 2-0, *Intelligence,* 23 Mar 2010, pp. 9-2 & 9-3

Immigration and Customs Enforcement (ICE). The principal investigative arm of the U.S. Department Homeland Security (DHS). Created in 2003 through a merger of the investigative and interior enforcement elements of the U.S. Customs Service and the Immigration and Naturalization Service,

> ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade and immigration. ICE's two principal operating components are Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO).
>
> See ICE website at: <http://www.ice.gov/index.htm>

Impersonal Communication. Communications between a handler and asset which do not involve direct contact. (HDI Lexicon, April 2008)

-- Also, secret communication techniques used between a case officer and a human intelligence asset when no physical contact is possible or desired. (CI Centre Glossary)

> ***Impersonal Communications…***
>
> *[C]landestine techniques to avoid risky face-to-face contact that often employed methods such as dead drops and elaborate systems of signaling readiness to send and receive those caches of information. This system had been used successfully by intelligence services for centuries.*
>
> -- Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present*, 2013, p. 10

Implant. Electronic device or electronic equipment modification designed to gain unauthorized interception of information-bearing emanations. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Implied Task. In the context of joint operation planning, a task derived during mission analysis that an organization must perform or prepare to perform to accomplish a specified task or the mission, but which is not stated in the higher headquarters order. (JP 5-0, Joint Operation Planning, 11 Aug 2011) Also *see essential task; specified task*.

Improvised Explosive Device (IED). A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components. (JP 1-02)

In the Gap. [Tradecraft jargon] Surveillance-free for a few seconds but not as long as a minute. (Spy Dust)

Inadvertent Disclosure. Type of incident involving accidental exposure of information to an individual not authorized access. (CNSS Instruction No. 4009)

-- Also, a set of circumstances or a security incident in which a person has had involuntary access to classified information to which the individual was or is not normally authorized. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Indication and Warning. Within DoD, term changed to "warning." See *warning.*

Indications. In intelligence usage, information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Indicator. In intelligence usage, an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *espionage indicator*.

-- Also, data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, *"Threat Indicator"* any observable action that suggests violent behavior, abnormal disgruntlement, radicalization, or an extreme religious or other ideological worldview. (US Army Tactical Reference Guide, Radicalization into Violent Extremism: *A Guide for Military Leaders*, Aug 2011) Also see *radicalization*, *terrorism*, *violent radicalization.*

Indirect Access. Descriptor used for sources who do not have firsthand access to the information provided and who have come upon it through one or more sub-sources. (DoDI S-5200.42, Defense HUMINT and Related Activities (U), 8 Dec 2009) Also see *direct access*.

Indoctrination (or read-on). An initial indoctrination and/or instruction provided each individual approved to a SAP prior to his exposure concerning the unique nature of program information and the policies, procedures, and practices for its handling. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Induced Defection. Tradecraft jargon for developing and encouraging a foreign official's defection from his country. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

> **"*Inducement" is the jargon used for persuading somebody to defect to you.***
> -- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

Induced Operation. An operation in which a source or agent is established in such a manner as to induce the opposition to recruit him as its agent. (CI Community Lexicon)

Induction. [One of the four basic types of reasoning applied to intelligence analysis, it is the process] of discovering relationships among the phenomena under study. …[it draws] generalizations on the basis of observations or other evidence. (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *abduction; deduction; scientific method.*

> For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003) and *Critical Thinking and Intelligence Analysis* by David Moore, JMIC Press (2006).

Industrial Espionage. The knowing misappropriation of trade secrets related to, or included in, a product that is made for or placed in interstate or foreign commerce to the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret.

-- Also, the act of seeking a competitive, commercial advantage by obtaining a competitor's trade secrets and/or logistics. The acquisition of industrial information through clandestine operations. (DSS Glossary)

> Industrial espionage is criminalized under the Economic Espionage Act of 1996, PL 104-294. See <http://www.gpo.gov/fdsys/pkg/PLAW-104publ294/content-detail.html>
>
> Industrial espionage, or theft of trade secrets, occurs when an actor, intending or knowing that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner by: (1) stealing, or without authorization appropriating, carrying away, concealing, or obtaining by deception or fraud information related to that secret; (2) copying, duplicating, reproducing, destroying, uploading, downloading, or otherwise transmitting that information without authorization; or (3) receiving that information knowing that that information had been stolen, appropriated, obtained or converted without authorization (Section 101 of the EEA, 18 USC § 1832).

Industrial Security. That portion of information security which is concerned with the protection of classified information in the custody of U.S. industry. (DoD 5220.22-M, NISPOM, 28 Feb 2006) Also see *Defense Security Service (DSS); National Industrial Security Program (NISP).*

-- Also, a mutli-disciplinary security program concerned with the protection of classified information developed by or entrusted to U.S. industry. (IC Standard 700-1, 4 Apr 2008 and DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012 w/ chg 1 dated 24 Apr 2013)

Infiltrate. Tradecraft jargon for the act of penetrating a country or organization. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Infiltration. In intelligence usage, placing an agent or other person in a target area in hostile territory. Usually involves crossing a frontier or other guarded line. Methods of infiltration are: black (clandestine); grey (through legal crossing point but under false documentation); and white (legal). (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

Inform and Influence Activities. The integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform United States and global audiences, influence foreign audiences, and affect adversary and enemy decisionmaking. (Army FM 3-13, Inform and Influence Activities, Jan 2013)

Informant. A person who, wittingly or unwittingly, provides information to an agent, a clandestine service, or the police. (ICS Glossary and Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Information. Facts, data, or instructions in any medium or form. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 3-13.1, Electronic Warfare, 25 Jan 2007)

Information and Communications Technology (ICT). Includes but is not limited to information technology as defined in section 11101 of title 40, U.S.C.. The term reflects the convergence of information technology and communications. ICT includes all categories of ubiquitous technology used for gathering, storing, transmitting, retrieving, or processing information (e.g., computing systems, software, mobile telephony, satellite communications, and networks. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD 8500.01E, Information Assurance and CNSSI-4009) Also see *Information Operations*.

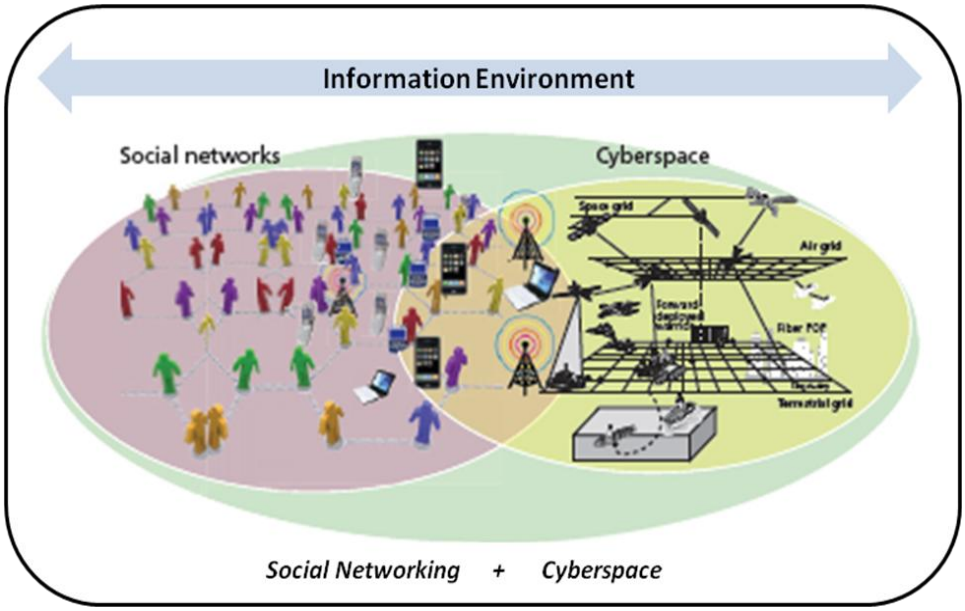
-- Also, actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. (JP 1-02 and JP 3-12, Cyberspace Operations, 5 Feb 2013)

-- Also, protecting information's confidentiality, integrity, and availability. (National Intelligence: A Consumer's Guide - 2009).

-- Also, the protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. IA is a security discipline that encompasses COMSEC, INFOSEC, and control of compromising emanations (TEMPEST). (AR 25-2, Information Assurance, 3 Aug 2007)

Information Collection. An activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination of systems in direct support of current and future operations. (Army FM 3-55, Information Collection, April 2012)

Information Environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02 and JP 3-13, Information Operations, 13 Feb 2006)



-- RAND Graphic

Information Fratricide. The result of employing information-related capabilities in a way that causes effects in the information environment that impede the conduct of friendly operations or adversely affect friendly forces. (Army FM 3-13, Inform and Influence Activities, Jan 2013)

Information Protection. Active or passive measures used to safeguard and defend friendly information and information systems. (ADRP 6-0, Mission Command, May 2012)

Information Operations (IO). The integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries, while protecting our own. (JP 3-13, Information Operation, 27 Nov 2012; approved for inclusion in update to JP 1-02)

For DoD policy see DoDD 3600.01, *Information Operations*, 2 May 2013

Counterintelligence investigations, operations, collection, analysis, production, and dynamic functional CI services are employed in support of appropriate IO activities to detect and mitigate foreign intelligence, hacker, and insider threats to DoD information and information systems.

IO will be the principal mechanism used during military operations to integrate, synchronize, employ, and assess a wide variety of information-related capabilities (IRCs) in concert with other lines of operations to effect adversaries' or potential adversaries' decision-making while protecting our own.

– DoDD 3600.01, *Information Operations*, 2 May 2013

Information Related Capability (IRC). A capability that is a tool, technique, or activity employed within a dimension(s) of the information environment that can be used to achieve a specific end(s). (DoDD 3600.01, Information Operations, 2 May 2013) Also see *information operations*.

Information Requirements. In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *intelligence requirement; collection requirement.*

The requirements process has traditionally been one of the most vexing aspects of intelligence management.

-- IC 21: HPSCI Staff Study, 6 Apr 1996

Information Security. The security discipline concerned with implementation of a system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information that is authorized protection by Executive order, statute, or regulation. Information security includes protection of classified, controlled unclassified, and sensitive compartmented information. (DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012, w/ chg 1 dated 24 Apr 2013)

-- Also, INFOSEC the system of policies, procedures, and requirements established in accordance with Executive Order 13526 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to Executive Order, statute or regulation. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012) Also see *computer security; cyber security.*

-- Also, protecting information's confidentiality, integrity, and availability. (National Intelligence: A Consumer's Guide - 2009)

To be withdrawn from JP 1-02 per JP 3-13, 27 Nov 2012; previously defined as: the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. INFOSEC includes those measures necessary to detect, document, and counter such threats. INFOSEC is composed of computer security and communications security.

-- JP 3-13, *Information Operations*, 13 Feb 2006

INFOSEC plays a vital role in national security and in the Critical Infrastructure

The goal of INFOSEC is to ensure that the National Security Community has reliable and secure networks to originate, store, manipulate, and make information available to those who need it and are authorized to have it.

-- Joint Security Commission II Report, 24 Aug 1999, p. 18

Information Security Oversight Office (ISOO). US Government office that is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program.

The ISOO is responsible to the President for policy and oversight of the Government-wide security classification system and the National Industrial Security Program. The ISOO is also responsible for implementing and overseeing the National Industrial Security Program (NISP) under Executive Order 12829, as amended, issued in 1993.

ISSO web site at: <http://www.archives.gov/isoo/>

Information Superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 1-02 and JP 3-13, Information Operations, 27 Nov 2012) Also see *information operations*.

Informer. One who intentionally discloses information about other persons or activities to police or a security service (such as the FBI), usually for a financial reward. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Infrared Imagery. That imagery produced as a result of sensing electromagnetic radiations emitted or reflected from a given target surface in the infrared position of the electromagnetic spectrum (approximately 0.72 to 1,000 microns). (JP 1-02 and JP 2-03, Geospatial Intelligence Support to Joint Operations, 31 October 2012)

InfraGard. A partnership between the FBI and the private sector. InfraGard is an association of individuals, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. (FBI)

Infragard a collaboration for infrastructure protection. For more information see <http://www.infragard.net/>

Infrastructure. The framework of interdependent physical and cyber-based systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, to the smooth functioning of government at all levels, and to society as a whole. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Inherited CPI. [Proposed DoD definition] CPI that is owned and generated by one RDA program, subsystem, or project that is incorporated into and used by another RDA program. (*Draft* DoDI 5200.39, CPI Identification and Protection within RDA Programs)

Initial Contact Point (ICP). A physical location where an intelligence officer makes an initial contact or brush pass with his source or asset. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Insider. [Within DoD,] anyone who has authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD. (DoDI 5240.26, Countering Espionage, International Terrorism, and Counterintelligence Insider Threat, 4 May 2012 with change 1 dated 15 Oct 2013) Also see *insider threat, CI insider threat.*

-- Also, any person with authorized access to any U.S. Government (USG) resource, to include personnel, facilities, information, equipment, networks, or systems. (U.S. Government Threat Detection Guide - 2011)

-- Also, anyone with access, privilege, or knowledge of information systems or services. Malicious insider is [a person] motivated to intentionally adversely impact an organization's mission (e.g., deny, damage, degrade, destroy). (Rand Study, *Understanding the Insider Threat*, March 2004)

Insider Threat (InT). A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities. (DoDI 5240.26, Countering Espionage, International Terrorism, and Counterintelligence Insider Threat, 4 May 2012 w/ chg 1 dated 15 Oct 2013 and DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012 w/ chg 1 dated 24 Apr 2013) Also see *insider, CI insider threat*.

-- Also, a person, known or suspected, who uses their authorized access to Department of Defense facilities, systems, equipment, information or infrastructure to damage, disrupt operations, commit espionage on behalf of a foreign intelligence entity or support international terrorist organizations. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the threat that an insider will use their authorized access to harm the security of the United States. This threat can include damage to the US through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities [sabotage]. (U.S. Government Threat Detection Guide - 2011 and IC Standard 700-2, 2 June 2011)

-- Also, activities conducted by a person with placement and access that intentionally or unintentionally compromise an agency's ability to accomplish its mission, including but not limited to espionage, other criminal activity, unauthorized disclosure of information and loss or degradation of departmental resources or capabilities. (National CI Strategy Operating Plan 2008-2010, 9 Aug 2007)

-- Also, the ability of a trusted insider to bypass or defeat security safeguards or otherwise adversely affect the national security. (IC Standard 700-1, 4 Apr 2008)

-- Also, an entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a person with placement and access who intentionally or unintentionally causes loss or degradation of resources or capabilities and compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, other criminal activity, or unauthorized release or disclosure of information. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, any insider with legitimate access to government information, personnel, and facilities may intentionally or unintentionally pose a threat. (NSA CI Awareness Pamphlet on Insider Threat, undated)

-- Also, the *insider threat to critical infrastructure* is one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm. (National Infrastructure Advisory Council's Report, *The Insider Threat to Critical Infrastructures*, 8 April 2008)

Trusted insiders with means, motive, and opportunity pose a major threat

"Countering insider threats are coordinated CI, security, information assurance (IA), law enforcement (LE), and antiterrorism & force protection (AT/FP) activities…"

-- DoDI 5240.26, *Countering Espionage, International Terrorism, and the CI Insider Threats*, 4 May 2012

"Insider threats remain the top counterintelligence challenge to our community."

-- Robert "Bear" Bryant, National Counterintelligence Executive

---

"The problem of insider spies has bedeviled intelligence services from time immemorial."

-- David L. Charney. M.D., "True Psychology of the Insider Spy," in *Intelligencer: Journal of U.S. Intelligence Studies* (Fall/Winter 2010), p. 47.

"[H]istory teaches us to expect spies among us and to anticipate that some of those spies will be us…. [W]e cannot eliminate espionage… [but we must] minimize the harm that those who betray us can do to our national security and minimize the time between their defection and detection."

-- Webster Commission Report (A Review of FBI Security Programs), March 2002, pp. 17-18.

"The Insider Threat is the single-most pervasive and damaging security risk facing global organizations and governments today."

-- www.intrusic.com

"Malicious insiders may exploit their access at the behest of foreign governments, terrorists groups, criminal elements, unscrupulous associates, or on their own initiative. Whether malicious insiders are committing espionage, making a political statement, or expressing personal disgruntlement, the consequences for DoD, and national security, can be devastating."

-- *DoD Strategy for Operating in Cyberspace*, July 2011

"…the threat lies in the potential that a trusted employee may betray their obligations and allegiances to their employer and conduct sabotage or espionage against them. Insider betrayals cover a broad range of actions, from secretive acts of theft or subtle forms of sabotage to more aggressive and overt forms of vengeance, sabotage, and even workplace violence. The threat posed by insiders is one most owner-operators neither understand nor appreciate."

-- T. Noonan and E. Archuleta, *The Insider Threat to Critical Infrastructures* , The National Infrastructure Advisory Council, April 6, 2008, p. 32.

"WikiLeaks represents a somewhat different kind of threat. It's an insider threat, as opposed to a remote threat where someone is trying to come across the networks at you."

-- William Lynn, US Deputy Defense Secretary, Interview reported in *DefenseNews*, 18 July 2011

"In addition to threats by foreign intelligence entities, insider threats will also pose a persistent challenge. Trusted insiders with the intent to do harm can exploit their access to compromise vast amounts of sensitive and classified information as part of a personal ideology or at the direction of a foreign government. The unauthorized disclosure of this information to state adversaries, nonstate activists, or other entities will continue to pose a critical threat."

-- DNI, Worldwide Threat Assessment of the US Intelligence Community, SSCI, 29 January 2014

See ONCIX classified report, *U.S. Government Insider Threat Detection Guide – 2011* (U).

See Army Directive 2013-18, Army Insider Threat Program, 31 Jul 2013; copy available at: <http://www.fas.org/irp/doddir/army/insider.pdf>

See SECNAV Instruction 5510.37, Department of the Navy Insider Threat Program, 8 Aug 2013; copy available at: <http://www.fas.org/irp/doddir/navy/secnavinst/5510_37.pdf>

See NCIS *CI & Insider Threat Awareness and Reporting Brief* – Briefers Handbook, March 2013 with DVD (a professionally produced briefing tool for NCIS Agents)

Also see "True Psychology of the Insider Spy," in AFIO *Intelligencer: Journal of U.S. Intelligence Studies* (Fall/Winter 2010), p. 47 -- copy available at < http://www.ncix.gov/issues/ithreat/Charney-PsychologyofInsiderSpyAFIO-INTEL_Fall-Winter2010.pdf >

Additional open source information on insider threat issues at <http://www.cert.org/insider_threat/>

"A nation can survive its fools and even the ambitious.
But it cannot survive treason from within."

-- Cicero (106-43 B.C.)
Speech in the Roman Senate – circa 58 BC

Instruments of National Power. All of the means available to the government in its pursuit of national objectives. They are expressed as diplomatic, economic, informational and military. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02)

Insurgency. The organized use of subversion and violence to seize, nullify, or challenge political control of a region. Insurgency can also refer to the group itself. (JP 3-24, Counterinsurgency, 22 Nov 2013)

-- Also, the organized use of subversion and violence to seize, nullify, or challenge political control of a region. (Army FM 3-24, Insurgencies and Countering Insurgencies, May 2014)

According to FM 3-24, insurgency in the most basic form is a struggle for control and influence, generally from a position of relative weakness, outside existing state institutions. Insurgencies can exist apart from or before, during, or after a conventional conflict.

Insurgent. See *insurgency.*

Integrated Defense Source Registration System (IDSRS). A DoD-level system to enable the sharing of HUMINT source information, meant to ensure Deconfliction of DoD-wide HUMINT sources. (Defense HUMINT Enterprise Manual, Vol II, 23 Nov 2010)

See USD(I) Memo, 13 August 2005 and IDSRS website on SIPRNet at: <http://dh.dia.smil/idsr/>

INTELINK. INTELINK is the classified, worldwide intranet for the U.S. Intelligence Community. At its most secure level, INTELINK utilizes the Joint Worldwide Intelligence Communications System (JWICS) as its communication vehicle. JWICS is a 24 hour a day network designed to meet the requirements for secure multi-media intelligence communications worldwide up to the Top Secret/SCI level.

INTELINK-S. INTELINK-S is similar to INTELINK except that it is accessed through the Secret Internet Protocol Router Network (SIPRNet). It is a 24 hour a day network designed to meet the requirements for secure multi-media intelligence communications worldwide at the Secret level and below.

Intelligence. 1) The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2) The activities that result in the product. 3) The organizations engaged in such activities. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *foreign intelligence; counterintelligence*.

"Intelligence deals with all things which should be known in advance of initiating a course of action"

-- Task Force on Intelligence Activities (Hoover Commission) – 1955

The term "intelligence" includes foreign intelligence and counterintelligence.

-- National Security Act of 1947 (as amended), 50 USC §401a, and EO 12333 (as amended 30 Jul 2008)

The main methods of collecting foreign intelligence (FI), collectively referred to as "intelligence collection disciplines" or the "INTs," are: human intelligence (HUMINT); signals intelligence (SIGINT); geospatial intelligence (GEOINT), including imagery intelligence (IMINT); measurement & signatures intelligence (MASINT); and open source intelligence (OSINT).

Recommended: Mark Lowenthal, PhD, *Intelligence: From Secrets to Policy* (2011, 5th edition)

-- Also, a body of evidence and the conclusions drawn there from that is acquired and furnished in response to the known or perceived requirements of Consumer's. It is often derived from information that is concealed or not intended to be available for use by the acquirer. (ODNI website www.dni.gov)

-- Also, information that has been analyzed and refined so that it is useful to policymakers in making decisions—specifically, decisions about potential threats to our national security. (FBI at <http://www.fbi.gov/about-us/intelligence/defined>)

-- Also, the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (TRADOC Pam 525-2-1, US Army Functional Concept for Intelligence, 13 Oct 10)

-- Also, secret, state activity to understand or influence foreign entities. (Michael Warner, "Wanted: A definition of Intelligence," *Studies in Intelligence,* 46: 3, 2002, pp.15-22)

A plethora of definitions for intelligence

Sherman Kent, former Chairman of CIA's Office of National Estimates asserted that intelligence can be thought of as a process, a product, as well as an organization. His point is valid, as organizations that make up the US Intelligence Community use the term "intelligence" in three different ways—*product, process, and organization*:

1) Intelligence is a ***product*** that consists of information that has been refined to meet the needs of policymakers/decision makers;
2) Intelligence is also a ***process*** through which that information is identified, collected, Analyzed, and disseminated; and
3) Intelligence refers to both the individual ***organizations*** that shape raw data into a finished intelligence product for the benefit of decision makers and the larger community of these organizations collected referred to as the Intelligence Community or IC.

_____

A word of caution about the term "intelligence" is in order. Too often it is used synonymously or interchangeably with "information." This is inaccurate and quite misleading. Information until may be interesting, amusing, or hitherto unknown to the person receiving it, but by and in itself it is inappropriate to call it intelligence.

-- William R. Corson, *The Armies of Ignorance: The Rise of the American Intelligence Empire* (1977)

_____

Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities.

-- Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. 4th Edition (2009), p. 8

[Intelligence is] *mainly secret activities---targeting, collection, analysis, dissemination and action—intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities.*

-- P. Gill, "Theories of Intelligence: Where Are We, Where Should We Go and How Might We Proceed?" in *Intelligence Theory: Key Questions and Debates*, 2009, p. 214

[I]ntelligence in general can be thought of as the complex process of understanding meaning in available information. A typical goal of intelligence is to establish facts and then to develop precise, reliable, and valid inferences (hypotheses, estimations, conclusions, or predictions) for use in strategic decisionmaking or operational planning.

-- Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (2004), p. 13

By definition, intelligence deals with the unclear, the unknown the deliberately hidden…. In the intelligence business, you are almost never completely wrong or completely right.

-- George J. Tenet, Director CIA (5 Feb 2004)

For intelligence to have any real value, it must be acted on, sometimes quite promptly and decisively; otherwise, it can be about as useful as warm spit, regardless how romantic or dramatic it may sound.

-- LTG Samuel Wilson (Retired), Former Director DIA, April 2009

"The truth is that there is never enough good intelligence."

-- R. Jack Smith (Former DDI CIA), *The Unknown CIA* (1989)

"Timely intelligence is a critical component of preserving our national security."

-- Ambassador John D. Negroponte (12 April 2005)

Intelligence Activities. All activities that elements of the Intelligence Community are authorized to conduct pursuant to Executive Order 12333. (EO 12333, as amended 30 Jul 2008) Also see *intelligence*.

-- Also, all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333. (DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect Unites States Persons, Dec 1982)

-- Also, the collection, production and dissemination of foreign intelligence and counterintelligence pursuant to DoDD 5143.01 and EO 12333. (DoDD 5240.01, DoD Intelligence Activities, 27 Aug 2007 w/ chg 1 dated 27 Aug 2013)

Note: Executive Order 12333 (United States Intelligence Activities) specifically defines the term *intelligence* as including foreign intelligence (FI) and counterintelligence (CI).

Intelligence Analysis. The process by which collected information is evaluated and integrated with existing information to facilitate intelligence production. (ADRP 2-0, Intelligence, Aug 2012) Also see *analysis*.

Intelligence analysis is an intellectual process.

-- Mark Lowenthal, PhD

Intelligence Analyst. A professional intelligence officer who is responsible for performing, coordinating, or supervising the collection, analysis, and dissemination of intelligence. (ODNI, U.S. National Intelligence – An Overview 2011)

> *Intelligence analysts use critical and creative thinking to conduct intelligence analysis and produce timely, predictive intelligence.*
>
> -- ADRP 2-0, *Intelligence,* August 2012

Intelligence Asset. Any resource utilized by an intelligence organization for an operational support role. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *asset*.

Intelligence Collection. The acquisition of information or intelligence information and the provision of it to processing and/or production elements. (CI Community Lexicon) Also see *counterintelligence collection*; *clandestine intelligence collection; intelligence collection.*

> The main methods of collecting foreign intelligence (FI), collectively referred to as "intelligence collection disciplines" or the "INTs," are: human intelligence (HUMINT); signals intelligence (SIGINT); geospatial intelligence (GEOINT), including imagery intelligence (IMINT); measurement & signatures intelligence (MASINT); and open source intelligence (OSINT).
>
> _____
>
> *[I]ntelligence collection is an imperfect process and will rarely be able to provide analysts with everything they need to know.*
>
> -- Mark Lowenthal, PhD, "Intelligence Analysis Guide to its Study," *The Intelligencer: Journal of U.S. Intelligence Studies*, Vol 18, No. 4, Summer/Fall 2011, p. 61

Intelligence Collection Activities. The collection of foreign intelligence and counterintelligence information. (Title 10 USC §431)

Intelligence Collection Plan. A plan for gathering information from all available sources to meet an intelligence requirement. Specifically, a logical plan for transforming the essential elements of information into orders or requests to sources within a required time limit. (JP 1-02)

Intelligence Collector. A phrase sometimes used to refer to an individual, system, organization or agency that engages in the collection step of the intelligence cycle. (ICS Glossary)

Intelligence Community (IC). All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. (JP 2-0, Joint Intelligence, 22 Oct 2013 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the federal agencies and departments that have a legal mandate to collect, analyze, and disseminate intelligence. Executive Order 12333 specifically identifies members of the IC. (CI Community Lexicon)

-- Also, a federation of Executive Branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of U.S. national security. (ODNI, U.S. National Intelligence – An Overview 2011)

U.S. Intelligence Community (50 USC §401a and EO 12333)

-- Office of the Director of National Intelligence
-- Central Intelligence Agency
-- National Security Agency
-- Defense Intelligence Agency
-- National Geospatial-Intelligence Agency
-- National Reconnaissance Office
-- Intelligence & CI components of the U.S. Army, Navy, Marines, and Air Force
-- Federal Bureau of Investigation (National Security Branch)
-- Department of Energy (Office of Intelligence & Counterintelligence)
-- Drug Enforcement Administration (Office of National Security Intelligence)
-- Department of Homeland Security (Office of Intelligence & Analysis)
-- Department of State (Bureau of Intelligence & Research)
-- Department of Treasury (Office of Intelligence & Analysis)
-- Intelligence & CI components of the Coast Guard

For additional information see "An Overview of the United States Intelligence Community" at <http://www.dni.gov/who_what/061222_DNIHandbook_Final.pdf>

Also see Jeffrey T. Richelson, *The US Intelligence Community* (2012, 5th Edition)

Intelligence Community Directives (ICDs). Principal issuances through which the Director of National Intelligence (DNI) provides policy direction to the Intelligence Community (IC). (ICD 1, 1 May 2006)

ICDs are overarching policy documents of the Intelligence Community signed by the DNI and are replacing the legacy Director of Central Intelligence Directives (DCIDs).

Intelligence Contingency Funds (ICF). Appropriated funds to be used for intelligence activities when the use of other funds is not applicable or would either jeopardize or impede the mission of the intelligence unit. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dtd 26 Aug 2011)

Intelligence Cycle. The process by which information is acquired, converted into intelligence, and made available to policymakers and Consumer's. (National HUMINT Glossary) Also see *intelligence process*.

-- Also, the steps through which information is converted into intelligence and made available to users. The cycle typically includes six steps: planning and direction, collection, processing and exploitation, analysis and production, dissemination, and evaluation. (ODNI, U.S. National Intelligence – An Overview 2011) [Note: "evaluation" recently added as the sixth step in the cycle.]

INTELLIGENCE CYCLE
Source: CIA
(Note: The sixth step – *evaluation* – is not captured in the above diagram)

The *Intelligence Cycle* is customarily illustrated as a repeating process consisting of [see graphic above].

[1] ***Planning and direction*** encompasses the management of the entire effort and involves, in particular, determining collection requirements based on customer requests.

[2] ***Collection*** refers to the gathering of raw data to meet the collection requirements. These data can be derived from any number and type of open and secret sources.

[3] ***Processing*** refers to the conversion of raw data into a format analysts can use.

[4] ***Analysis and production*** describes the process of evaluating data for reliability, validity, and relevance; integrating and analyzing it; and converting the product of this effort into a meaningful whole, which includes assessments of events and implications of the information collected.

[5] [***Dissemination***] the product is disseminated to its intended audience.

-- Judith Meister Johnston and Rob Johnston., Chapter Four – "Testing the Intelligence Cycle Through Systems Modeling and Simulation," in *Analytic Culture in the U.S. Intelligence Community*, The Center for the Study of Intelligence, CIA, 2005, pp 45-46.

-- Also, the process of developing unrefined data into polished intelligence for the use of policymakers (FBI at <http://www.fbi.gov/about-us/intelligence/intelligence-cycle>)

The "Intelligence" Cycle

[The intelligence cycle is] a series of feedback loops, with analyst at the center. Initial problem definition may come from either a policymaker request or an analyst's assessment that an issue merits analytic attention. The analyst then looks at the data available and ideally may engage in a series of interactions with collectors, a series of feedback loops. While in the collection phase, the analyst should be simultaneously engaging with policymakers or the war fighters, as appropriate, to refine questions as conditions change. When a finished intelligence product is produced, it should generate further questions from the consumer, and the feedback loops continue. The process operates on a continuum, as opposed to a discrete series of events with a defined beginning and end.

-- VADM J.M. (Mike) McConnell, USN (Ret) in CISSM, *The Future of Intelligence Analysis, Volume I Final Report*, 10 March 2006
(CISSM = Center for International and Security Studies at Maryland, University of Maryland)

-- Also, an iterative process in which collection requirements based on national security threats are developed, and intelligence is collected, analyzed, and disseminated to a broad range of customers. Consumers sometimes provide feedback on finished intelligence products, which can be used to refine any part of the intelligence cycle to ensure consumers are getting the intelligence they need to make informed decisions and/or take appropriate actions. (Congressional Research Service (CRS) Report RL33616, 14 Jan 2009)

The Intelligence Cycle – *An Iterative Process*

Source: www.intelligence.gov (accessed 27 Jul 2012)

Intelligence shapes national security policies…

The successful intelligence process converts acquired information into clear, comprehensible intelligence and delivers it to the President, policymakers, and military commanders in a form they can utilize to make educated policy decisions. Generating reliable, accurate intelligence is an active, never-ending process commonly referred to as the intelligence cycle.

The process begins with identifying the issues in which policy makers are interested and defining the answers they need to make educated decisions regarding those issues. We then lay out a plan for acquiring that information and go about collecting it. Once we have the proper intelligence, we sort through it, analyze what it means, and prepare summary reports and recommendations, which we deliver to national security policy makers. The answers our reports supply often reveal other areas of concern, which lead to more questions. In this way, the end of one cycle effectively leads to the start of the next.

-- Intelligence.Gov – How Intelligence Works (accessed 28 April 2011) <http://www.intelligence.gov/about-the-intelligence-community/how-intelligence-works/>

Dynamic Process Fueling Dynamic Solutions

Intelligence Cycle… still valid????

According to Kristan J. Wheaton, Assistant Professor of Intelligence Studies at Mercyhurst University, *"Intelligence professionals have long known that the traditional way of describing the intelligence process, the so called 'intelligence cycle,' is flawed." He concludes the intelligence cycle fails on three counts: "We cannot define what it is and what it isn't, it does not match the way intelligence actually works in the 21st Century, and it does not help us explain our processes to the decision-makers we support. Efforts to fix these flaws have not worked and, furthermore, this is all widely recognized by those who have studied the role and impact of the cycle."*

-- See Kristan J. Wheaton, "Let's Kill the Intelligence Cycle," *Competitive Intelligence,* Vol 15 No 2, April/June 2012, pp. 9-24. See article at <http://mciis.org/files/Wheaton_LetsKillTheIntelligenceCycle.pdf>

Intelligence Database. The sum of holdings of intelligence data and finished intelligence products at a given organization. (JP 1-02 and 2-01, Joint and National Intelligence Support to Military Operations, 5 January 2012)

Intelligence Discipline. A well-defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *human intelligence (HUMINT); geospatial intelligence (GEOINT); measurement and signature intelligence MASINT); signals intelligence (SIGINT); open-source intelligence (OSINT); technical intelligence (TECHINT); counterintelligence (CI)*.

Intelligence Enterprise. The sum total of the intelligence efforts of the entire U.S. intelligence community. (ADRP 2-0, Intelligence, Aug 2012, p. 2-6)

Intelligence Estimate. The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Intelligence Federation. A formal agreement in which a combatant command joint intelligence center receives preplanned intelligence support from other joint intelligence centers, Service intelligence organizations, Reserve organizations, and national agencies during crisis or contingency operations. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Intelligence Gap. Information that is needed to inform intelligence analysis but is absent from reporting—*what we know we don't know*.

-- Also, a missing element that, if found, allows one to choose among alternatives with greater confidence. (Robert M. Clark, *Intelligence Analysis: A Target Centric Approach*, 2004)

Identifying [intelligence] gaps is a continuous and iterative process…
-- Robert M. Clark, *Intelligence Analysis: A Target Centric Approach* (2004), p. 143

Intelligence Information Need. A need, expressed by users of intelligence, for information necessary to support their mission. (Intellipedia)

Intelligence Information Report (IIR). The primary vehicle used to provide HUMINT information to the consumer. It utilizes a message format structure that supports automated data entry into the Intelligence Community databases. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

IIRs contain *raw intelligence*—unevaluated intelligence information, generally from a single source, that has not been fully evaluated, integrated with other information, or interpreted and analyzed.

-- Also, a report used to provide information collected via HUMINT to DoD and IC customers. The IIR utilizes a message format to support automated data entry into IC databases. (DHE-M 3301.001, Vol I: Collection Requirement, Reporting, and Evaluation Procedures, 30 Jan 2009, w/ chg 2 dated 1 Feb 2012)

Intelligence Interrogation. The systematic process of using approved interrogation approaches to question a captured or detained person to obtain reliable information to satisfy intelligence requirements, consistent with applicable law. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *educing information; elicitation; debriefing; interrogation; intelligence interviewing; interview.*

-- Also, the systematic process of using interrogation approaches to question a captured or detained person to obtain reliable information to satisfy foreign intelligence collection requirements. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

> DoD Policy: No person in the custody or physical control of DoD or detained in a DoD facility shall be subject to cruel, inhuman, or degrading treatment or punishment as defined in title XIV of Public Law 109-163, also known as, "The Detainee Treatment Act of 2005." Acts of physical or mental torture are prohibited.
>
> All intelligence interrogations, debriefings, or tactical questioning to gain intelligence from captured or detained personnel shall be conducted humanely, in accordance with applicable law and policy, including Army FM 2-22.3 (*Human Intelligence Collector Operations*, 6 Sep 2006).
>
> ---
>
> Intelligence interrogations and tactical questioning will be conducted only by personnel trained and certified IAW DoDD 3115.09. All DoD interrogations will operate using US Army Field Manual 2-22.3, Human Intelligence Collector Operations.
>
> -- JP 2-01.2, *CI & HUMINT in Joint Operations (U),* 16 Mar 2011 w/ chg 1 dated 26 Aug 2013, p. IV-9
>
> ---
>
> For DoD policy see DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, 11 Oct 2012 with change 1 dated 15 Nov 2013.
>
> Also see *Interrogation: World War II, Vietnam, and Iraq* (Washington, DC: National Intelligence College, Sep 2008); available online at <http://www.ndic.edu/press/12010.htm>

Intelligence Interviewing. The [non-coercive] gathering of useful and accurate information by professionals questioning detainees. (Intelligence Science Board, *Intelligence Interviewing: Teaching Papers and Case Studies*, April 2009) Also see *educing information; elicitation; debriefing; interrogation; interview.*

> See the 2009 Intelligence Science Board report, *Intelligence Interviewing: Teaching Papers and Case Studies*, available online at <www.fas.org/irp/dni/isb/interview.pdf> -- the emphasis of this report is on non-coercive intelligence interviewing.
>
> This report may be of interest to the full range of intelligence professionals involved with interrogation and intelligence interviewing. In particular to those who focus on strategic interrogation and/or "high-value" detainees.

Intelligence Liaison. [Activity which] includes official contacts between a component of the US Intelligence Community and a foreign intelligence or security service which are directly related to espionage or counterintelligence, or other intelligence activities. (DCID 5/1P) Also see *liaison.*

Intelligence Mission Management (IMM). A systematic process by a joint intelligence staff to proactively and continuously formulate and revise command intelligence requirements, and track the resulting information through the processing, exploitation, and dissemination process to satisfy user requirements. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Intelligence Officer (IO). A professionally trained member of an intelligence service. He or she may be serving in the home country or abroad as a member of a legal or illegal residency. (AFOSI Manual 71-142, 9 Jun 2000 and FBI FCI Terms)

-- Also, a professional employee of an intelligence organization engaged in intelligence activities. (ODNI, U.S. National Intelligence – An Overview 2011)

Intelligence Operations. The variety of intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. Intelligence operations include planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

-- Also, the tasks undertaken by military intelligence units and Soldiers to obtain information to satisfy validated requirements. (ADRP 2-0, Intelligence, Aug 2012)

Note: Intelligence consists of two components: foreign intelligence (FI) and counterintelligence (CI). *Intelligence operations* is a broad term with broad application, whereas "CI operations" is a specific term with a precise application.

_____

Intelligence operations are conducted to provide intelligence in support of all missions.

Intelligence operations gain and maintain contact with threat forces; collect signatures and observables to identify, locate, and provide intentions of threat forces and threat networks. Intelligence operations are not solely accomplished from airborne platforms or standoff surveillance sites. They are often executed in and amongst local populations and in close proximity to threat forces and/or groups. Intelligence operations also facilitate understanding of the terrain and civil considerations within an area of operations.

-- U.S. Army TRADOC Pam 525-2-1, US Army Concept for Intelligence 2016-2028, 13 Oct 2010, p. 9

Intelligence Oversight. The process of independently ensuring all DoD intelligence, counterintelligence, and intelligence-related activities are conducted in accordance with applicable U.S. law, E.O.s, Presidential directives, and DoD issuances designed to balance the requirement for acquisition of essential information by the IC, and the protection of Constitutional and statutory rights of U.S. persons. Intelligence Oversight also includes the identification, investigation, and reporting of questionable intelligence activities and S/HS matters involving intelligence activities. (DoDD 5148.11, ATSD/IO, 24 Apr 2013)

Intelligence Planning (IP). The intelligence component of the Adaptive Planning and Execution system, which coordinates and integrates all available Defense Intelligence Enterprise capabilities to meet combatant commander intelligence requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *Counterintelligence Functional Support Plan (CI FSP).*

-- Also, the intelligence portion of Adaptive Planning and Execution (APEX). Intelligence planning provides a process that effectively integrates, synchronizes, prioritizes and focuses Defense intelligence (both Theater and National) on achieving the supported commander's operational objectives and desired effects during all phases of the plan. Additionally, the process identifies knowledge gaps and capability shortcomings within the DoD intelligence community (IC). (CJCSM 3314.01, Intelligence Planning, 28 Feb 2008)

Note: the term "Intelligence Campaign Planning" or "ICP" is no longer in use; the process is now referred to as "Intelligence Planning."

Intelligence Planning Process. The intelligence component of Adaptive Planning. It is a process that integrates, synchronizes, prioritizes, and focuses DoD Intelligence (both theater and national) on achieving the supported commander's operational objectives and desired effects during all phases of an OPLAN or concept plan. Additionally, the process identifies knowledge gaps and capability shortfalls within DoD Intelligence. (DoDI 5105.21, DIA, 18 Mar 2008)

Intelligence Preparation of the Battlespace (IPB). The analytical methodologies employed by the Services or joint force component commands to reduce uncertainties concerning the enemy, environment, time, and terrain. Intelligence preparation of the battlespace supports the individual operations of the joint force component commands. (JP 1-02 and JP 2-01.3, Joint Intelligence Preparation of the Operational Environment) Also see *Joint Intelligence Preparation of the Operational Environment.*

Intelligence Process. The process by which information is converted into intelligence and made available to users. The process consists of six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012) Also see *intelligence cycle*.

-- Also, the Army refers to the intelligence cycle as the "intelligence process," which it defines as: intelligence operations are conducted by performing four steps that constitute the intelligence process: Plan, Prepare, Collect, and Produce. Additionally, there are four continuing activities that occur across the four intelligence process steps: Generate intelligence knowledge, Analyze, Assess, and Disseminate. (See Chapter 4, "Intelligence Process in Full Spectrum Operations," Army FM 2-0, Intelligence, Mar 2010)

-- Also, those steps by which information is collected, converted into intelligence, and disseminated. (Senate Report 95-755, Book I – Glossary, 26 Apr 1976)

Intelligence Processing. Conversion of collected information and/or intelligence into a form more suitable for the production of intelligence. (CI Community Glossary and ICS Glossary)

Intelligence Product. An intelligence report disseminated to customers by an intelligence agency or element. The report contains information and/or analysis of potential intelligence value to meet the intelligence needs of users within and outside the Intelligence Community. It may involve current or future developments or capabilities, intentions, and activities of entities of interest. (ICD 208, 17 Dec 2008)

Intelligence Production. The integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence for known or anticipated military and related national security consumer requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *production*.

-- Also, conversion of material into finished intelligence through the integration, analysis, evaluation, and/or interpretation of all available data and the preparation of intelligence products is support of known or anticipated customer requirements. (CI Community Glossary and ICS Glossary)

Intelligence Reach. The activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command. (ADRP 2-0, Intelligence, Aug 2012)*

* Note: Supersedes the definition in Army FM 2-0, *Intelligence*, 23 Mar 2010

Three important aspects of intelligence reach
are searches and queries, data mining, and collaboration.
-- ADRP 2-0, *Intelligence*, Aug 2012

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). An act to reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purposes. IRTPA established both the position of Director of National Intelligence (DNI) and the National Counterterrorism Center (NCTC). (PL 108-458, 17 Dec 2004)

Link to the IRTPA: <http://www.ncix.gov/publications/law/index.html>

Intelligence-Related Activities. Those activities outside the consolidated defense intelligence program that: respond to operational commanders' tasking for time-sensitive information on foreign entities; respond to national intelligence community tasking of systems whose primary mission is support to operating forces; train personnel for intelligence duties; provide an intelligence reserve; or are devoted to research and development of intelligence or related capabilities. (Specifically excluded are programs that

are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data.) (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Intelligence Report (INTREP). A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

-- Also, a product of the production step of the intelligence cycle. (ICS Glossary)

Intelligence Reporting. The preparation and conveyance of information by any means. More commonly, the term is restricted to reports as they are prepared by the collector and as they are transmitted by the collector to the latter's headquarters and by this component of the intelligence structure to one or more intelligence-producing components. Thus, even in this limited sense, reporting embraces both collection and dissemination. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Intelligence Requirement (IR). 1) Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence; 2) A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *information requirements; collection requirement*.

The articulation of the requirement is the most important part of the process, and it seldom is as simple as it might seem.
– DIA, *Intelligence Essentials for Everyone*, June 1999

-- Also, a requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations (U), 9 Jan 2013 w/ chg 1 dated 13 Jun 2013)

-- Also, [intelligence] requirement: a general or specific validated request for intelligence information made by a user. (National HUMINT Glossary)

-- Also, a type of information requirement developed by subordinate commanders and the staff (including subordinate staffs) that requires dedicated ISR collection for the elements of threat, terrain and weather, and civil considerations. (Army FM 2-0, Intelligence, 23 Mar 2010)

-- Also, the need to collect intelligence information or to produce intelligence, either general or specific, on a particular subject. (ODNI, U.S. National Intelligence – An Overview 2011)

Intelligence Sensemaking. Encompasses the processes by which specialized knowledge about ambiguous, complex, and uncertain issues is created. This knowledge is generated by professionals who in this context become known as Intelligence Sensemakers. (*Sensemaking: A Structure for an Intelligence Revolution* by David T. Moore) Also see *sensemaking*.

Copy of *Sensemaking: A Structure for an Intelligence Revolution* by David T. Moore available at <http://ni-u.edu/ni_press/pdf/Sensemaking.pdf>

Intelligence Source. The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. (JP 2-0, Joint Intelligence, 22 Oct 2013)

An "intelligence source" can be people, documents, equipment, or technical sensors.

Intelligence Sources and Methods. 1) *Sources*: Persons, images, signals, documents, data bases, and communications media capable of providing intelligence information through collection and analysis programs, e.g., HUMINT, IMINT, SIGINT, and MASINT; and 2) *Methods*: Information collection and analysis strategies, tactics, operations and technologies employed to produce intelligence products. If intelligence sources and methods are disclosed without authorization their effectiveness may be substantially negated or impaired. (IC Standard 700-1, 4 Apr 2008)

> The terms "intelligence sources and methods" are used in legislation and executive orders to denote specific protection responsibilities of the Director of National Intelligence (DNI).

Intelligence, Surveillance, and Reconnaissance (ISR). An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations; this is an integrated intelligence and operations function. (DoDD 5143.01; JP 1-02; and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Intelligence Synchronization. The "art" of integrating information collection and intelligence analysis with operations to effectively and efficiently support decisionmaking. (ADRP 2-0, Intelligence, Aug 2012)

Intelligence System. Any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data, and to provide reasoned judgments to decision makers as a basis for action. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Intelligence Task List (ITL). A compilation of the specified and implied intelligence tasks required to satisfy the information needs to support the successful achievement of the Combatant Command's operational objectives. The ITL is developed by the Combatant Command J2 and Defense Intelligence Operations Coordination Center (DIOCC). Assignment of roles and responsibilities for the specific collection, analysis and production is accomplished during the development of the [COCOM's IPLAN] and the NISP. The end state is a synchronized collection, analysis and production effort, from tactical to national level that will support the successful achievement of the Combat Command's operational objectives. (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007)

Intelligence Threat. The intention and capability of any adversary to acquire and exploit critical information. The purpose of the acquisition is to gain a competitive edge or diminish the success of a particular U.S program, operations, or industrial activity. (IOSS Intelligence Threat Handbook - Jun 2004) Also see *threat; threat to national security; transnational threat; foreign intelligence collection threat.*

> *Foreign intelligence services, along with terrorist groups, transnational criminal organizations, and other nonstate actors, are targeting and acquiring our national security information, undermining our economic and technological advantages, and seeking to influence our national policies and processes covertly. These foreign intelligence efforts employ traditional methods of espionage and, with growing frequency, innovative technical means.*
>
> *Among significant foreign threats,* ***Russia*** *and* ***China*** *remain the most capable and persistent intelligence threats and are aggressive practitioners of economic espionage against the United States.*
>
> -- DNI, *Worldwide Threat Assessment of the US Intelligence Community*, SSCI, 12 March 2013

Intellipedia. The Intelligence Community's version of the famous encyclopedia. It is used by analysts, working groups, and engineers throughout the IC. (CIA news release March 2008)

Interagency. United States Government agencies and departments, including the Department of Defense. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011) Also see interagency coordination.

Interagency Coordination. Within the context of DoD involvement, the coordination that occurs between elements of DoD, and engaged US Government agencies and departments for the purpose of accomplishing an objective. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Inter-dependency. [In critical infrastructure usage] relationships or connections between entities of different DoD Components and defense infrastructure sectors. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *intra-dependency*.

Interdiction. 1) An action to divert, disrupt, delay, or destroy the enemy's military surface capability before it can be used effectively against friendly forces, or to otherwise achieve objectives; and 2) In support of law enforcement, activities conducted to divert, disrupt, delay, intercept, board, detain, or destroy, as appropriate, vessels, vehicles, aircraft, people, and cargo. See also air interdiction. (JP 1-02 and JP 3-03, Joint Interdiction, 3 May 2007)

Intergovernmental Organization (IGO). An organization created by a formal agreement (e.g., a treaty) between two or more governments. It may be established on a global, regional, or functional basis for wide-ranging or narrowly defined purposes. Formed to protect and promote national interests shared by member states. Examples include the United Nations, North Atlantic Treaty Organization, and the African Union. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011)

-- Also, an organization comprised primarily of sovereign states (referred to as member states), or of other IGOs. (w/ chg 2 dated 21 Sep 2012, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010)

Internal Security. The state of law and order prevailing within a nation. (JP 1-02 and JP 3-08, Inter-organizational Coordination During Joint Operations, 24 Jun 2011)

International Terrorist Activities. Activities undertaken by or in support of terrorists or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum. (DoD 5240.1-R, 7 Dec 1982)

International Terrorism. Activities that involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a state. Local, or tribal jurisdiction; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by assassination or kidnapping; and occur totally outside the United States, or transcend national borders in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. (50 USC 1810 Section 101(c) and FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

International Traffic in Arms Regulations (ITAR). A set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML). (Wikipedia, accessed 10 Sep 2013)

> ITAR implements the provisions of the Arms Export Control Act (AECA), and are described in Title 22 (Foreign Relations), Chapter I (Department of State), Subchapter M of the Code of Federal Regulations. The Department of State Directorate of Defense Trade Controls (DDTC) interprets and enforces ITAR. Its goal is to safeguard U.S. national security and further U.S. foreign policy objectives.
>
> The related Export Administration Regulations are enforced and interpreted by the Commerce Department. DoD is also involved in the review and approval process. Physical enforcement of import and export laws at border crossings is performed by Customs and Border Protection, an agency of the Department of Homeland Security.
>
> See State Department web site at: http://www.pmddtc.state.gov/regulations_laws/itar_official.html

INTERPOL. The world's largest international police organization, with 188 member countries. Created in 1923, it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime. (www.interpol.int/)

> INTERPOL aims to facilitate international police co-operation even where diplomatic relations do not exist between particular countries. Action is taken within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights. INTERPOL's constitution prohibits "any intervention or activities of a political, military, religious or racial character."

Interpretation. A part of the analysis and production phase in the intelligence process in which the significance of information is judged in relation to the current body of knowledge. (Previously in JP 2-0, Joint Intelligence, 22 Jun 2007)

Interrogation. Systematic effort to procure information by direct questioning of a person under the control of the questioner. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 **w/** chg 1 dated 26 Aug 2011; and Senate Report 94-755, Book I – Glossary, 26 Apr 1976) Also see *educing information; elicitation; debriefing; intelligence interrogation; intelligence interviewing; interview; strategic intelligence interrogation.*

-- Also, interaction and conversation with a source who appears initially unwilling to provide information. (Educing Information – Interrogation: Science and Art, Dec 2006)

-- Also, systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of a person who is in the custody of the forces conducting the questioning. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006 and FM 2-0, Intelligence, 23 Mar 2010)

-- Also [law enforcement interrogation], the systematic effort by law enforcement investigators to prove, disprove, or corroborate information relevant to a criminal investigation using direct questioning in a controlled environment. (FM 19-10 / ATTP 3-39, Law and Order Operations, June 2011)

-- Also, a methodology employed during the interview of a person to obtain information that the source would not otherwise willingly disclose. A typical purpose is not necessarily to force a confession, but rather to develop, playing on the source's character, sufficient rapport as to prompt the source to disclose information valuable to the interrogator. (Wikipedia; accessed 1 Aug 2007)

> Within DoD: Intelligence interrogation is the systematic process of using approved techniques, consistent with applicable law, to question a captured or detained person to obtain reliable information responsive to intelligence requirements. Interrogation is considered an overt HUMINT collection method but is regulated separately from other DoD HUMINT activities.
>
> _____
>
> For DoD policy see DoDD 3115.09, *DoD Intelligence Interrogation, Detainee Debriefings, and Tactical Questioning*, 11 Oct 2012.
>
> Per Executive Order 13491, *Ensuring Lawful Interrogations* (22 Jan 2009), only those interrogation approaches and techniques addressed in U.S. Army FM 2-22.3 are authorized.
>
> U.S. Army FM 2-22.3, *Human Intelligence Collector Operations* (Sep 2006), available online at: <http://www.fas.org/irp/doddir/army/fm2-22-3.pdf>

Interrogation Approach. [In detainee operations] an interrogation technique as identified in U.S. Army Field Manual 2-22.3 that is used by trained and certified interrogators to establish and maintain control over and rapport with a detainee in order to gain the detainee's cooperation to answer the interrogator's questions. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

Interview. [In intelligence usage,] to gather information from a person who is aware that information is being given although there is ignorance of the true connection and purposes of the interviewer. Generally overt unless the collector is other than purported to be. (JP 1-02) Also see *educing information; elicitation; debriefing; intelligence interrogation; intelligence interviewing; interrogation.*

-- Also, a nonstructured discussion, where open-ended questions are asked to determine facts about an incident or crime. (FM 19-10 / ATTP 3-39, Law and Order Operations, June 2011)

-- Also, a dynamic human interaction to collect facts to be used for decision-making and/or action-taking. Interviewing is the gathering of facts/information; it is non-accusatory and less structured than an interrogation.

-- Also, a conversation between two or more people (the interviewer and the interviewee) where questions are asked by the interviewer to obtain information from the interviewee. Interviews can be divided into two rough types, interviews of assessment and interviews for information. (Wikipedia)

> Investigative interview is the process whereby an investigator verbally obtains information from people associated with direct knowledge relevant to the investigation.

Intra-dependency. Relationships or connections between entities of a DoD Component and a defense infrastructure sector. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *inter-dependency*.

Intrusion. [In cyber usage], unauthorized access to a DoD, DIB [defense industrial base], or critical infrastructure network, information system, or application. (DoDI S-5240.23, CI Activities in Cyberspace (U), 13 Dec 2010 with change 1 dated 16 Oct 2013)

-- Also, unauthorized act of bypassing the security mechanisms of a system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also. movement of a unit or force within another nation's specified operational area outside of territorial seas and territorial airspace for surveillance or intelligence gathering in time of peace or tension. (JP 1-02)

Investigation. The systematic inquiry into an allegation of unfamiliar or questionable activities, wherein evidence is gathered to substantiate or refute the allegation or questionable activity. An investigation is initiated when there are articulable facts that indicate a possible violation of law or policy. Some investigations may be conducted unilaterally by an agency (depending on their authorities), jointly with an external investigate body, or referred to an external investigate body for unilateral investigation. (ONCIX Insider Threat Detection – Glossary) Also see *counterintelligence investigation.*

-- Also, the application of law enforcement and/or counterintelligence authorities and methodologies to conduct a detailed, sustained, structured, and objective inquiry to ascertain the truth about an event, situation, or individual. (SECNAVINST 5430.107, Mission & Functions of the NCIS, 28 Dec 2005)

-- Also, the act of investigating; the process of inquiring into or following up; research; study; inquiry, especially patient or thorough inquiry or examination…. (Wiktionary; accessed 28 June 2012)

> *Conducting a successful investigation is often the result of having a wide range of knowledge and using common sense in its application. There are certain actions that apply to all investigations. Investigators follow these intelligent and logical steps to ensure that an investigation is conducted systematically and impartially. There are certain actions that, over time, have proven useful for specific investigations. It is a wise investigator who understands and applies the knowledge, skills, and techniques learned for a particular investigation and uses them wherever they are most useful in any investigation.*
>
> -- FM 3-19.13, *Law Enforcement Investigations*, Jan 2005, p. 1-15

Investigations, Collections & Operations Nexus (ICON). The Air Force's central counterintelligence and counterterrorism analysis center of excellence; an element of the Air Force Office of Special Investigations (AFOSI).

> *The ICON is AFOSI's primary stop for analytical and specialist support for all criminal and counterintelligence investigations and operations. It is the home to AFOSI's 24/7 Global Watch Center and the current Intelligence Desk which produces AFOSI"S flagship publication, the "AFOSI Blue Line." Additionally, the ICON is responsible for acting as the key liaison and interface with National Intelligence and Law Enforcement organizations for AFOSI's CI, CT, criminal, economic crime, and cyber operational issues.*
>
> -- Air Force Office of Special Investigations

Investigative Jurisdiction. Term for the jurisdiction of an investigative agency over a particular crime or over the locus of where the crime was committed. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Investigative Lead. A person who possesses information about or was a witness to an incident under investigation or a record which contains information of value to the investigation. (AR 381-20, Army CI Program, 25 May 2010) Also see *lead*.

Investigative Plan (IP). A detailed plan for the conduct of a CI investigation to ensure that all investigative activity is conducted in a properly sequenced, coordinated, coherent, timely and efficient manner. The plan should outline the actions to be accomplished to resolve an allegation, a report, or information relating to matters under investigation. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, a document used to plan proposed investigative activities, including special investigative techniques, to support counterintelligence investigation. (Army FM 2-22.2, CI, Oct 2009)

> ***Blueprint for a CI Investigation – a tool to describe the purpose & objectives***
>
> *The IP is the equivalent of an operations order for the conduct of a CI investigation.*
>
> -- 902d MI Group Investigations Handbook, Jun 2012, p.94

> *CI investigations will vary is scope, objective, and resources to successfully resolve the incident under investigation. The IP is the document that provides a detailed road map on the conduct of CI investigations including all investigative participants, all investigative activities required, all resources and external support required, and all interagency or legal coordination required to successfully resolve the incident. IPs are living documents and may require revision due to information development and case direction.*
>
> – Army FM 2-22.2, *Counterintelligence*, Oct 2009 (Chapter 2 - CI Investigations, pp. 2-1 thru 2-47)

Investigative Source. See FOUO definition in AR 381-20, Army CI Program (U), 25 May 2010.

Investigative Source Operation (ISO). A controlled counterintelligence operation that may be used in counterintelligence investigations. Also see *counterintelligence investigation*.

> Three types of CI Investigative Source Operations are: role players; collaborative sources; and investigative access sources.
>
> Proposals for the use of an ISO require proper legal review and formal approval. For detailed information see classified Army Regulation 381-20, *Army Counterintelligence Program (U),* 25 May 2010, Chapter 10 - Counterintelligence Operations, paragraph 10 -2 (pp. 44-47).

Irregular Warfare (IW) A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

-- Also, a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will. (DoD 3000.07, Irregular Warfare, 1 Dec 2008)

-- Also, [as defined by Army] a violent struggle among state and nonstate actors for legitimacy and influence over a population. (FM 3-0, Operations, Feb 2008)

ITAR. See *International Traffic in Arms Regulations*.

J ==========

J-2X. The staff element of the intelligence directorate of a joint staff that combines and represents the principal authority for counterintelligence and human intelligence support. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *2X*.

-- Also, a J-2 staff element normally associated with a deployed joint force, consisting basically of the HUMINT operations cell (HOC) and the task force counterintelligence coordinating authority (TFCICA), and the Operational Support Element (OSE). The J-2X is responsible for coordination and deconfliction of all human source-related activity. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Jack-in-the-Box (JIB). A dummy—sometimes inflatable—placed in a car to deceive [surveillance] about the number of persons in the vehicle. (Spy Book)

> *"A three-dimensional human torso sitting atop a spring-activated scissor-lift mechanism fitted with a rotating head, which collapse[s] into a small portable briefcase or duffel bag. " Can be used to effectively elude surveillance by "controlling the location of the event (an empty street…), the lighting (an unlit area), the audience (the trailing surveillance car), the timing (when the cars were a sufficient distance apart), and the sight line (visible only from the rear)."*
>
> -- H. Keith Melton and Robert Wallace, *The Official CIA Manual of Trickery and Deception* (2009)
>
> ---
>
> *"It is used in an automobile to evade surveillance, by deceiving (a) surveillant(s) that a person being tailed is still in the automobile, when, in fact, the jib has replaced him or her. The FBI was allegedly thus deceived while staking out Edward Lee Howard, the former CIA case officer who escaped and subsequently defected to the former USSR."*
>
> -- Leo D. Carl, *The CIA Insider's Dictionary* (1996), p. 319
>
> ---
>
> *"A jib is an inflatable man-sized dummy first employed by the CIA in the early 1980s. It was designed to replace an operative escaping from the inside of a moving vehicle. As the escapee rolls from the passenger side of the vehicle, the jib is employed. Thus, the jib serves as a decoy for pursuers [trailing surveillance team]."*
>
> -- W. Thomas Smith, Jr., *Encyclopedia of the CIA*, 2003

Jihad. Arabic word derived from a verb that means "to struggle, strive, or exert oneself." Violent extremists understand the concept *jihad* as a "religious call to arms." Also see *jihadist*.

> Historically, key Sunni and Shia religious texts most often referred to *jihad* in terms of religious approved fighting on behalf of Islam and Muslims. Most Al Qaeda-produced ideological material reflects Al Qaeda supporters' shared view of *jihad* as an individual duty to fight on behalf of Islam and Muslims, and, in some case, to offensively attack Muslims and non-Muslims who are deemed insufficiently pious or who oppose enforcement of Islamic principles and religious law.
>
> The terms *jihadist, violent Islamist*, and *militant Islamist* refer to groups and individuals whose statements indicate that they share such an understanding of *jihad* and who advocate or use violence against the United States or in support of transnational Islamist agendas.
>
> -- Congressional Research Service (CRS) Report R41674, 8 Mar 2011
>
> ---
>
> *…[J]ihad is a complex term that can be understood in a number of different ways. Traditional Islamic jurisprudence distinguishes between two major levels of jihad. The Greater Jihad refers to the inner struggle of the individual believer to affirm his or her commitment to the requirements of Islam, and is also called jihad of the heart. It is the Lesser Jihad, or jihad of the sword (often translated "holy war," a translation the author scrupulously avoids) that is the central concern of his study.*

Sometimes called the "sixth pillar of Islam," there is no question that jihad is a required commitment of the Muslim. Moreover, although most Qur'anic verses define it as the collective responsibility all Muslims to defend the community against non-Muslim aggressors, there are a few verses, as well as hadith (authentic traditions ascribed to the Prophet Muhammad), that can be interpreted to justify wars of imperial conquest. It is also certainly true that at various times in Islamic history conquerors have used the concept of jihad to justify imperial expansion.

-- Max L. Gross, Dean of the School of Intelligence Studies, Joint Military Intelligence College, and Middle East scholar and intelligence analyst. (As quoted in Joint Military Intelligence College, Discussion Paper 13, entitled *Global War Terrorism: Analyzing the Strategic Threat*, Nov 2004, p. viii-ix).

Jihadist. Term describes radicalized individuals using Islam as an ideological and/or religious justification for their belief in the establishment of a global caliphate, or jurisdiction governed by a Muslim civil and religious leader known as a caliph. (CRS Report R41416, 23 Jan 2013) Also see *jihad*.

Jihadists draw on Salafi Islam—the fundamentalist belief that society should be governed by Islamic law based on the Quran and following the model of the immediate followers and companions of the Prophet Muhammad.

The CRS Report points out there is an important distinction between the terms "radicalization" and "violent extremism" as it relates to the threshold of U.S. law enforcement interest and action. This is because Americans have the right under the First Amendment to adopt, express, or disseminate ideas, even hateful and extremist ones. But when radicalized individuals mobilize their views, i.e., they move from a radicalized viewpoint to membership in a terrorist group, or to planning, materially supporting, or executing terrorist activity, then the nation's public safety and security interests are activated. Thus, the terms may be differentiated as follows:

-- ***"Radicalization"*** describes the process of acquiring and holding radical, extremist, or jihadist beliefs.

-- ***"Violent Extremism"*** describes violent action taken on the basis of radical or extremist beliefs. For many, this term is synonymous with "violent jihadist" and "jihadist terrorist."

The term "violent jihadist" characterizes jihadists who have made the jump to illegally supporting, plotting, or directly engaging in violent terrorist activity.

See CRS Report R41416, *American Jihadist Terrorism: Combating a Complex Threat*. For more on Salafi Islam, see CRS Report RS21695, *The Islamic Traditions of Wahhabism and Salafiyya*.

For more on Al Qaeda's global network, see CRS Report R41070, *Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy*.

Joint. Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (JP1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02)

Joint Base. For purposes of base defense operations, a joint base is a locality from which operations of two or more of the Military Departments are projected or supported and which is manned by significant elements of two or more Military Departments or in which significant elements of two or more Military Departments are located. (JP 1-02 and JP 3-10, Joint Security Operations in Theater, 03 February 2010)

Joint Captured Materiel Exploitation Center (JCMEC). A physical location for deriving intelligence information from captured enemy materiel. It is normally subordinate to the Joint Force/J-2. (JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Joint Counterintelligence Unit (JCIU). An organization composed of Service and Department of Defense agency counterintelligence personnel, formed under the authority of the Secretary of Defense and assigned to a combatant commander, which focuses on the combatant command strategic and operational counterintelligence missions. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, an organization composed of Service and Defense agency CI personnel, formed under the authority of a Secretary of Defense-approved operation order, which focuses on combatant command strategic and operational CI missions within an area of conflict. This unit is under the command authority of the Combatant Commander, or his or her duly designated subordinate joint force commander, for the duration of the operation, or as otherwise specified in the operation plan or order. (DoDI S-5240.09, OFCO, 29 Oct 2008)

For more detailed discussion of the JCIU see Appendix B, Joint Counterintelligence Unit (U), JP 2-01.2, *CI & HUMINT in Joint Operations (U),* 16 Mar 2011 w/ chg 1 dated 26 Aug 2011.

Also see the *Joint Counterintelligence Unit Handbook (U)*, published June 2010 by the Defense CI & HUMINT Center (D2X-ES-C Lessons Learned Branch).

For lessons learned see the following classified reports —
-- (U) *Strategic CI Directorate Iraq (SCID-I) Lesson Learned Report*, 5 Jun 2009
-- (U) *Strategic CI Directorate Afghanistan (SCID-A) Lesson Learned Report*, undated circa Jun 2010)

Note: The transition of Strategic CI Directorates (SCIDs) to Joint CI Units (JCIUs) was not merely a change in title—it fundamentally changed the SCID from a CI organization with no clear chain of command to a CI unit that is directed, controlled, and focused by the Combatant Commander at the operational level of war.

Joint Counterintelligence Training Academy (JCITA). Professional training and education institution for advanced joint DoD CI training. (DoDI 3305.11, DoD CI Training, 19 Mar 2007) See *counterintelligence training.*

-- Also, the primary professional training and education center for advanced and joint CI training within DoD and is known as the DoD Center of Excellence for CI training. (DoDI JCITA, 13 Nov 2013)

JCITA provides advanced counterintelligence training to the Department of Defense and other national security stakeholders agencies within the federal government.

JCITA SIPRNet website at: <https://jcita.dia.smil.mil>

JCITA …training counterintelligence today to protect our nation tomorrow.

Joint Deployable Intelligence Support System (JDISS). A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Joint Doctrine. Fundamental principles that guide the employment of US military forces in coordinated action toward a common objective. Joint doctrine contained in joint publications also includes terms, tactics, techniques, and procedures. It is authoritative but requires judgment in application. (JP 1-02)

Joint Document Exploitation Center (JDEC). A physical location for deriving intelligence information from captured adversary documents including all forms of electronic data and other forms of stored textual and graphic information. It is normally subordinate to the joint force intelligence directorate. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, a joint center established to receive, inventory, catalogue, selectively translate, and disseminate captured or acquired documents and media. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Joint Force. A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander. (JP 1-02)

Joint Force Commander (JFC). A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. (JP1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02) Also see *joint force*.

Joint Intelligence. Intelligence produced by elements of more than one Service of the same nation. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Joint Intelligence Operations Center (JIOC). An interdependent, operational intelligence organization at the Department of Defense, combatant command, or joint task force (if established) level, that is integrated with national intelligence centers, and capable of accessing all sources of intelligence impacting military operations planning, execution, and assessment. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, those centers, below the Defense-level (COCOM and specified Unified Commands) established by the Secretary of Defense on 3 April 2006, to plan, prepare, integrate, direct, synchronize, and manage continuous, full-spectrum defense intelligence operations within their respective AORs. The J2 of each command is designated as the respective JIOC Director. (DIA HUMINT Manual, Vol I, DHE-M 3301.001, 30 Jan 2009 w/ chg 2 dated 1 Feb 2012)

Joint Intelligence Preparation of the Operational Environment (JIPOE). The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. It is a continuous process that includes defining the operational environment; describing the impact of the operational environment; evaluating the adversary; and determining adversary courses of action. (JP 1-02 and JP 2-01.3, Joint Intelligence Preparation of the Operational Environment)

Joint Intelligence Support Element (JISE). A subordinate joint force element whose focus is on intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Joint Intelligence Task Force-Combating Terrorism (JITF-CT). See *Defense Combating Terrorism Center (DCTC).*

In the fall of 2012 the JITF-CT transitioned to the Defense Combating Terrorism Center (DCTC).

Joint Intelligence Training (JIT). Fundamental training that guides the development and utilization of intelligence professionals and organizations designed to support two or more Services employed in coordinated action. (DoDI 3305.14, JIT, 28 Dec 2007)

Joint Inter-Agency Cyber Task Force (JIACTF). Joint inter-agency task force created by the Director of National Intelligence (DNI) to execute DNI responsibilities in monitoring and coordinating the CNCI and to report to the President on Comprehensive National Cybersecurity Initiative (CNCI) implementation, together with recommendations as deemed appropriate. (Securing Cyberspace for the 44th Presidency, Dec 2008)

Joint Interrogation and Debriefing Center (JIDC). Physical location for the exploitation of intelligence information from detainees and other sources. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> JIDCs are established under the direction of the joint force commander within the joint operations area and are normally collocated with detainee holding facilities. The mission of the JIDC is to conduct screening and interrogation of detainees, questioning of walk-in sources, and translation and exploitation of documents associated with detainees. The JIDC coordinates exploitation of captured equipment with the joint captured material exploitation center, captured documents with the joint document exploitation center, and high-value human sources with the joint strategic exploitation center.
>
> For additional information see JP 3-63, *Detainee Operations*, 30 May 2008

Joint Interrogation Operations (JIO). 1) Activities conducted by a joint or interagency organization to extract information for intelligence purposes from enemy prisoners of war, dislocated civilians, enemy combatants, or other uncategorized detainees; or 2) Activities conducted in support of law enforcement efforts to adjudicate enemy combatants who are believed to have committed crimes against US persons or property. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Joint Investigation. An investigation in which more than one investigative agency has established investigative authority over an offense and/or subject of the investigation, and the agencies involved agree to pursue the investigation in concert, with agreements reached detailing investigative responsibilities, procedures, and methods. (CI Community Lexicon)

Joint Operational Planning. Planning activities associated with joint military operations by combatant commanders and their subordinate joint force commanders in response to contingencies and crises. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Joint Operation Planning and Execution System (JOPES). An Adaptive Planning and Execution system technology. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Joint Operation Planning Process (JOPP). An orderly, analytical process that consists of a logical set of steps to analyze a mission, select the best course of action, and produce a joint operation plan or order. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Joint Operations. A general term to describe military actions conducted by joint forces and those Service forces employed in specified command relationships with each other, which of themselves, do not establish joint forces. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Joint Operations Area (JOA). An area of land, sea, and airspace, defined by a geographic combatant commander or subordinate unified commander, in which a joint force commander (normally a joint task force commander) conducts military operations to accomplish a specific mission. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Joint Personnel Adjudication System (JPAS). The centralized database of standardized personnel security processes; virtually consolidates the DoD Central Adjudication Facilities by offering real time information concerning clearances, access, and investigative statuses to authorized DoD security personnel and other interfacing organizations. (IC Standard 700-1, 4 Apr 2008)

-- Also, the centralized Department of Defense database of standardized personnel security processes; virtually consolidates the DoD Central Adjudication Facilities by offering real time information concerning clearances, access, and investigative statuses to authorized DoD security personnel and other interfacing organizations (e.g., Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Management, and the Air Force personnel Center). (DSS Glossary)

Joint Personnel Recovery Center (JPRC). The primary joint force organization responsible for planning and coordinating personnel recovery for military operations within the assigned operational area. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

Joint Strategic Capabilities Plan (JSCP). A plan that provides guidance to the combatant commanders and the Joint Chiefs of Staff to accomplish tasks and missions based on current military capabilities. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Joint Strategic Exploitation Center (JSEC). Theater-level physical location for an exploitation facility that functions under the direction of the joint force commander and is used to hold detainees with potential long-term strategic intelligence value, deemed to be of interest to **counterintelligence** or criminal investigators, or who may be a significant threat to the Unites States, its citizens or interest, or US allies. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> The JSEC is a theater-level exploitation facility and is normally collocated with a rear area collection and holding center for detainees. The JSEC's mission is the conduct of interrogations and debriefings to generate intelligence information responsive to theater and national requirements, and to identify detainees with potential long-term strategic intelligence value, deemed to be of interest to **counterintelligence** or criminal investigators, or who may be a significant threat to the United States, its citizens or interests, or US allies.

Joint Task Force (JTF). A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. (JP 1-02)

Joint Task Force Counterintelligence Coordinating Authority. See *Task Force Counterintelligence Coordinating Authority (TFCICA).*

Joint Terrorism Task Forces (JTTFs). Small cells of highly trained, locally based, investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. It is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. (DoJ website: <http://www.usdoj.gov/jttf/>) Also see *National Joint Terrorism Task Force*.

-- Also, a coordinated "action arm" for federal, state, and local government response to terrorist threats in specific U.S. geographic regions. The FBI is the lead agency that oversees the JTTFs. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, an FBI-led task force whose primary mission is to collect intelligence of actual, suspected, or planned acts of terrorism directed against U.S. persons and property. (DoD FCIP Strategy FY 2013-2017)

> *JTTFs were established by the FBI to conduct operations to predict and disrupt terrorist plots. JTTFs are in over 100 cities nationwide; in addition, there is at least one in each of the FBI's 56 field offices. The National Joint Terrorism Task Force (NJTTF), in Washington, D.C., coordinates all the JTTFs.*
>
> -- ODNI, *U.S. National Intelligence – An Overview 2011*, p. 30
>
> ---
>
> *Joint Terrorism Task Forces (JTTFs) are based in 103 cities nationwide, with at least one in each of the FBI's 56 field offices. They include more than 4,400 members nationwide and represent some 600 state and local agencies and 50 federal agencies.*
>
> -- FBI, *Today's FBI: Facts & Figures 2013-2014*
>
> ---
>
> *DoD CI personnel participating on JTTFs work in partnership with other JTTF members to detect and neutralize terrorists, terrorist-enabling individuals, and organizations threatening DoD interest.*
>
> -- DoDI 5240.22, *CI Support to Force Protection*, 24 Sep 2009, p. 6

Joint Worldwide Intelligence Communications System (JWICS). The sensitive compartmented information portion of the Defense Information Systems Network, which incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, the Intelligence Community's TS-SCI global network; a communications network that delivers secure information services to national and defense intelligence components around the world. All U.S. Government TS-SCI networks run off of JWICS. (National Intelligence: A Consumer's Guide - 2009)

Judgment. [As used in intelligence analysis] Judgment is what analysts use to fill gaps in their knowledge. It entails going beyond the available information and is the principal means of coping with uncertainty. It always involves an analytical leap, from the known into the uncertain. Judgment is an integral part of all intelligence analysis. (*Psychology of Analysis* by Richards J. Heuer, Jr, 1999)

K ==========

Key. A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Key Enabler. That crucial element that supplies the means, knowledge, or opportunity that allows for the success of an assigned task or mission. (USJFCOM Glossary)

Key Facilities List. A register of selected command installations and industrial facilities of primary importance to the support of military operations or military production programs. It is prepared under the policy direction of the Joint Chiefs of Staff. (JP 1-02)

Keystroke Monitoring. The process used to view or record both the keystrokes entered by a computer user and the computer's response during an inactive session. (NIST, Glossary of Key Information Security Terms, May 2013)

Khobar Towers Bombing. A terrorist [truck] bombing of the residence of U.S. military personnel at the Khobar Towers complex in Dhahran, Saudi Arabia, on 25 June 1996 killed 19 American military personnel and wounded hundreds more. (Words of Intelligence, 2nd Edition, 2011)

Knowledge. In the context of the cognitive hierarchy, information analyzed to provide meaning and value or evaluated as to implications for the operation. (FM 6-0, Mission Command, 11 Aug 2003).

Knowledge Management. The process of enabling knowledge flow to enhance shared understanding, learning, and decisionmaking. (ADRP 6-0, Mission Command, May 2012)

Knowledgeability Brief (KB). A document used to notify consumers of the availability and background of an overt source for debriefing. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

L ==========

Laundering. In counterdrug operations, the process of transforming drug money into a more manageable form while concealing its illicit origin. Foreign bank accounts and dummy corporations are used as shelters. (JP 1-02 and JP 3-07.4, Joint Counterdrug Operations, 13 Jun 2007)

-- Also, a process of hiding sources, transmittal, and people involved in financial matters and transfers of money for intelligence and today more commonly for criminal purposes, primarily associated with terrorist activity and narcotics trafficking. (Words of Intelligence, 2nd Edition, 2011)

Law Enforcement. Activities to protect people, places and things from criminal activity resulting from non-compliance with laws, includes patrols, emergency responses, undercover operations, arrests, raids, etc.

-- Also, the generic name for the activities of the agencies responsible for maintaining public order and enforcing the law, particularly the activities of prevention, detection, and investigation of crime and the apprehension of criminals. (www.ojp.usdoj.gov; accessed 29 Apr 2013)

Counterintelligence is part art, part science, a discipline aimed at identifying and exploiting or stopping foreign spies. Law enforcement is easier: You identify the bad guys and arrest them.

-- Bill Gertz, "Enemies," *The Washington Times*, 18 Sep 2006

Traditional law enforcement activities aim at apprehending and prosecuting perpetrators of criminal activity after the commission of their crimes. In most circumstances, the primary responsibility of law enforcement is to determine whether a crime has been committed, conduct an investigation to identify and apprehend the perpetrator, and gather evidence to assist prosecutors in a criminal trial.

Law Enforcement is police work waging a war against crime—*it's evidence-prosecution centric*. Whereas counterintelligence is national security work waging a war against foreign intelligence threats—*it's information-exploitation centric.*

Each operates in fundamentally dissimilar manners… *different legal authorities, oversight structures, governing paradigms, cultures, etc.* These two disciplines merge or intersect when hidden intelligence activity is also criminal, i.e., national security crimes (espionage, treason, spying, etc.).

"Effective enforcement of U.S. espionage statues and Articles 104 and 106 of the Uniform Code of Military Justice is essential to national security…. Services have different approaches to counterintelligence due to their unique missions.… NCIS and AFOSI counterintelligence doctrine holds that counterintelligence primarily is a law enforcement issue. …under Army counterintelligence doctrine, counterintelligence is, first and foremost, an intelligence mission…. Considerable intersection exists between law enforcement, counterintelligence, and intelligence in the areas of espionage, terrorism, and low-intensity conflict…. The law enforcement, counterintelligence, and intelligence collection disciplines must complement one another."

-- "Report of the Advisory Board on the Investigative Capability in the Department of Defense - Vol. I," Department of Defense, January 1995, pp. 67-75.
Copy available online at: <http://handle.dtic.mil/100.2/ADA299523>

The goals of law enforcement and intelligence collection conflict…

"Law enforcement agencies collect information solely to put criminals in prison—a onetime, short-term goal; pay the informant, make a bust, go to trial with the informer as witness. Espionage is conducted for long-term production of intelligence: recruit the agent, collect the information, hopefully for years or decades."

-- Duane R. Clarridge, *A Spy For All Seasons: My Life in the CIA* (1997), p. 409

Law Enforcement Agency (LEA). Any of a number of agencies (outside the Department of Defense) chartered and empowered to enforce US laws in the United States, a state or territory (or political subdivision) of the United States, a federally recognized Native American tribe or Alaskan Native Village, or within the borders of a host nation. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

Law Enforcement Officer. An employee, the duties of whose position are primarily the prevention, investigation, apprehension, or detention of individuals suspected or convicted of offenses against the criminal laws, including an employee engaged in this activity who is transferred to a supervisory or administrative position; or serving as a probation or pretrial services officer. (Cited as 18 USC at <http://www.lectlaw.com/def/l008.htm>)

Law of War. That part of international law that regulates the conduct of armed hostilities. Also called the law of armed conflict. (JP 1-02 and JP 1-04, Legal Support to Military Operations,17 August 2011)

Lawful Search. An examination, authorized by law, of a specific person, property, or area for specified property evidence, or a specific person, for the purpose of seizing such property, evidence or person. (AR 190-30, Military Police Investigation, 1 Nov 2005)

Lead. In intelligence usage, a person with potential for exploitation, warranting additional assessment, contact, and/or development. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *Counterintelligence Operational Lead (CIOL).*

-- Also, an identified potential source. (HDI Lexicon, April 2008 and Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, [for investigative purposes,] single investigative element of a case requiring action. (IC Standard 2008-700-01, 4 Apr 2008)

-- Also, any source of information that, if exploited, may reveal information of value in the conduct of a counterintelligence investigation. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, for CI collection purposes, any person who has the potential to provide information of value to the supported command. (DoD, CI Functional Services IWG Handbook, 19 Feb 2009)

Lead Agency. The US Government agency designed to coordinate the interagency oversight of the day-to-day conduct of an ongoing operation. (JP 1-02 and JP 3-08 Interorganizational Coordination During Joint Operations, 24 June 2011)

-- Also, in CI usage concerning an investigation, the agency in a joint investigation that has primary authority concerning the offense committed or is designated as such by agreement of the investigative agencies involved. The lead agency is ultimately responsible for determination of investigative responsibilities, procedures, and methods. Also see *joint investigation.*

Lead Federal Agency (LFA). The federal agency that leads and coordinates the overall federal response to an emergency. Designation and responsibilities of a lead federal agency vary according to the type of emergency and the agency's statutory authority. (JP 1-02 and JP 3-41, CBRNE Consequence Management, 2 Oct 2006)

Leaks. See *unauthorized disclosure*.

National Security Leaks

"I am deeply disturbed by the continuing leaks of classified information to the media…, disclosures of this type endanger American lives and undermine America's national security."

-- Senator Dianne Feinstein, Chairman of the Senate Intelligence Committee, 5 June 2012

Least Intrusive Means. See *Rule of Least Intrusive Means*. The collection of information about US persons shall be accomplished by the *least intrusive means*.

Legal Attaché (LEGAT). The FBI has offices around the globe. These offices—called legal attachés or legats—are located in U.S. embassies. (fbi.gov) -- See <http://www.fbi.gov/contact-us/legat>

-- Also, the title of FBI special agents deployed abroad to liaison posts in overseas diplomatic missions… (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Legal Residency. An intelligence apparatus in a foreign country composed of intelligence officers assigned as overt representatives of their government, but not necessarily identified as intelligence officers. (ICS Glossary)

Legal Traveler. Any individual traveling with legitimate documentation to perform a specific collection or support mission. (National HUMINT Glossary)

-- Also, any individual traveling with legal documentation to perform specified intelligence collection or support missions, or any individual who may be selected for debriefing on legal travel to or through geographical areas of interest. (AR 381-20, Army CI Program, 25 May 2010)

Legend. The complete cover story developed for an operative. (CI Centre Glossary)

-- Also, a coherent and plausible account of an individual's background, living arrangements, employment, daily activities, and family given by a foreign intelligence service by an illegal or agent. Often the legend will be supported by fraudulent documents. (FBI FCI Terms)

-- Also, false identify that an agent builds up through forged documents and other means such as living under the name of the person whose identify he assumes. (Spy Book)

-- Also, a carefully constructed cover for an intelligence officer. (Spycraft)

-- Also, a spy's fictional identity and a complete cover story developed for operatives. (*Encyclopedia of Cold War Espionage, Spies, and Secret Operations*, 3rd edition, 2012)

Liaison. That contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011) Also see *intelligence liaison*.

-- Also, [activity] conducted to obtain information and assistance, to coordinate or procure material, and to develop views necessary to understand counterparts. Liaison contacts are normally members of the government, military, law enforcement, or other member of the local or coalition infrastructure. The basic tenet of liaison is *quid pro quo*. An exchange of information, services, material, or other assistance is usually a part of the transaction. (Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

A basic tenet of liaison is quid pro quo (something for something exchange.

-- FM 2-22.2, Counterintelligence , October 2009, p. 4-8

"A crucial but often overlooked part of U.S. intelligence efforts is liaison with foreign intelligence services…. A productive liaison relationship does not necessarily preclude spying on each other—but it does mean both sides try to be especially careful not to get caught at it."

-- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)

"*Liaison is not explicitly spelled out in the theoretical approaches [regarding] intelligence. If one looks to the intelligence cycle paradigm, one will even discover that liaison has no fixed location in the cycle… it is actually a mode of activity in every point in the intelligence cycle [and] shares this quality with counter-intelligence*."

-- Dutch Analysts Bob De Graaf and Cees Wiebes in Jeffreys-Jones, *External Vigilance* (1997)

"Answering questions about the costs and benefits of foreign intelligence liaison requires a thorough understanding of the subject in theory and in U.S. practice. Although sometimes equated with intelligence sharing, intelligence liaison is actually better understood as a form of subcontracted intelligence collection based on barter."

-- Dr. Jennifer E. Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," *International Journal of Intelligence and Counterintelligence*, Vol 19 No 2 (Summer 2006), p. 196

"Liaison has a number of associated risks, one being the problem of false corroboration. It is not uncommon for several intelligence services to unwittingly use the same agent."

-- Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (2004), p. 72

Liaison Operations. Operations to coordinate activities and exchange information with foreign military, governmental, and non-governmental civilian agencies. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2011)

According to Army FM 2-22.3 (HUMINT Collector Operations), "liaison operations" are programs to coordinate activities and exchange information with host country and allied military and civilian agencies and NGOs. CI liaison activities are designed to ensure a cooperative operating environment for CI elements and/or to obtain information, gain assistance, develop CI leads for further exploitation, procure material, etc.

Lie. Any statement made with the intent to deceive. (Textbook of Political-Military Counterdeception: Basic Principles & Methods, August 2007)

Light Cover [aka shallow cover]. A type of cover that will not withstand close scrutiny or due diligence. (National HUMINT Glossary)

Line of Operations. 1) A logical line that connects actions on nodes and/or decisive points related in time and purpose with an objective(s). 2) A physical line that defines the interior or exterior orientation of the force in relation to the enemy or that connects actions on nodes and/or decisive points related in time and space to an objective(s). (JP 1-02)

-- Also, a line that defines the directional orientation of a force in time and space in relation to the enemy and links the force with its base of operations and objectives. (Army FM 3-0, Operations, Feb 2008)

Link. A behavioral, physical, or functional relationship between nodes. (JP 1-02)

Link Analysis. Subset of network analysis, exploring associations between objects.

Listening Post. A secure site at which signals from an audio operation are monitored and/or received. (Spycraft)

Load. Tradecraft jargon… to put something in a dead drop; to service a dead drop. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Load Signal. A visual signal to indicate the presence of an individual or object at a given location. (HDI Lexicon, April 2008)

-- Also, …a visual signal displayed in a covert manner to indicate the presence of an individual or object at a given location. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

Local Agency Check (LAC). A review of the appropriate criminal history and court records in jurisdictions over areas where the Subject has resided, attended school, or been employed during a specific period of time. (IC Standard 700-1, 4 Apr 2008) Also see *Military Agency Check; National Agency Check*.

-- Also, a records or files check of official or publicly available information retained by any local office or government agency within the AO [area of operation] of the field element conducting the check. (FM 2-22.2, Counterintelligence, October 2009)

-- Also, a records or files check of official or publicly available information conducted at any local office or government agencies within the operational area of the [CI] field element conducting the check. These records may include holdings and databases maintained by local and state law agencies, local courts, and local offices of federal agencies. (902d MI Group Investigations Handbook, Jun 2012)

-- Also, an investigative check of local police departments, courts, etc., to determine whether the subject has been involved in criminal conduct. The LAC is a part of all Personnel Security Investigations (PSIs) except the Entrance National Agency Check (ENTNAC). (DSS Glossary)

Logic Bomb. A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. (NIST, Glossary of Key Information Security Terms, May 2013)

-- Also, computer jargon for programmed instructions clandestinely inserted into software, where they remain inactive and undetected until the computer reached a certain point in its operations, at which time the instructions take over. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

-- Also, [in cyber usage] also known as a "time bomb," a program that allows a Trojan to lie dormant and then attack when the conditions are just right. Triggers for logic bombs include a change in a file, a particular series of keystrokes, or a specific time or date. (McAfee Labs - Threat Glossary)

Lone Wolf. A lone wolf or lone-wolf fighter is someone who commits violent acts in support of some group, movement, or ideology, but does so alone, outside of any command structure. (Wikipedia; accessed 28 Jun 2011)

The lone wolf – one of the biggest challenges

Individuals who sympathize with or actively support al-Qa'ida may be inspired to violence and can pose an ongoing threat, even if they have little or no formal contact with al-Qa'ida.

-- National Strategy for Counterterrorism, June 2011, p. 4

_____

Lone wolf terrorism involves terrorist attacks carried out by persons who (a) operate individually, (b) do not belong to an organized terrorist group on network, and (c) whose modi operandi are collected are conceived and directed by the individual without any direct outside hierarchy.

-- Flükiger, "The Radical," pp. 111-119.

_____

"Inspire" magazine -- al Qaeda of the Arabian Peninsula's English-language magazine -- has a regular feature called "Open Source Jihad" …that is intended to train… lone wolves and small cells in the West to conduct attacks and to provide them with the tools necessary to do attacks. [This magazine seeks to encourage] …jihadists to conduct lone wolf attacks. Lone wolf assailants are really the most difficult type for government intelligence and security agencies to gather intelligence about. Really to find a lone wolf assailant, you need to monitor his activities closely and understand what's going on inside his head if he doesn't communicate to other people. Because of this, the lone wolf really presents a challenge to Western security and intelligence agencies.

-- Stratfor.com (4 April 2010)
<http://www.stratfor.com/analysis/20110404-dispatch-al-qaedas-inspire-magazine>

A Lone Wolf is characterized by the following operational strengths and weaknesses. First, it is difficult to anticipate who a Lone Wolf is because there is no longer any need for physical contact with extremists for radicalization to occur. As Raffaello Pantucci puts it in his article on Lone Wolves: "The increasing prevalence of the Internet and the easy availability of extremist material online have fostered the growth of the autodidactic extremist." Second, ***the Lone Wolf actor is the most difficult terrorist to detect, deter, or capture, because his planning takes place almost entirely within his own mind*** [emphasis added].

-- Thomas F. Ranieri with Spencer Barrs, "Internet and Ideology: The Military Counterintelligence Challenges of the *Net Wolf*," *American Intelligence Journal*, Vol 29, No 2, 2011, p. 82

Lookout. Stationary position from which a fixed surveillance is conducted and is ostensibly hidden from view or knowledge of the target of the surveillance. (Words of Intelligence, 2nd Edition, 2011)

Low Visibility Operations. Sensitive operations wherein the political-military restrictions inherent in covert and clandestine operations are either not necessary or not feasible; actions are taken as required to limit exposure of those involved and/or their activities. Execution of these operations is undertaken with the knowledge that the action and/or sponsorship of the operation may preclude plausible denial by the initiating power. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

M ==========

M3. Acronym for "Multimedia Message Manager" within the DoD Intelligence Information System (DoDIIS). M3 provides automated text message handling to the military and civilian intelligence community in a classified environment.

> M3 is the standard message handler for the DoDIIS community which provides: real-time dissemination of incoming message traffic based on user interest profiles; retrospective search of archive message database; and message composition, co-ordination, release and validation. M3 software automatically filters and delivers personalized information to individuals and groups, based on their content and delivery preferences. The search software also enables users to search through more than 20 years' worth of stored messages.

Mail Cover. The process by which a record is made of any data appearing on the outside cover of any class of mail matter as permitted by law, other than that necessary for the delivery of mail or administration of the Postal Service. (DoD 5240.1-R, Dec 1982)

-- A record of information on the outside (cover) of any mail piece. It is kept to locate a fugitive, protect national security, or obtain evidence of a crime punishable by a prison term exceeding 1 year. This record is one of the few ways information on mail may be disclosed outside the USPS, and its use is lawful only if authorized by postal regulations. (USPS Pub 32, *Glossary of Postal Terms*, May 1997)

-- Also, an investigative tool used to record information on the outside container, envelope, or wrapper of mail, including the name and address of the sender and the place and date of postmarking. (USPS Publication 146, *A Law Enforcement Guide to the U.S. Postal Service,* Sep 2008)

> Postal Service Regulation 39 CFR § 233.3 is the sole authority and procedure for opening a *mail cover* and for processing, using and disclosing information obtained from a *mail cover*.
>
> See USPS Pub 146, *A Law Enforcement Guide to the U.S. Postal Service* (Sep 2008)* and USPS Pub 55, *USPS Procedures: Mail Cover Requests,* available from the US Postal Service by request to authorized users.
>
> * USPS Pub 146 also available at: <www.hsdl.org/?view&doc=112575&coll=limited>

Make (aka made). Tradecraft jargon… surveillance term for the surveillant being detected by the subject of a surveillance. (Leo D. Carl, The CIA Insider's Dictionary, 1996)

Malicious Code. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. (NIST, Glossary of Key Information Security Terms, May 2013) Also see *malware, Trojan Horse.*

Malicious Cyber Activity. Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. (PPD-20, US Cyber Operation (U), 16 Oct 2012)

Malware. A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. (NIST, Glossary of Key Information Security Terms, May 2013)

-- Also, a generic term used to describe malicious software such as viruses, Trojan horses, spyware, and malicious active content. (McAfee.com; accessed 15 Nov 2010)

-- Also, malicious or malevolent software, including viruses, worms, and Trojans, that is preprogrammed to attack, disrupt, and/or compromise other computers and networks. A packaged exploitation of vulnerability, there is often a "payload" of instructions detailing what the system should do after it has been compromised. (Cybersecurity and Cyberwar)

-- Also, malicious software that secretly accesses a computer system without the owner's informed consent. A general term to mean a variety of forms of hostile, intrusive, or annoying software or program code, including computer viruses, worms, trojan horses, spyware, most rootkits, and other malicious software or program. (Wikipedia)

Malware -- an acronym that stands for MALicious softWARE -- comes in many forms. Generally speaking, malware is software code or snippets of code designed with malice in mind and usually performs "undesirable actions" on a host system.

According to Kevin Coleman, *Defense Systems*, "…in 2009, there were 25 million new strains of malware. That equals a new strain of malware every 0.79 seconds." Recently he blogged that "…in the past month [Sep 2012] there were more than 2,166,000 new strains of malware introduced into our operational environment."

-- Source: <http://defensesystems.com/blogs/cyber-report/2012/09/cyber-threats.aspx?sc_lang=en > (accessed 15 Dec 2012)

According to an article in the *Journal of Homeland and National Security Perspectives*, In 2008, *"a service member in the Middle East inserted a flash drive with malware known as agent.btz into a classified government computer. The worm infected the classified intranets titled Secret Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence communication System (JWICS). The worm had been designed to execute a predetermined search once on the targeted computer system, upon finding the desired data it would transfer it covertly to the thumb drive, and once reinserted into a machine connected to the internet the data immediately transferred from the thumb drive back to the creators of the malware. The foreign intelligence agency that designed this worm, suspected of being Russian Intelligence, created a highly sophisticated worm in agent.btz that could think for itself, morphing when threatened and capable of identifying and using multiple exfiltration paths. Agent.btz is probably not the only malware that has successfully accessed classified American systems. Foreig intelligence agencies are constantly working to develop more advanced intrusion sets, at the same time the U.S. attempts to detect intrusions. It would be irresponsible to assume that U.S. networks are fully secure, and the U.S., and every other nation, will have to deal with that reality for the foreseeable future."*

-- Ashley Tanner, "Examining the Need for a Cyber Intelligence Discipline," *Journal of Homeland and National Security Perspectives* 1:1, 2014

Manipulation. The mixing of factual and fictitious or exaggerated evidence (one of the four deception means for conveying deception information to a target). (CIA, D&D Lexicon, 1 May 2002)

Maritime Domain. All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances. (NSPD-41/HSPD-13, Maritime Security Policy, 21 Dec 2004)

-- Also, the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. (JP 3-32, Command and Control for Joint Maritime Operations, 8 Aug 2006)

Marine Corps Intelligence Activity (MCIA). MCIA provides tailored intelligence and services to the Marine Corps, other services, and the IC based on expeditionary mission profiles in littoral areas. (DoD FCIP Strategy FY 2013-2017)

> For Marine Corps doctrine, tactics, techniques, and procedures on counterintelligence see Marine Corps Warfighting Publication (MCWP) 2-14, *Counterintelligence*, 5 Sep 2000.

Maskirovka. Soviet term -- a set of measures to deceive, or mislead, the enemy with respect to Soviet national security capabilities, actions, and intentions. These measures include concealment, simulation, diversionary actions and disinformation. The Soviet Union doctrine of *maskirovka* calls for the use of camouflage, concealment and deception (CC&D) in defense-related programs and in the conduct of military operations. (NSSD 108, 12 Oct 1983) Also see *deception*.

> *Maskirovka* is actually a very broad concept that encompasses many English terms. These include: camouflage, concealment, deception, imitation, disinformation, secrecy, security, feints, diversions, and simulation. While terms overlap to a great extent, a complication is that the Russian term is greater than the sum of these English terms. Thus, those in the West should attempt to grasp the entire concept rather than its components.
>
> *Maskirovka* is not a new concept in the USSR. Its roots can be traced to the Russian Imperial Army. Several Soviet authors trace it back to Dmitry Donskoy's placing a portion of his mounted forces in an adjacent forest at the Battle of Kulikovo Field in 1380. Seeing a smaller force than anticipated, the Tatars attacked, only to be suddenly overpowered by the concealed force.
>
> -- Charles Smith,"Soviet Maskirovko," *Airpower Journal*, Spring 1988
> Copy available at <http://www.airpower.au.af.mil/airchronicles/apj/apj88/spr88/smith.html>

MCC. See *Military Counterintelligence Collection*.

McCarthyism. The practice of making accusations of disloyalty, subversion, or treason without proper regard for evidence. (<http://en.wikipedia.org/wiki/McCarthyism>; accessed 29 Aug 2012)

> *The term has its origins in the period in the United States known as the Second Red Scare, lasting roughly from 1950 to 1954 and characterized by heightened fears of communist influence on American institutions and espionage by Soviet agents. Originally coined to criticize the anti-communist pursuits of Republican U.S. Senator Joseph McCarthy of Wisconsin, "McCarthyism" soon took on a broader meaning, describing the excesses of similar efforts. The term is also now used more generally to describe reckless, unsubstantiated accusations, as well as demagogic attacks on the character or patriotism of political adversaries.*
>
> -- Source: Wikipedia at <http://en.wikipedia.org/wiki/McCarthyism> (accessed 29 Aug 2012)

Meaconing. A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations. (JP 1-02 and JP 3-13.1, Electronic Warfare, 25 Jan 2007)

Measurement and Signature Intelligence (MASINT). Information produced by quantitative and qualitative analysis of physical attributes of targets and events in order to characterize, and identify them. (ICD 1, Intelligence Community Leadership, 1 May 2006)

-- Also, technically derived intelligence data other than imagery and SIGINT. The data results in intelligence that locates, identifies, or describes distinctive characteristics of targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, information produced by quantitative and qualitative analysis of physical attributes of targets and events in order to characterize, locate, and identify them. MASINT exploits a variety of phenomenolgies to support signature development and analysis, to perform technical analysis, and to detect, characterize, locate, and identify targets and events. MASINT is derived from specialized, technically-derived measurements of physical phenomenon intrinsic to an object or event and it includes the use of quantitative signatures to interpret the data. (DoDI 5105.58, MASINT, 22 Apr 2009)

-- Also, information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify targets and events, and derived from specialized, technically derived measurements of physical phenomenon intrinsic to an object or event. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, describes a category of technically derived information that provides distinctive characteristics of a specific event such as a nuclear explosion, or locates, identifies, and describes distinctive characteristics of targets through such means as optical, acoustic, or seismic sensors. (WMD Report)

MASINT will become increasingly important in providing unique scientific or highly technical information contributions to the IC. It can provide specific weapon identifications, chemical compositions and material content, and a potential adversary's capability to employ weapons.

-- IC21: HPSCI Staff Study, 6 Apr 1996 (p. 40)

MASINT is scientific and technical intelligence information used to locate, identify, or describe distinctive characteristics of specific targets. It employs a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences. For example, MASINT can identify distinctive radar signatures created by specific aircraft systems or the chemical composition of air and water samples.

The Central MASINT Organization, a component of the Defense Intelligence Agency, is the focus for all national and Department of Defense MASINT matters.

-- www.intelligence.gov (accessed 13 Aug 2012)

An excellent open source book on MASINT see: Robert M. Clark, *The Technical Collection of Intelligence*. Washington, DC: CQ Press, 2011.

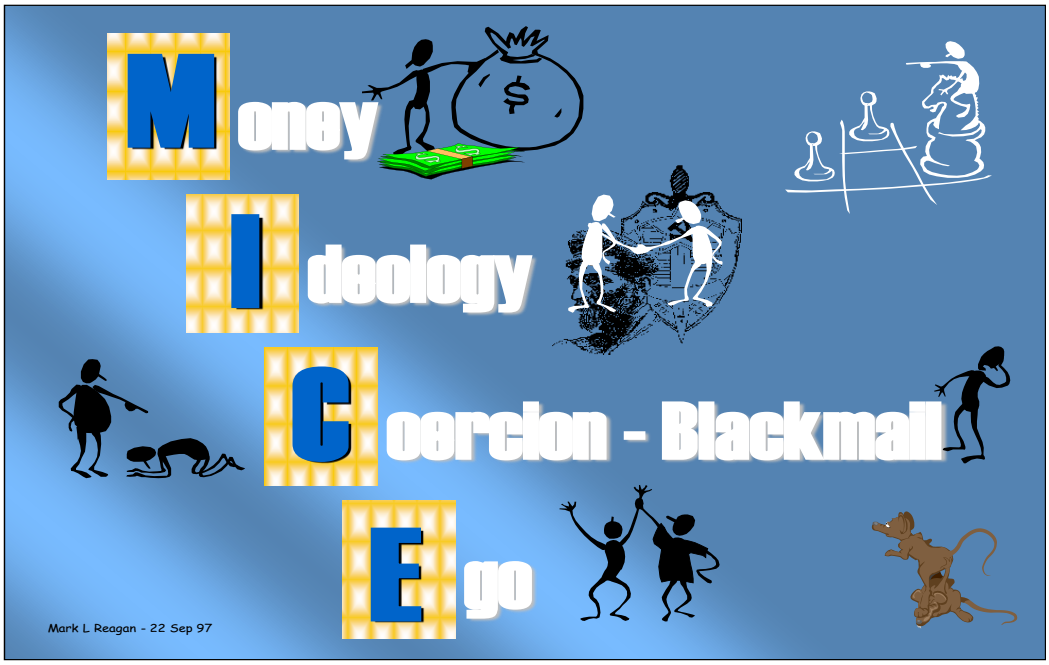
Measures of Effectiveness (MOE). A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Media Exploitation. The receipt, cataloging, duplication, screening/prioritizing, gisting, initial evaluation, translating key pieces of media, uploading data into appropriate data bases, identifying the need for further detailed exploitation of pieces of media, tracking the requested detailed exploitation efforts, and disseminating selected media for further use/analysis by the Intelligence Community. (National Media Exploitation Center CONOPS, Jan 2004)

MI5. British Security Service is responsible for "protecting the UK against threats to national security from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means." (www.mi5.gov.uk/)

MI6. British Secret Intelligence Service (SIS) is responsible for foreign intelligence. MI6 collects secret intelligence and mounts covert operations overseas in support of British Government objectives IAW the UK's Intelligence Services Act of 1994. (www.sis.gov.uk/)

MICE. The commonly used acronym to explain the motivation of traitors. MICE stands for "money, ideology, coercion, and ego," a combination of which may prompt an individual to betray his/her country. (*Historical Dictionary of Cold War Counterintelligence*, 2007) Also see *motivation.*



Motivations for espionage vary

If you add "revenge" to the list above, then the acronym is "CRIME"

"MALICE" is another acronym for **M**oney, **A**nger, **L**ust, **I**deology, **C**ompromise, and **E**go.

"*Spies, being human, often invent a better-sounding motive if their sole reason for betraying their country is money."*

-- General Frantisek Moravec, Former head of Czech Military Intelligence

Microdot. Photographic reduction of documents to three by six millimeters. (FBI FCI Terms) See *Mikrat.*

-- Also, the photographic reduction of writing or other material to facilitate transfer from one location to another without detection. (Spy Book)

-- Also, an optical reduction of a photographic negative to a size that is illegible without magnification, usually 1mm or smaller in area. (Spycraft)

Microdots are another method of surreptitious communication between an agent in the field and his controller. Photographs are reduced down to microscopic size, so that they are practically invisible to the naked eye. Microdots are generally concealed under stamps, on top of punctuation marks in typewritten letters, or under the lips of envelopes.

– Peter Wright, *Spycatcher* (1987), p. 119

Mikrat. Smaller than a microdot. (FBI FCI Terms) See *microdot.*

-- Also, the product of microphotography, as used in microdots. (Spy Book)

Military Agency Check (MAC). A records or files check conducted at any military agency with the AO [area of operations] of the field element conducting the check. (FM2.22-2, Counterintelligence, Oct 2009). Also see *local agency check; national agency check.*

Military Assistance Advisory Group (MAAG). A joint Service group, normally under the military command of a commander of a unified command and representing the Secretary of Defense, which primarily administers the US military assistance planning and programming in the host country. (JP 1-02 and JP 3-22, Foreign Internal Defense, 12 Jul 2010)

Militarily Critical Technology. See *critical technology; militarily critical technologies list; technology.*

Militarily Critical Technologies List (MCTL). A technical reference for the development and implementation of DoD technology security policies on international transfers of defense related goods, services, and technologies as administered by the Director, Defense Technology Security Administration (DTSA). (DoDI 3020.46, MCTL, 24 Oct 2008)

-- MCTL website at <http://www.dtic.mil/mctl/>
-- Also see <http://www.acq.osd.mil/rd/tech_security/mctp/mctl.html>
-- Also see <http://www.dhra.mil/perserec/csg/t1threat/mctl.htm>

Military Counterintelligence Collection (MCC). An CI collection activity using recruited or non-recruited sources to collect information responsive to operational, tactical, and strategic CI requirements, to include those of the Military Departments. (DoDI S-5240.17, CI Collection Activities, 14 Mar 2014) Also see *collection; counterintelligence collection*; *counterintelligence collection activities*.

Military Deception (MILDEC). Deception that is conducted to deliberately mislead adversary and potential adversary decision makers and commanders in order to cause the adversary to take specific actions or inactions that will contribute to the accomplishment of the friendly mission. [This definition is proposed for inclusion in the next edition of JP 1-02]. (DoDI S-3604.01, Department of Defense Military Deception, 11 Mar 2013) Also see *deception, deception in support of OPSEC*.

-- Also, actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006)

-- Also, those actions executed to deliberately mislead adversary decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (Army FM 3-0, Operations, with Chg 1, 2011)

In war-time, truth is so precious that she should always be attended by a bodyguard of lies

-- Winston Churchill (November 1943)

as cited in Anthony Cave Brown, *Bodyguard of Lies: The Extraordinary True Story Behind D-Day* (1975)

MILDEC is conducted to deliberately mislead adversary and potential adversary decision makers and commanders in order to cause the adversary to take specific actions or inactions that will contribute to accomplishment of the friendly mission.

MILDEC can mask, protect, reinforce, exaggerate, minimize, distort, or otherwise misrepresent U.S. technical and operational capabilities, intentions, operations, and associated activities.

According to JP 3-13.4, Counterintelligence provides the following for MILDEC planners:

1) Identification and analysis of adversary intelligence systems to determine the best deception conduits;
2) Establishment and control of deception conduits within the adversary intelligence system, also known as offensive CI operations;
3) Participation in counterdeception operations;
4) Identification and analysis of the adversary's intelligence system and its susceptibility to deception and surprise; and
5) Feedback regarding adversary intelligence system responses to deception operations.

For additional information see Joint Pub 3-13.4, *Military Deception*, 13 Jul 2006

_____

It was Desert Storm that I became convinced of the power of deception in warfare, it truly is a force multiplier.

-- Tommy Franks (General, USA Ret), *American Solider* (2004)

Military Department (MILDEP). One of the departments within the Department of Defense created by the National Security Act of 1947, which are the Department of the Army, the Department of the Navy, and the Department of the Air Force. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Military Department Counterintelligence Organization (MDCO). Elements of the Military Departments authorized to conduct CI investigations, i.e., Army CI, Naval Criminal Investigative Service [NCIS], and the Air Force Office of Special Investigations [AFOSI]. (DoDD 5240.06, CIAR, 17 May 2011 w/ chg 1 and DoDI 5240.10, CI in the Combatant Commands and Other DoD Components, 5 Oct 2011 w/ chg 1)

MDCO, formerly known as "CI Lead Agencies," approved for inclusion in next edition of JP 1-02.

Military Information Support Operations (MISO). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP 1-02 and JP 3-13.2, Psychological Operations, 7 Jan 2010)

Previously known as Psychological Operations or PSYOP; this change directed by SECDEF Memo, subject: Changing the Term Psychological Operations (PSYOP) to Military Information Support Operations (MISO), dated 3 Dec 2010. Also FY2012 National Defense Authorization Act (P.L.112-81) Section 1086, re-designates "psychological operations" as "military information support operations" in Title 10, United States Code, to conform to DoD usage.

Military Intelligence (MI). The collection, analysis, production, and dissemination of information relating to any foreign military or military-related situation or activity that is significant to military policy-making or the planning and conduct of military operations and activities. (DoDD 5143.01, USD/I, 23 Nov 2005)

Military intelligence appears in three basic forms: strategic, operational, and tactical.

-- **Strategic Intelligence**: intelligence that is required for the formulation of strategy, policy, and military plans and operations at the national and theater levels.

-- **Operational Intelligence**: intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas. It focuses on narrower, but significant theater-oriented military responsibilities.

-- **Tactical Intelligence**: intelligence that is required for planning and conducting tactical military operations at the local level. It concerns information about the enemy that is designed to help locate the enemy and decide which tactics, units, and weapons will most likely contribute to victory in an assigned area, and when properly applied, it can be a significant force multiplier.

Military Intelligence Board (MIB). A decision-making forum which formulates Department of Defense intelligence policy and programming priorities. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Military Intelligence Program (MIP). The MIP consists of programs, projects, or activities that support the Secretary of Defense's intelligence, counterintelligence, and related intelligence responsibilities. This includes those intelligence and counterintelligence programs, projects, or activities that provide capabilities to meet warfighters' operational and tactical requirements more effectively. The term excludes capabilities associated with a weapons system whose primary mission is not intelligence. The term "MIP" replaces the terms "Joint Military Intelligence Program (JMIP)" and "Tactical Intelligence and Related Activities (TIARA)." (DoDD 5205.12, MIP, 14 Nov 2008)

> The Joint Military Intelligence Program (JMIP) and the Tactical Intelligence and Related Activities (TIARA) were combined in 2005 to form the MIP.
>
> *"The MIP was established to improve management of Defense Intelligence capabilities and resources. USD/I is the Program Executive for the MIP."*
>
> -- USD/I Memo, subj: Establishment of the MIP, 1 Sep 2005

Military Service. A branch of the Armed Forces of the United States, established by act of Congress, in which persons are appointed, enlisted, or inducted for military service, and which operates and is administered within a military or executive department. The Military Services are: the United States Army, the United States Navy, the United States Air Force, the United States Marine Corps, and the United States Coast Guard. (JP 1-02)

Military Source Operations. The collection, from, by and/or via humans, of foreign, military and military-related intelligence. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, DoD HUMINT collection and operations focused on foreign military and military-related intelligence conducted under the authorities of the Secretary of Defense. Military source operations are conducted by appropriately trained and certified personnel under the control of a Defense HUMINT Executor. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013, with chg 1 dated 13 Jun 2013)

-- Also, the collection from, by, and/or via humans, of foreign military and military-related intelligence conducted under SecDef authorities to satisfy DoD needs. (HDI Lexicon, April 2008)

-- Also, DoD HUMINT activity or operation which is conducted to specifically respond to, and satisfy, DoD intelligence collection requirements. These operations directly support the execution of the Secretary's responsibilities, commanders in the field, military operational planners, and the specialized requirements of the military departments (e.g., research and development process, the acquisition of military equipment, and training and doctrine) and span the entire HUMINT operational continuum, utilizing varying degrees of tradecraft to ensure the safety and security of the operation. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

> Military Source Operations are conducted by trained personnel under the control of Defense HUMINT Executors. See DoDD S-5200.37, *Management and Execution of Defense HUMINT (U),* 9 Feb 2009 for specifics.

Misdirection. A classic conjurer's trick, misdirection is the term applied in the counterintelligence community for the tactic of supplying an ostensibly plausible explanation for an event actually caused by something quite different, probably by an individual or an operation, deemed sufficiently valuable to require protection. Invariably a human asset may produce some information which requires action that could compromise him or her, so misdirection is intended to divert attention elsewhere. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

Misperception. The formation of an incomplete or inaccurate image or perception of some aspect of reality. The faulty image may be formed due to a lack of information or intentionally erroneous information provided to the perceiver. (CIA, D&D Lexicon, 1 May 2002)

Mission. 1) The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore; 2) in common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Mission Assurance. A process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the execution of DoD mission-essential functions in any operating environment or condition. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, the process or state of ensuring the survival of an organization's essential missions and operating capability when confronted by natural or man-made emergencies and disasters. (DoD Strategy for Operating in Cyberspace, May 2011)

Mission Critical Functions. Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed. (DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012)

Mission Manager. A position with the [Intelligence] Community for an individual, operating with the Director's [DNI] authorities, who coordinates all intelligence activities against a specific country or topic [e.g., counterterrorism counterproliferation, counterintelligence]. (HPSCI Report 27 Jul 2006)

-- Also, *Mission Managers* are the principal Intelligence Community officials overseeing all aspects of national intelligence related to their respective mission areas. Mission Managers are designated for counterintelligence, counterterrorism, Counterproliferation, Iran, North Korea, and Cuba & Venezuela. (ICD 900, Mission Management, 21 Dec 2006)

> The NCIX serves as the Mission Manger for Counterintelligence.
> The Director NCTC serves as the Mission Manager for Counterterrorism.

Mission Need. A requirement for access to specific information to perform or assist in a lawful and authorized governmental function. Mission needs are determined by the mission and functions of an IC element or the roles and responsibilities of particular IC personnel in the course of their official duties. (ICD 501, 21 Jan 2009)

Mission Statement. A short sentence or paragraph that describes the organization's essential task(s), purpose, and action containing the elements of who, what, when, where, and why. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *mission*.

Mission Tasking Authority (MTA). See *Counterintelligence Mission Tasking Authority*.

Mitigation. Actions taken in response to a warning or after an incident occurs that are intended to lessen the potentially adverse effects on a given military operation or infrastructure. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. Includes solutions that contain or resolve risks through analysis of threat activity and vulnerability data, which provide timely and accurate responses to prevent attacks, reduce vulnerabilities, and fix systems. (DSS Glossary)

-- Also, capabilities necessary to reduce loss of life and property by lessening the impact of disasters. (PPD-8, 2011)

Modus Operandi (MO). A distinct pattern or method of procedure thought to be characteristic of or habitually followed by an individual or an organization involved in criminal or intelligence activity. (AR 381-20, Army CI Program, 25 May 2010)

> *Modus Operandi*--a Latin phrase--approximately translated as "method of operating." The term is used to describe someone's habits or manner of working, their method of operating or functioning. In English, it is frequently shortened to M.O.

Mole. A member of an organization who is spying and reporting on his/her own organization on behalf of a foreign country; also called a penetration. (National HUMINT Glossary) Also see *mole hunt*; *penetration.*

-- Also, a human penetration into an intelligence service or other highly sensitive organization. Quite often a mole is a defector who agrees to work in place. (CI Centre Glossary)

-- Also, literary and media term for penetration agent infiltrated into an opposition government agency. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

-- Also, the opposing faction's insert, or penetration, into an intelligence apparatus. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

> In 1622, Sir Francis Bacon used the term "mole" in the *History of the Reign of King Henry VII:*
>
> > *He was careful and liberal to obtain good Intelligence from all parts abroad…. As for his secret spials, which he did employ both at home and abroad, by them to discover what practices and conspiracies were against him, surely his care required it; he had such* ***moles*** [emphasis added] *perpetually working and casting to undermine him.* (p. 216)
>
> In modern times, the term was popularized by John le Carré (penname for David Cornwell, a British author of espionage novels) who used the term "mole" to mean a "penetration" of a adversary intelligence service. In le Carré's 1974 novel, *Tinker, Tailor, Soldier, Spy*, Smiley is recalled to hunt down a Soviet "mole" in the Circus (British Secret Intelligence Service, aka MI6).
>
> Also a title of a book by William Hood, *Mole: The True Story of the First Russian Spy to Become an American Counterspy* about Pyotr Semyonovich Popov, a Major in Soviet Military Intelligence (the GRU); see <http://en.wikipedia.org/wiki/Pyotr_Semyonovich_Popov>.
>
> Hood's book, *Mole*, is one of the best publicly available descriptions of a penetration of an intelligence service and provides a detailed and highly personal account of how intelligence tradecraft is practiced, the mental and psychological toll this takes, and the risks involved (for both agent and case officer).

Mole Hunt. The term popularized by John le Carré for a counterintelligence investigation conducted into hostile penetration. (*Historical Dictionary of Cold War Counterintelligence*, 2007) Also see *mole*.

-- Also, the search for moles in one's own service. (Encyclopedia of Cold War Espionage, Spies, and Secret Operations, 3rd edition, 2012)

> Also the title of a book by David Wise, *Molehunt: The Secret Search for Traitors That Shattered the CIA* (1992).

Money Laundering. Generally refers to financial transactions in which criminals, including terrorist organizations, attempt to disguise the proceeds, sources or nature of their illicit activities. (US Department of Treasury)

Moscow Rules. The ultimate tradecraft methods for use in the most hostile of the operational environments. During the Cold War, Moscow was considered the most difficult of operating environments. (Spy Dust)

Once, an accident. Twice, a coincidence. Three times, an enemy action.

-- Ian Fleming, *Goldfinger* (1959)

Auric Goldfinger mentions this rule to James Bond in Goldfinger's warehouse in Geneva.

"Moscow rules" …the precepts we all understand for conducting our operations in the most difficult of operating environments: the Soviet capital. …They were dead simple, and all full of common sense:

-- Never make surveillance mad or embarrassed—they will shut you down.
-- Never look over your shoulder or steal free looks in store windows when on the street.
-- Make them think it was their fault that they had lost you, not vice versa, because KGB officers knew better than to report their own mistakes.

… a mantra that could guide them in determining whether they were the subject of hostile surveillance: Once, an accident. Twice, a coincidence. Three times, an enemy action.

-- Antonio and Jonna Mendez, *Spy Dust: Two Masters of Disguise Reveal the Tools and Operations that Helped Win the Cold War* (2002), p. 36

Motivation. The complex of reasoning and emotional or other drives that induces a person to accept employment or cooperate with an agency for a particular assignment. (AFOSI Instruction 71-101, 6 Jun 2000) Also see *"MICE."*

-- Also, broadly defined, is a feeling or state of mind that influences one's choices and actions. (PERSEREC Technical Report 05-10, May 2005)

-- Also, tradecraft jargon for bases for agent recruitment that are usually (1) ideological; (2) financial; (3) coercion or blackmail; (4) sexual; (5) ego satisfaction; (6) familial; (7) love of adventure or excitement; (8) a combination of two or more of the preceding. (Leo D. Carl, *The CIA Insider's Dictionary*, 1996)

Motivation for espionage results from a complex interaction between personality characteristics and situational factors

-- PERSEREC Technical Report 05-10, May 2005 (p.1)

Psychological portraits of the major spies show complex motivations, which often include dissatisfaction with the job. …The profile of a traitor may not be significantly different from that of many sociopaths or felons. …Spies also usually have two other characteristics: They relish the secret world of intrigue and they enjoy the chance to show others as fools. …The typical spy enjoys deception and may have a personality bordering on, or well into, the psychotic.

-- Thomas B. Allen and Norman Polmar, *Merchants of Treason: America's Secrets for Sale* (1988), pp.51-52

Espionage Motivations

Motives by which spies are driven are highly individualized—simple motives often conceal deeper and more complicated motivations. Motivation for espionage is often elusive and frequently involves multiple reasons. According to a 2008 PERSEREC study, assigning the motivation for committing espionage is often most accurate when motivation is inferred from evidence available while the crime was being committed, rather than from the self justifications after the fact. Like most criminals, once caught, spies see their own past intentions and the pressures that may have affected their behavior in a changed light. Motives for espionage can also change over the course of espionage activities.

MONEY: Historically a leading motivation -- the primacy of money as a motive is a common observation in studies of espionage. Money (financial gain) also appears frequently in combination with other motives. Americans most consistently have cited money as the dominant motive for espionage, especially in the 1980s—*the decade of the spy*. This motivation reflects a person's need for money (e.g., indebtedness, financial pressures), or simple greed, or some combination thereof. Often seen in people who see themselves as underpaid (whether real or perceived). Many

cases involved indebtedness. Being in debt or having a history of insolvency, bankruptcy, or late payments is a major component of the financial considerations scrutinized in a personnel security investigation for a security clearance. Among the typical financial motives of debt or greed, debt continues to motivate espionage more than just greed. Although no recent cases, several past spies were frequent gamblers. Money remains one of multiple motives in many recent cases.

> *"Spies, being human, often invent a better-sounding motive if their sole reason for betraying their country is money."*
> -- General Frantisel Moravec, Former Head of Czech Military Intelligence

IDEOLOGY/DIVIDED LOYALTIES: This motivation encompasses both ideological driven motives (commitment to a competing political or economic system, e.g. Communism or Jihadism) and/or those with competing allegiances (i.e., intellectual or emotional commitments to another country through birth, family ties or cultural affinity). Ideology was the dominant motive in the 1940s, whereas divided loyalties has increased over time of all motives for espionage. Divided loyalties—holding and acting on an allegiance to a foreign country or cause in addition to or in preference to allegiance to the United States—has dramatically increased since 1990. PERSEREC studies indicate that spying prompted by divided loyalties has become the most common motive for American espionage, replacing spying for money as the primary motive. Additionally this trend has been accelerating since 2000.

COMPROMISE/COERCION: Being forced to commit espionage through blackmail or threat to relatives in a foreign country. Used to recruit spies most often in the early period before 1980, when foreign intelligence services engaged in occasional blackmail using relatives overseas, or entrapped Americans in sexual blackmail scams. Has not been seen in recent cases.

EGO/THRILLS: Some spies commit espionage for thrills or to make themselves feel important—ego-boosting. Some have a fascination with spying and find espionage a thrilling enterprise that allows them to enact fantasies of secret lives and heroic deeds they have read about in popular spy novels. Includes the related ego-boost of getting away with it, as well as the thrill of successfully maintaining a secret life parallel to the spy's professional career, and thereby cleverly demonstrating that his competence surpasses his colleagues. Although rarely the primary motive, there have been several cases involving individuals who spied for the thrill of getting away with espionage, or from their need to stroke their egos.

DISGRUNTLEMENT/REVENGE: In recent cases, disgruntlement was the second most common cause. This motive takes many different forms: disenhancement, extreme unhappiness with people and employment, disaffection, bitterness, frustration, anger, disillusionment, and alienation. Usually directly related to employment/work-related issues caused by the person's relationships or treatment in the workplace, and associated desire to take revenge. Disappointment, anger, frustration, or alienation can arise from interactions among coworkers or between employees and supervisors. Feelings of disgruntlement often lead to efforts to get revenge and espionage is one way to get bak at the offending individual, organization, or at the whole government they represent. A common motivation among those who volunteer.

INGRATIATION: The desire to help or please someone else motive some to commit espionage. Most often through an emotional, personal relationship or attachment. This motivation can also manifest when trying to impress a potential future employer. Most spies who committed espionage to please others tended to be successful.

RECOGITION: Usually a secondary motive of spies seeking recognition, approval and/or attention from those to whom they provided information. Individuals often feel overworked and underappreciated and espionage allows them to connect or bond with an agent handler and seek the approval and attention of the handler.

For more information, see following Defense Personnel Security Research Center (PERSEREC) Reports:

-- *Americans Who Spied Against Their Country Since World War II*, Rpt PERS-TR-92-005, May 1992
-- *Espionage Against the United States by American Citizens 1947-2001*, Rpt 02-5, Jul 2002
-- *Changes in Espionage by Americans: 1947-2007*, Tech Rpt 08-05, Mar 2008
-- *Espionage and Other Compromises of National Security: Case Summaries from 1975 to 2008*, 2 Nov 2009

MTAC. See *Multiple Threat Alert Center.*

Multiple Threat Alert Center (MTAC). Department of Navy's fusion, analysis and dissemination center for terrorist, criminal, counterintelligence and security information; operated by the Naval Criminal Investigative Service (NCIS).

> *The terrorist attack on the World Trade Center in New York and the Pentagon in Washington, DC on September 11, 2001 led NCIS to transform the Antiterrorist Alert Center (ATAC) into the MTAC in 2002.*
>
> -- NCIS <http://www.ncis.navy.mil/AboutNCIS/History/Pages/default.aspx>

Multilateral Collection. A collection activity conducted with two or more cooperating foreign intelligence services against a mutually targeted foreign intelligence, security service, or international terrorist entity. (Previously in DoDI S-5240.17, CI Collection, 12 Jan 2009) Also see *bilateral.*

> Multilateral: activities conducted with more than one nation.

Multilateral OFCO. An OFCO [Offensive Counterintelligence Operation] conducted by a U.S. CI agency with two or more cooperating foreign intelligence services against a mutually targeted FISS, foreign entity, or terrorist element. (DoDI S-5240.09, 29 Oct 2008)

Multilevel Security (MLS). Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Multinational. Between two or more forces or agencies of two or more nations or coalition partners. Also see also *alliance; coalition*. (JP 1-02)

Multinational Force (MNF). A force composed of military elements of nations who have formed an alliance or coalition for some specific purpose. (JP 1-02) Also see multinational operations.

Multinational Operations. A collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance. (JP 1-02 and JP 3-16, Multinational Operations, 7 Mar 2007) Also see *alliance; coalition; coalition action.*

Multispectral Imagery (MSI). The image of an object obtained simultaneously in a number of discrete spectral bands.(JP 1-02 and JP 3-14, Space Operations, 6 Jan 2009)

N ==========

Narcoterrorism. Terrorism that is linked to illicit drug trafficking. (JP 1-02 and JP 3-07.4, Joint Counterdrug Operations, 13 Jun 2007)

Name Trace. A search of available recorded data to find information about a person, normally conducted to determine the presence or absence of derogatory information about the person, as a first step in judging his suitability or intelligence value. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, a search of data for information about an individual, organization, or subject. (National HUMINT Glossary)

National Agency Check (NAC). An in-depth name trace consisting of Federal Bureau of Investigation Name and Criminal History Fingerprint Checks, Defense Clearance Investigation Index (DCII) search, and can include checks on military personnel records, citizenship, selective service, Central Intelligence Agency records, State Department records, and other US Government agencies. Also see *local agency check; military agency check.*

-- Also, [part of a] personnel security investigation consisting of a review of: investigative and criminal history files of the Federal Bureau of Investigation, including a technical fingerprint check; Office of Personnel Management Security/Suitability Investigations Index; DoD Central Index of Investigations (DCII) and Joint Personnel Adjudication System (JPAS); and such other national agencies (e.g., CIA, DNI) as appropriate to the individual's background. (IC Standard 700-1, 4 Apr 2008)

-- Also, formal request to federal agencies for searches of their records and supporting databases and files for information of investigative [/CI] interest. (FM 2-22.2, Counterintelligence, Oct 2009 and 902d MI Group Investigations Handbook, Jun 2012)

-- Also, an integral part of all background investigations, the NAC consists of searches of OPM's Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); the FBI Identification Division's name and fingerprint files, and other files or indices when necessary. (Army – see below)

> National Agency Check and Inquiries (NACI) - This is the basic and minimum investigation required on all new Federal employees. It consists of a NAC with written inquiries and searches of records covering specific areas of a person's background during the past five years. Those inquiries are sent to current and past employers, schools attended, references, and local law enforcement authorities.
>
> Access NACI (ANACI) - This is a new investigation designed as the required initial investigation for Federal employees who will need access to classified national security information at the Confidential or Secret level. The ANACI includes NACI and Credit coverage with additional local law enforcement agency checks.
>
> NAC with Local Agency Check and Credit (NACLC) - This is a new investigation which is the same as the ANACI without the written inquiries to past employers, schools attended, etc. It is designed as the initial investigation for contractors at the Confidential and Secret national security access levels. The NACLC also is to be used to meet the reinvestigation requirement for all individuals (including contractors) who have Confidential or Secret clearances.
>
> -- US Army at: <http://www.dami.army.pentagon.mil/site/PerSec/InvTypes.aspx> (accesses 24 Sep 2013)

National Capital Region (NCR). A geographic area encompassing the District of Columbia and eleven local jurisdictions in the State of Maryland and the Commonwealth of Virginia. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

National Center for Credibility Assessment (NCCA). A federally funded institution providing graduate and continuing education courses in psychophysiological detection of deception (PDD). (www.ncca.mil/mission.htm)

-- Also, an interagency training institute that provides polygraph education and training, conducts credibility assessment research and development, and manages the Polygraph Quality Assurance Program. (DoD FCIP Strategy FY 2013-2017)

For DoD policy see DoDD 5210.48, Polygraph and Credibility Assessment Program. NCCA is under the operational control of the Defense Counterintelligence and Human Intelligence Center (DCHC), DIA. It was previous known as the Defense Academy for Credibility Assessment (DACA) and before that as the DoD Polygraph Institute (DoDPI).

National Clandestine Service (NCS). The NCS operates as the clandestine arm of the CIA, and serves as the national authority for the coordination, deconfliction, and evaluation of clandestine human intelligence operations across the Intelligence Community. The NCS supports our country's security and foreign policy interests by conducting clandestine activities to collect information that is not obtainable through other means. The NCS also conducts counterintelligence and special activities as authorized by the President. (CIA at <https://www.cia.gov/offices-of-cia/clandestine-service/index.html>)

-- Also, the NCS serves as the national authority for the integration, coordination, deconfliction, and evaluation of human intelligence operations across the entire Intelligence Community, under authorities delegated to the Director of the CIA who serves as the National HUMINT Manager. The Director of the NCS reports directly to the Director of the CIA and will work with the Office of the Director of National Intelligence to implement all of the DNI's statutory authorities. (ODNI News release 3-05, 13 Oct 2005) Also see *Defense Clandestine Service*.

Formerly known as CIA Directorate of Operations or DO (in 2005, the DO transitioned to the NCS). The NCS was established in response to recommendations made in March 2005 by the President's Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.

Collecting foreign intelligence — finding someone who has protected information and convincing that person to share it — is the "bread and butter" of what the clandestine service does, although "if we succeed, we'd rather not talk about it."

-- Thomas Twetten, Former Chief of CIA Clandestine Operations, 27 Jan 2011

Clandestine Service…

A clandestine service does much more than simply collect "HUMINT" clandestinely, that is secretly exploit agents for the purpose of collecting intelligence. A clandestine service also works in liaison with other spy services to run all types of operations; it taps telephones and installs listening devices; it breaks into or otherwise gains access to the contents of secured facilities, safes, and computers; it steals, compromises, and influences foreign cryptographic capabilities so as to make them exploitable by US SIGINT; it protects its operations and defends the government from other intelligence services by engaging in a variety of counterespionage activities, including the aggressive use of double agents and penetrations of foreign services; and it clandestinely emplaces and services secret SIGINT and MASINT sensors. It also has the capability of using its techniques and access to run programs at the President's direction to influence foreign governments and developments, that is, "covert action." The unifying aspect of these activities is not some connection to HUMINT; rather, they are highly diverse but interdependent activities that are best conducted by a clandestine service.

-- *IC 21: Intelligence Community in the 21st Century,* Chap. IX – Clandestine Service; available on line at: <http://www.gpo.gov/fdsys/pkg/GPO-IC21/html/GPO-IC21-9.html>

National Counterintelligence Executive (NCIX). Performs duties provided in the CI Enhancement Act of 2002 and such other duties as may be prescribed by the Director of National Intelligence or specified by law. NCIX serves as Mission Manager of Counterintelligence and the Chairperson of the National CI Policy Board. Resides within the Office of the Director of National Intelligence (ODNI). (CI Enhancement Act of 2002) Also see *Office of the National Counterintelligence Executive*.

-- Also, the NCIX serves as the head of national counterintelligence for the U.S. Government, per the CI Enhancement Act of 2002. (National Intelligence: A Consumer's Guide - 2009)

Additional information on NCIX at <http://www.ncix.gov/about/index.html>

National Counterintelligence Policy Board (NACIPB). Special board established by statue within the executive branch of Government; reports to the President through the National Security Council. The Board serves as the principal mechanism for developing policies and procedures for the approval of the President to govern the conduct of counterintelligence activities; and upon the direction of the President, resolving conflicts that arise between elements of the Government conducting such activities. The Board also acts as an interagency working group to ensure the discussion and review of matters relating to the implementation of the Counterintelligence Enhancement Act of 2002 and provides advice to the National Counterintelligence Executive on priorities in the implementation of the *National Counterintelligence Strategy*. (Extracted from 50 U.S.C. §402a)

NACIPB is chaired by the National Counterintelligence Executive and consists of senior USG personnel appointed by the head of the department or element concerned, as follows: Department of Justice, including the Federal Bureau of Investigation (FBI); Department of Defense, including the Joint Chiefs of Staff; Central Intelligence Agency (CIA); Department of State; Department of Energy; and any other department, agency, or element of the US Government specified by the President.

National Counterproliferation Center (NCPC). Coordinates strategic planning within the Intelligence Community (IC) to enhance intelligence support to United States efforts to stem the proliferation of weapons of mass destruction and related delivery systems. It works with the IC to identify critical intelligence gaps or shortfalls in collection, analysis or exploitation, and develop solutions to ameliorate or close these gaps. It also works with the IC to identify long-term proliferation threats and requirements and develop strategies to ensure the IC is positioned to address these threats and issues. NCPC will reach out to elements both inside the IC and outside the IC and the U.S. Government to identify new methods or technologies that can enhance the capabilities of the IC to detect and defeat future proliferation threats. (ODNI News release 9-05, 21 Dec 2005)

-- Also, the NCPC, which resides in the ODNI, is the bridge from the IC to the policy community for activities within the U.S. Government associated with countering the proliferation of weapons of mass destruction (WMD). (National Intelligence: A Consumer's Guide - 2009)

National Counterterrorism Center (NCTC). The primary center for US government analysis of terrorism. It falls under the Office of the Director of National Intelligence (ODNI). One of its primary missions is "to serve as the central and shared knowledge bank on known and suspected terrorists and international terrorist groups, as well as their goals, strategies, capabilities, and networks of contacts and support." (EO 13354, National Counterterrorism Center, 27 Aug 2004)

In August 2004, the President established the NCTC to serve as the primary USG organization for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism and to conduct strategic operational planning by integrating all instruments of national power. In December 2004, Congress codified the NCTC in the Intelligence Reform and Terrorism Prevention Act (IRTPA) and placed the NCTC in the Office of the Director of National Intelligence (ODNI). NCTC is a multi-agency organization dedicated to eliminating the terrorist threat to US interests at home and abroad.

-- NCTC website: <http://www.nctc.gov/about_us/about_nctc.html >

NCTC was established in 2004 to ensure that information from any source about potential terrorist acts against the U.S. could be made available to analysts and that appropriate responses could be planned. Investigations of the 9/11 attacks had demonstrated that information possessed by different agencies had not been shared and thus that disparate indications of the looming threat had not been connected and warning had not been provided.

NCTC prepares studies ranging from strategic assessments of potential terrorist threats to daily briefings and situation reports. It is also responsible, directly to the President, for planning (but not directing) counterterrorism efforts. The NCTC received a statutory charter in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458); it currently operates with a staff of more than 500 personnel from its headquarters in northern Virginia.

-- Congressional Research Service (CRS) Report R41022, 19 Dec 2011

National Crime Information Center (NCIC). A computerized system of crime records and data, maintained by the Federal Bureau of Investigation, that can be tapped into by virtually every criminal justice agency nationwide. (Cyber Threats to National Security, Symposium Five, 2011)

See <http://www.fbi.gov/about-us/cjis/ncic/ncic >

National Critical Infrastructure and Key Assets (NCI & KA). *Within DoD: None – term removed from JP 1-02.*

Previously defined in JP 3-28, Civil Support (14 Sep 2007) as: The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. They include telecommunications, electrical power systems, gas and oil distribution and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations.

National Critical Systems and Technology Joint Task Force (NCST-JTF). A collaborative forum to lead USIC and federal agency counterintelligence efforts for the protection of critical technologies. (NCST-JTF tri-fold, undated, circa 2012)

NCST-JTF Mission

Leverage the collective CI resources of the Task Force member agencies to prevent, preempt, deter, and investigate attempts to acquire, proliferate and transfer critical US technologies to foreign powers.

Apprehend and prosecute individuals who may commit or plan such acts negatively affecting U.S. National Security interest.

National Cyber Investigate Joint Task Force (NCIJTF). The focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigations. The FBI is responsible for developing and supporting the joint task force, which includes 19 intelligence agencies and law enforcement, working side by side to identify key players and schemes. Its goal is to predict and prevent what's on the horizon and to pursue the enterprises behind cyber attacks. (www.fbi.gov; accessed 18 Jun 2013)

On 8 January 2008, the President signed Presidential Directive NSPD-54/HSPD-23 which mandated the National Cyber Investigative Joint Task Force to be the focal point for all government agencies and to coordinate, integrate, and share information related to all domestic cyber threat investigations.

NCIJTF Mission: Ensure the U.S. Government is coordinating all its efforts to address national security cyber intrusions, including intelligence operations and investigations. The NCITF's functions are structured in three groups: the Information Operations Group, the Analysis Group, and the Law Enforcement Group.

For more information on the NCIJTF see <http://www.fbi.gov/about-us/investigate/cyber/ncijtf>

National Cyber Investigative Joint Task Force - Analytical Group (NCIJTF-AG)

The Defense Cyber Crime Center (DC3) resources and manages the Analytic Group of the NCIJTF, which operates under overall FBI stewardship, joined by other national LE/CI organizations. Focused on nation-state threat actors, AG leads a collaborative analytical and technical exchange with subject matter experts from LE/CI, CND, IC, and IA agencies to build a threat picture to enable proactive LE/CI cyber operations.

National Defense Strategy (NDS). A document approved by the Secretary of Defense for applying the Armed Forces of the United States in coordination with Department of Defense agencies and other instruments of national power to achieve national security strategy objectives. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

National Detainee Reporting Center (NDRC). National-level center that obtains and stores information concerning enemy prisoners of war, civilian internees, and retained personnel and their confiscated personal property. May be established upon the outbreak of an armed conflict or when persons are captured or detained by U.S. military forces in the course of the full range of military operations. Accounts for all persons who pass through the care, custody, and control of the U.S. Department of Defense. (JP 1-02 and JP 3-63, Detainee Operations, 30 May 2008)

National Disclosure Policy (NDP-1). A document that promulgates national policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance required by U.S. departments and agencies having occasion to disclose classified information to foreign governments and international organizations. NDP-1 establishes and provides for management of interagency mechanisms and procedures required for effective implementation of the national policy.

National Disclosure Policy Committee. Central authority for formulation, promulgation, administration, and monitoring of the NDP-1.

National Emergency. A condition declared by the President or the Congress by virtue of powers previously vested in them that authorize certain emergency actions to be undertaken in the national interest. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

National Essential Functions. That subset of Government functions that are necessary to lead and sustain the Nation during a catastrophic emergency. (PDD-21, 12 Feb 2013)

National Foreign Intelligence Program. All programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of Central Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by US Armed Forces. (50 USC §401a)

National Geospatial-Intelligence Agency (NGA). A member of the US Intelligence Community, as well as a Combat Support Agency of the Department of Defense, that provides timely, relevant and accurate geospatial intelligence in support of national security objectives.

The term “geospatial intelligence” or “GEOINT” means the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence and geospatial (e.g., mapping, charting and geodesy) information.

-- See NGA website at <https://www1.nga.mil/>

The National Imagery and Mapping Agency (NIMA) transitioned to the National Geospatial-Intelligence Agency (NGA) in 2003. NIMA established its internal CI element on 1 April 2002. See the official history of the NGA and predecessors, *Advent of the National Geospatial-Intelligence Agency*, September 2011, by the Office of the NGA Historian, available at <www.nga1.mil>

National HUMINT Collection Directive (NHCD). A set of national-level strategic collection requirements for a particular country, geographic area, or transnational issue, prepared by the NHRTC in coordination with IC and other organizations. (DHE-M 3301.001, Vol I: Collection Requirement, Reporting, and Evaluation Procedures, 30 Jan 2009, w/ chg 2 dated 1 Feb 2012)

-- Also, an integrated inter-agency mechanism for tasking human intelligence requirements to members of the Intelligence Community that have the best capability and probability of acquiring that information at the least cost and least risk. A standing / enduring intelligence requirement. (National HUMINT Glossary)

National HUMINT Requirements Tasking Center (NHRTC). Congressionally mandated to integrate all HUMINT collection and reporting capabilities within the US Government. [Staffed by] senior officers from the Department of State, Department of Defense, and CIA; the center produces National HUMINT Collection Directives (NHCDs) and Collection Support Briefs (CSBs). (National HUMINT Glossary)

> The NHRTC reports to the National HUMINT Manager. See DCID 3/7, *National HUMINT Requirements Center (U)*, 1 Jun 1992 (classified CONFIDENTIAL).

National Industrial Security Program (NISP). National program established by EO 12829 for the protection of information classified under EO 12958 as amended, or its successor or predecessor orders, and the Atomic Energy Act of 1954, as amended. The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense is the Executive Agent for the NISP. The Information Security Oversight Office (ISOO) is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies. (DoD 5220.22-M, NISPOM, 28 Feb 2006) Also see the *Defense Security Service (DSS); industrial security.*

> The Defense Security Service (DSS) is designated as the DoD Cognizant Security Office (CSO) for cleared contractors within the NISP.
>
> For additional information see Information Security Oversight Office (ISSO) website at: <http://www.archives.gov/isoo/policy-documents/>

National Infrastructure Coordinating Center. The national physical critical infrastructure center, as designated by the Secretary of Homeland Security, which coordinates a national network dedicated to the security and resilience of critical infrastructure of the United States by providing 24/7 situational awareness through information sharing, and fostering a unity of effort. (www.dhs.gov)

National Infrastructure Protection Center (NIPC). The FBI's NIPC is charged with detecting, preventing and responding to cyber and physical attacks on US critical infrastructure and overseeing computer crime investigation conducted by FBI field offices.

National Infrastructure Protection Plan (NIPP). A plan developed by the Department of Homeland Security [DHS] to provide the unifying structure for the integration of a wide range of efforts for the enhanced protection and resiliency of the nation's critical infrastructure and key resources into a single national program. (Cyber Threats to National Security, Symposium Five, 2011)

> See <http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf>
>
> Copy of the NIPP 2013 also available at: <https://www.hsdl.org/?view&did=747827>

National Infrastructure Sector. One of the 18 national CI/KR [critical infrastructure and/or key resource] sectors identified in Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," 17 December 2003. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

National Insider Threat Task Force (NITTF). National Task Force focused on Insider Threat issues under joint leadership of the Attorney General and the Director of National Intelligence; established IAW EO 13587, October 2011 The NCIX and FBI co-direct the daily activities of the NITTF.

> *The NITTF assists federal agencies develop insider threat programs to help prevent, deter, and detect compromises of classified information by malicious insiders. Its goals is to prevent classified information from getting into the hands of people who can harm the national security of our country.*
> -- NITTF Fact Sheet, subj: NITTF External Communications Guidance, undated

National Insider Threat Working Group (NISTWG). Interagency, cross-discipline working group established by the National Counterintelligence Policy Board to focus exclusively on insider threat issues.

National Intelligence. All intelligence, regardless of the source from which derived and including information gathered within or outside of the United States, which pertains, as determined consistent with any guidelines issued by the President, to the interests of more than one department or agency of the Government; and that involves (a) threats to the United States, its people, property, or interests; (b) the development, proliferation, or use of weapons of mass destruction; or (c) any other matter bearing on United States national or homeland security. (Intelligence Reform and Terrorism Prevention Act of 2004, §1012; also JP 1-02 and JP 2-01, Joint & National Intelligence Support to Military Operations, 5 Jan 2012)

-- Also, intelligence which pertains to the interest of more than one department or agency of the US Government. (50 USC §401a)

> The US Government uses intelligence to improve and understand the consequences of its national security decisions.

National Intelligence Board. Serves as the senior Intelligence Community advisory body to the Director of National Intelligence (DNI) on the analytic judgments and issues related to analysis of national intelligence; functions include: production, review, and coordination of national intelligence; interagency exchanges of national intelligence information; sharing of IC intelligence products with foreign governments; protection of intelligence sources and methods; activities of common concern and other matters as may be referred to it by the DNI. (ICD 202, National Intelligence Board, 16 Jul 2007)

National Intelligence Council (NIC). The Intelligence Community's center for mid-term and long-term strategic thinking. Its primary functions are to: 1) Support the DNI in his role as head of the Intelligence Community; 2) Provide a focal point for policymakers to task the Intelligence Community to answer their questions; 3) Reach out to nongovernmental experts in academia and the private sector to broaden the Intelligence Community's perspective; 4) Contribute to the Intelligence Community's effort to allocate its resources in response to policymakers' changing needs; and 5) Lead the Intelligence Community's effort to produce National Intelligence Estimates (NIEs) and other NIC products. (ODNI website)

> The NIC is responsible for the US Intelligence Community's most authoritative assessments of major issues affecting the national security. By law [50 USC §403-3b(b)(1)], the NIC is to consist of "senior analysts within the intelligence community and substantive experts from the public and private sector, who shall be appointed by, report to, and serve at the pleasure" of the DNI. The senior analysts are known as National Intelligence Officers (NIOs).
>
> NIC responsibilities are set forth in ICD 207, *National Intelligence Council*, 9 June 2008.

National Intelligence Coordination Center (NIC-C). Provides a mechanism to strategically manage and direct collection across defense, foreign and domestic realms. [Interfaces with the Defense Intelligence Coordination Center (DIOCC]. (National Intelligence: A Consumer's Guide - 2009)

National Intelligence Estimate (NIE). The DNI's most authoritative written judgment concerning national security issues. NIEs contain the coordinated judgments of the Intelligence Community regarding the likely course of future events. (ODNI website)

-- Also, a strategic estimate of the capabilities, vulnerabilities, and probable courses of action of foreign nations produced at the national level as a composite of the views of the intelligence community. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

National Intelligence Priorities Framework (NIPF). The Director of National Intelligence's guidance to the IC on the national intelligence priorities approved by the President. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, the DNI's sole mechanism for establishing national intelligence priorities. The NIPF consists of: intelligence topics approved by the President; a process for assigning priorities to countries and non-state actors relevant to the approved intelligence topics; and a matrix showing those priorities. It is updated semi-annually. The NIPF is used by the ODNI and IC elements in allocating collection and analytical resources. (ICD 204, 13 Sep 2007)

> *A key instrument for keeping the IC attentive to both policymaker concerns and potential shocks… The NIPF process gathers the needs of senior decision makers across the US government on a semi-annual basis to support prudent allocation of both collection and analytical resources for the following 6-to-12 months.*
>
> – DNI 2006 Annual Report of the US Intelligence Community (Feb 2007)

National Intelligence Program (NIP). All programs, projects, and activities of the IC, as well as any other programs of the IC designated jointly by the DNI and the head of a US department or agency or by the President. It does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by US Armed Forces. (National Security Act §3(6) and ICD 1, 1 May 2006)

> Formerly known as the National Foreign Intelligence Program (NFIP), the NIP provides the resources needed to develop and maintain intelligence capabilities that support national priorities. The DoD Foreign Counterintelligence Program or FCIP is part of the NIP.
>
> ———————————
>
> The Federal Budget (FY 2012) disclosed for the first time the aggregate funding for NIP – $55 billion in 2012. However, detailed funding requests for intelligence activities remain classified. See White House Factsheet at: <http://www.whitehouse.gov/omb/factsheet_department_intelligence>

National Intelligence Strategy. A strategy document prepared by the ODNI in consultation with the relevant departments that establishes the strategic objectives for the Intelligence Community (IC); it sets forth the framework for a more unified, coordinated and effective IC [and] guides IC policy, planning, collection, analysis, operations, programming, acquisition, budgeting, and execution. (ODNI News release 4-05)

> The National Intelligence Strategy (NIS) sets forth the framework for a more unified, coordinated, and effective US Intelligence Community (IC) and guides IC policy, planning, collection, analysis, operations, programming, acquisition, budgeting, and execution. The strategy outlines strategic objectives that are referred to as either mission or enterprise objectives. The unclassified *National Intelligence Strategy* (Aug 2009) is available at <http://www.dni.gov/reports/2009_NIS.pdf>
>
> CI is one of six mission objectives of the NIS (Mission Objective 4 is *Integrate Counterintelligence*). This is the first time that CI was identified as a mission objective within the NIS; see NIS pp 8-9.

National Intelligence Support Plan (NISP). The NISP, in conjunction with the Combatant Command's Annex B: [Intelligence Plan or IPLAN] supports COCOM operational plans directed by the President and the Secretary of Defense. The NISP defines the national Intelligence Community (IC) agencies' and related organizations' intelligence collection, and analysis & production support roles and responsibilities within the COCOM area of responsibility and the national IC to ensure integrated intelligence operations, synchronized with the COCOM operational plan. The NISP supports the COCOM's operational objectives during all phases of the operation and contributes to the achievement of the COCOM's desired operational effects. (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007) Also see *Counterintelligence Functional Support Plan (CI FSP).*

National Joint Terrorism Task Force (NJTTF). The NJTTF was established in July 2002 to serve as a coordinating mechanism with the FBI's partners on terrorism issues. Over 40 agencies are represented in the NJTTF, which has become a focal point for information sharing and the management of large-scale projects that involve multiple partners. Also see *Joint Terrorism Task Force (JTTF)*. (DoJ website: <http://www.usdoj.gov/jttf/>)

-- Also, the NJTTF was created to act as a liaison and conduit for information on threats and leads from FBI Headquarters to the local JTTFs and to 40 participating agencies including representatives from members of the Intelligence Community; components of the departments of Homeland Security, Defense, Justice, Treasury, Transportation, Commerce, Energy, State, and Interior; NYPD; Nuclear Regulatory Commission; Railroad Police; U.S. Capitol Police; and others. (FBI)

See FBI web site at: <http://www.fbi.gov/news/stories/2008/august/njttf_081908>

National Media Exploitation Center (NMEC). A Director of National Intelligence (DNI) Center composed of DIA, CIA, FBI, NSA, and Defense Cyber Crime Center (DCCC) as partner organizations; DIA is the Executive Agent. NMEC acts as a DOMEX [document and media exploitation] service of common concern and ensures prompt and responsive DOMEX support to meet the needs of intelligence, defense, homeland security, law enforcement, and other US Government Consumer's, to include provision of timely and accurate collection, processing, exploitation, and dissemination consistent with the protection of intelligence sources and methods. (ICD 302, Document and Media Exploitation, 6 Jul 2007)

Director DIA is the IC Executive Agent for the NMEC (para 2d, DoDD 3300.03).

National Military Strategy (NMS). A document approved by the Chairman of the Joint Chiefs of Staff for distributing and applying military power to attain national security strategy and national defense strategy objectives. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013) Also see *national security strategy*.

The NMS defines the national military objectives, establishes the strategy to accomplish these objectives, and addresses the military capabilities required to execute the strategy. The Chairman develops the NMS by deriving overall security policy guidance from the President's NSS, and through consulting with the other JCS members and combatant commanders. The NMS describes the strategic landscape and includes a discussion of the potential threats and risks.

-- CJCSI 3100.01A, *Joint Strategic Planning System*, 1 Sep 1999

National Policy. A broad course of action or statements of guidance adopted by the government at the national level in pursuit of national objectives. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

National Reconnaissance Office (NRO). Responsible for integrating unique and innovative space-based reconnaissance technologies, and the engineering development, acquisition, and operation of space reconnaissance systems and related intelligence activities. (JP 2-0, Joint Intelligence, 22 Oct 2013)

The NRO is responsible for research and development (R&D), acquisition, launch, deployment, and operation of overhead reconnaissance systems, and related data-processing facilities to collect

intelligence and information to support national and DoD missions and other United States Government (USG) needs (DoD Directive 5105.23, NRO, 28 June 2011).

The NRO designs, builds and operates the nation's reconnaissance satellites. According to the NRO, their satellites provide constant global access to critical information otherwise unavailable to the President, his cabinet, other national leaders and numerous customers in the Defense and Intelligence communities. These satellites provide services in three broad categories: GEOINT, SIGINT, and Communications.

In recent years, the NRO has implemented a series of actions declassifying some of its operations. The existence of the organization was declassified in September 1992.

On 6 Sep 1961, the NRO was established as a joint CIA-Air Force operation. Throughout the 1960s, U.S. operation of reconnaissance satellites was officially classified. It was not until Jan 1971 that the NRO's existence was first disclosed by the media, when it was briefly mentioned in a New York Times article. A more extensive discussion of the NRO appeared in the Washington Post (9 Dec 1973) as a result of the inadvertent disclosure in a Congressional report.

In September 1992 DoD acknowledged the existence of the NRO, an agency established in 1961 to manage the development and operation of the nation's reconnaissance satellite systems.

See NRO website at <www.nro.gov/ > For additional information see Jeffrey T. Richelson, "Undercover in Outer Space: The Creation and Evolution of the NRO," *International Journal of Intelligence and Counterintelligence*, 13, 3 (Fall 2000): pp. 301-344.

National Security. A collective term encompassing both national defense and foreign relations of the United States with the purpose of gaining: a) a military or defense advantage over any foreign nation or group of nations; b) a favorable foreign relations position; or c) a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

-- Also, the national defense or foreign relations of the United States. (EO 13526, Classified National Security Information, 29 Dec 2009)

National Security Act. The National Security Act of 1947 realigned and reorganized the United States' armed forces, foreign policy, and Intelligence Community apparatus in the aftermath of World War II. The Act merged the Department of War and the Department of the Navy into the National Military Establishment (NME) headed by the Secretary of Defense. It was also responsible for the creation of a separate Department of the Air Force from the existing United States Army Air Forces. Initially, each of the three service secretaries maintained quasi-cabinet status, but the act was amended in 1949 to assure their subordination to the Secretary of Defense. At the same time, the NME was renamed as the Department of Defense. Aside from the military reorganization, the act established the National Security Council, a central place of coordination for national security policy in the Executive Branch, and the Central Intelligence Agency, the United States' first peacetime intelligence agency. (Public Law No. 235, 80 Cong., 61 Stat. 496)

The cornerstone of the current national security system is the National Security Act of 1947 as amended, designed to meet the challenges of the post-WWII, Cold War world. That legislation laid the foundations of a new national security regime, including the creation of the National Security Council, the Central Intelligence Agency, the Department of Defense, a separate Department of the Air Force, and a permanent Joint Chiefs of Staff. See National Security Act of 1947, P.L. 80-235.

The National Security Act has been amended numerous times since its enactment. Reference to the *"National Security Act of 1947, as amended"* indicates the legal authority cited is legislation passed after 1947 that replaced one or more provisions of the original act.
-- See <http://www.intelligence.gov/0-natsecact_1947.shtml>

National Security Agency (NSA). The U.S.'s cryptologic organization, with responsibility for protecting U.S. National Security information systems and collecting and disseminating foreign signals intelligence. Areas of expertise include cryptanalysis, mathematics, computer science, and foreign language analysis. (National Intelligence: A Consumer's Guide - 2009)

-- Also, a member of the US Intelligence Community, as well as a Combat Support Agency of the Department of Defense. NSA/Central Security Service leads the community in delivering responsive, reliable, effective, and expert Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Network Warfare operations to gain a decisive information advantage for the Nation and our allies under all circumstances. (www.nsa.gov)

NSA is the U.S. Government lead for cryptology, and its mission encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) activities. The Central Security Service (CSS) conducts SIGINT collection, processing, analysis, production, and dissemination, and other cryptologic operations as assigned by the Director, NSA/Chief, CSS. NSA/CSS provides SIGINT and IA guidance and assistance to the DoD Components, as well as national customers.

-- DoDD 5100.20, *NSA/CSS*, 26 Jan 2010

The Central Security Service (CSS) oversees the function of the military cryptologic system, develops policy and guidance on contributions of military cryptology to the Signals Intelligence / Information Security (SIGINT/INFOSEC) enterprise, and manages the partnership of NSA and the Service Cryptologic Components. NSA as a whole is known as "NSA/CSS."

-- National Intelligence: A Consumer's Guide – 2009. p. 43

The U.S. SIGINT effort… employs space and airborne collection ground stations, covert listening posts, surface ships, and submarines.

-- Jeffrey T. Richelson, *The US Intelligence Community* (2012, Sixth Edition)

I think it's fair to say that the demands on the Agency approach infinity.
Everybody wants to know everything about everything.

-- Louis Tordella, a longtime deputy director of NSA (1995)

See *60 Years of Defending Our Nation*, National Security Agency, 2012; available at : <http://www.nsa.gov/about/cryptologic_heritage/60th/book/NSA_60th_Anniversary.pdf>

Also see –

Matthew M. Aid, *The Secret Sentry: The Untold History of the National Security Agency.* New York: Bloomsbury, 2009.

James Bamford, The *Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York: Anchor Book, 2008.

National Security Branch (NSB). Major element of the FBI that executes the FBI's national security mission to lead and coordinate intelligence efforts that drive actions to protect the United States. The NSB is composed of the Counterterrorism Division (CTD), Counterintelligence Division (CD), Directorate of Intelligence (DI), Weapons of Mass Destruction Directorate (WMDD), Terrorist Screening Center (TSC), and High-Value Detainee Interrogation Group (HIG). (www.fbi.gov; accessed 31 Jul 2013)

The FBI's national security and intelligence missions are unified under the authority of the Executive Assistant Director (EAD) who reports to the Deputy Director FBI. The EAD-NSB has full operational and management authority over all FBI Headquarters and field national security programs, including the authority to initiate, terminate, or reallocate any of the investigations or other activities within the NSB.

The EAD-NSB is also responsible for the continued development of a specialized national security workforce and is the lead FBI official responsible for coordination and liaison with the Director of National Intelligence (DNI) and the Intelligence Community (IC).

-- See <http://www.fbi.gov/about-us/nsb/national-security-branch-brochure>

National Security Council (NSC). A governmental body specifically designed to assist the President in integrating all spheres of national security policy. (JP 1, Doctrine for the Armed Forces of the United States. 25 Mar 2013)

> The NSC was established by the National Security Act of 1947 as the principal forum to consider national security issues that require presidential decision. Congress envisioned that the NSC would allow military and civilian government departments and agencies to work more effectively together on national security matters.
>
> _____
>
> *The National Security Council (NSC) is the President's principal forum for considering national security and foreign policy matters with the senior national security advisors and cabinet officials. For DOD, the President's decisions drive strategic guidance promulgated by the Office of the Secretary of Defense (OSD) and refined by the Joint Strategic Planning System (JSPS). To carry out Title 10, United States Code (USC), statutory responsibilities, the Chairman of the Joint Chiefs of Staff (CJCS) utilizes the JSPS to provide a formal structure in aligning ends, ways, and means, and to identify and mitigate risk for the military in shaping the best assessments, advice, and direction of the Armed Forces for the President and SecDef.*
>
> -- JP 5-0, *Joint Operation Planning* (11 Aug 2011)

National Security Council Intelligence Directive (NSCID). A formal statement of policy by the National Security Council, binding upon those US Government agencies within the purview of NSC authority. (National HUMINT Glossary)

> Regarding counterintelligence, see NSCID 5, *US Espionage and Counterintelligence Activities Abroad,* 17 Feb 1972.

National Security Crimes. Crimes likely to impact upon the national security, defense, or foreign relations of the United States, including but not limited to espionage, spying, sabotage, treason, and sedition.

National Security Division (NSD). Element of the Department of Justice (DoJ) created by the reauthorization of the USA PATRIOT Act in March 2006, the Division merges the primary national security elements of DoJ, fulfilling a key recommendation of the March 2005 report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission). The Division consists of the Counterterrorism and Counterespionage Sections; the Office of Intelligence Policy and Review; and a Law & Policy Office. (DoJ website at <http://www.usdoj.gov/nsd/>)

> The Counterespionage Section (CES), NSD, DoJ, supervises the investigation and prosecution of cases affecting national security, foreign relations, and the export of military and strategic commodities and technology.
>
> CES has executive responsibility for authorizing the prosecution of cases under criminal statutes relating to espionage, sabotage, neutrality, and atomic energy. It provides legal advice to U.S. Attorney's Offices and investigative agencies on all matters within its area of responsibility, which includes 88 federal statutes affecting national security. It also coordinates criminal cases involving the application of the Classified Information Procedures Act (CIPA). In addition, the Section administers and enforces the Foreign Agents Registration Act of 1938 (FARA) and related disclosure statutes.
>
> The Office of Intelligence Policy and Review (OIPR), NSD, DoJ, prepares and files all applications for electronic surveillance and physical search under the Foreign Intelligence Surveillance Act of 1978 (FISA). The Office also advises the National Security Division and various client agencies, including the CIA, FBI, and the Defense and State Departments, on questions of law, regulation, and guidelines, as well as on the legality of domestic and overseas intelligence operations.

National Security Emergency. Any occurrence, including natural disaster, military attack, technological, or other emergency, that seriously degrades or threatens the national security of the United States. (DoDD 5111.13, ASD(HD&ASA), 16 Jan 2009)

National Security Information (NSI). Any information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and that is so designated. (IC Standard 700-1, 4 Apr 2008)

Note: EO 12958 superseded by EO 13526, *Classified National Security Information*, 29 Dec 2009. For additional information see Information Security Oversight Office (ISSO) website at: <http://www.archives.gov/isoo/policy-documents/ >

National Security Interests. The foundation for the development of valid national objectives that define United States goals or purposes. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

National Security Letter (NSL). An administrative demand for documents or records that are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

-- Also, a NSL seeks customer and consumer transaction information in national security investigations from communications providers, financial institutions, and credit agencies. Five statutory provisions vest government agencies responsible for foreign intelligence investigations with authority to issue written commands comparable to administrative subpoenas. (CRS Report RS22406, 27 Sep 2010)

National security letters, which are analogous to administrative subpoenas and are authorized by five federal statutes. They are only available for authorized national security investigations (international terrorism or foreign intelligence/CI investigations), not general criminal investigations or domestic terrorism investigations. NSLs are issued directly by federal agency officials.

NSLs can only be used to seek certain transactional information permitted under the five NSL provisions, and cannot be used to acquire the content of any communications. The scope of documents which may be obtained pursuant to a national security letter is more limited than that which might be authorized in a FISA order. Statutory provisions at 18 USC §2709, 12 USC §3414, 15 USC §1681u, 15 USC §1681v and 50 USC §436; as amended by PL 109-177 and PL 109-178.

_____

"FBI currently issues an average of nearly 60 NSLs per day."

-- CRS Report RL 33320 (3 Jan 2014), p. 22, footnote 139

_____

For additional information see <http://www.fbi.gov/pressrel/pressrel07/nsl_faqs030907.htm>

Also see CRS Report RS22406 at <http://www.fas.org/sgp/crs/intel/RS22406.pdf> and CRS Report RL33320 at <https://www.fas.org/sgp/crs/intel/RL33320.pdf>

National Security Strategy (NSS). A document approved by the President of the United States for developing, applying, and coordinating the instruments of national power to achieve objectives that contribute to national security. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

National Special Security Event (NSSE). A designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity. (JP 1-02 and JP 3-28, Defense Support of Civil Authorities, 31 Jul 2013)

-- Also, major event considered to be nationally significant as designated by the President or his designated representative, the Secretary of the Department of Homeland Security. Some events categorized as NSSE include presidential inaugurations, major international summits held in the United States, major sporting events, and presidential nominating. NSSE designation factors include: anticipated attendance by U.S. officials and foreign dignitaries; size of the event; and significance of the event. (CRS Report RS22752, updated 19 Mar 2008)

The US Secret Service is the lead federal agency responsible for coordinating, planning, exercising, and implementing security for NSSEs. Designated the lead agency in PL 106-544.

National Threat Identification and Prioritization Assessment (NTIPA). A strategic threat assessment produced by the Office of the National Counterintelligence Executive (ONCIX) that defines and prioritizes threats to the US posed by traditional and emerging foreign intelligence activities. It is designed to assist senior policymakers and officials with CI responsibilities focus on the current and emerging foreign intelligence threats that could cause unacceptable damage to US national security. The NTIPA fulfills the reporting requirement outlined in the Counterintelligence Enhancement Act of 2002. (ONCIX)

"The NTIPA informs the President if the United States of the gravest threats to our nation."

-- National Counterintelligence Strategy of the United States of America – 2012

"*The NTIPA is a compendium of foreign intelligence threat data, mandated by statute to be produced annually by the Office of the National Counterintelligence Executive and submitted to the President for approval.... Community work on the NTIPA (the first of which submitted in 2004 and approved in 2005) revealed broad challenges in collection and analysis on these difficult targets. Prioritizing foreign intelligence threats is an even more demanding analytical task, depending as it does on the consumer's interests (for example, foreign threats to [CIA] DO operations in country X or to deployed forces in country Y may be far different from the rank ordering of country threats to U.S. national security information at home) and the national security context in which they arise (that is, threat priorities do not directly correlate to foreign intelligence capability alone but must be measured against the potential for harm or disruption to U.S. national security concerns and objectives, as prioritized by policy leadership)."*

-- Michelle K. Van Cleave (former NCIX), Counterintelligence and National Strategy, School for National Security Executive Education, National Defense University, April 2007, footnote 36, pp. 33-34

The NTIPA does not go into effect until approved by the President. The NCIX submits each approved NTIPA or modification thereof to the congressional intelligence committees.

NTIPA *versus* NIPF – CI action is driven by the approved NTIPA and foreign intelligence (FI) collection is driven by the NIPF (National Intelligence Priorities Framework). Each has different focus and priorities, as well as a totally different operational dynamic.

Need for CI action is much different from the need for FI collection.

National Virtual Translation Center (NVTC). Provides timely and accurate translations of foreign intelligence for all elements of the IC. Its mission includes acting as a clearinghouse for facilitating interagency use of translators; partnering with elements of the U.S. Government, academia, and private industry to identify translator resources and engage their services; building a nationwide team of highly qualified, motivated linguists and translators, connected virtually to the program office in Washington, D.C.; and applying state-of-the-art technology to maximize translator efficiency. (National Intelligence: A Consumer's Guide - 2009)

The NVTC is a DNI Center and the FBI is the IC Executive Agent.

Naval Criminal Investigative Service (NCIS). The federal law enforcement agency charged with conducting investigations of felony-level offenses affecting the Navy and Marine Corps – that is, crimes punishable by confinement for more than one year. NCIS also performs investigations and operations aimed at identifying and neutralizing foreign intelligence, international terrorist, and cyber threats to the Department of the Navy. In addition, it provides warning of threats and specialized defensive force protection support to U.S. naval forces around the world. Criminal investigation is at the foundation of virtually all the organization does, but the NCIS mission is broad. Transnational terrorism has been and remains a key focus area for the agency. Today, NCIS' mantra is: *Prevent Terrorism, Protect Secrets, and Reduce Crime*. (www.ncis.navy.mil; accessed 28 Jun 2012)

Mission: NCIS is a federal law enforcement agency that protects and defends the DON [Department of Navy] against terrorism and foreign intelligence threats, investigates major criminal offenses, enforces the criminal laws of the United States and the UCMJ, assists commands in maintaining good order and discipline, and provides law enforcement and security services to the Navy and Marine Corps on a worldwide basis.

Director NCIS reports directly to the Secretary of the Navy and is the senior official for criminal investigations, counterintelligence, and security with the DON. Additionally, the Director NCIS is the senior official within DON for terrorism investigations and related operations designed to identify, detect, neutralize, or prevent terrorist planning and activities, and provides antiterrorism expertise and services to DON components.

-- SECNAV Instruction 5430.107, Mission and Functions of the NCIS, 28 Dec 2005

Also see SECNAV Instruction 3850.2C, *Department of the Navy Counterintelligence*, 20 Jul 2005

"Criminal investigation is at the foundation of virtually all the organization does…"
-- <http://www.ncis.navy.mil/AboutNCIS/Pages/default.aspx> (accessed 28 June 2012)

NCIS. Acronym, see *Naval Criminal Investigative Service*.

Near Real Time. Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JP 1-02 and TRADOC Pam 525-2-1, US Army Functional Concept for Intelligence, 13 Oct 2010) Also see *real time*.

Need-to-know. A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, a determination that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012)

-- Also, a determination within the executive branch in accordance with directives issued pursuant to this order [EO 13526] that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (EO13526, Classified National Security Information, 29 Dec 2009)

"The need-to-know principle is fundamental to the intelligence business."
-- Duane R. Clarridge, *A Spy For All Seasons: My Life in the CIA* (1997), p. 310

The "need-to-know" principle, simply put, is that a person in authorized possession of classified information must determine that another person requires access to that information in order to perform a specific and authorized function and that such person has appropriate clearances and access approvals.

…A major tightening up of the "need-to-know" practice is in order. It is particularly disturbing to see the proliferation of detailed knowledge about intelligence sources and methods.

-- HPSCI Report (#100-5), "United States Counterintelligence and Security Concerns – 1986," 100th Congress 1st session, 4 Feb 1987, p. 9

Net-Centric. The ability to provide a framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Network. [In critical infrastructure protection usage] a group or system of interconnected or cooperating entities, normally characterized as being nodes (assets), and the connections that link them. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Network Operations (NetOps). Activities conducted to operate and defend the Global Information Grid. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010)

Neutralize. 1) As pertains to military operations, to render ineffective or unusable. 2) To render enemy personnel or material incapable of interfering with a particular operation. 3) To render safe mines, bombs, missiles, and booby traps. 4) To make harmless anything contaminated with a chemical agent. (JP 1-02)

Neutrality. In international law, the attitude of impartiality during periods of war adopted by third states toward a belligerent and subsequently recognized by the belligerent, which creates rights and duties between the impartial states and the belligerent. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Neutral State. In international law, a state that pursues a policy of neutrality during war. (JP 1-02)

Nickname. A combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes. (JP 1-02) Also see *codeword*.

Non Attributable Internet Access. Use of a commercial internet service provider to access publicly available information on the internet while protecting the unit's U.S. government affiliation, disclosing essential elements of friendly information, or exposing U.S. government information systems to intrusion or manipulation. (AR 381-20, Army CI Program, 25 May 2010)

Noncustodial Interview. Interview conducted when subjects are interviewed without depriving them of their freedom in any significant manner (e.g., arrest or detention). Subjects voluntarily consent to the interview and are advised that they may depart at any time. (Army FM 2-22.2, CI, Oct 2009)

Non-Disclosure Agreement (NDA). An official authorized contract between an individual and the United States (U.S.) Government signed by an individual as a condition of access to classified national intelligence. The NDA specifies the security requirements for access and details the penalties for non-compliance. (DSS Glossary)

Nongovernmental Organization (NGO). A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. (JP 1-02 and JP 3-08, Interorganizational Coordination During Joint Operations, 24 Jun 2011)

-- Also, a legally-constituted organization created by persons having the legal authority to do so with no participation or representation of any government. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Non-Official Cover (NOC). Term used by case officers who operate overseas outside the usual diplomatic cover. (Spy Book)

-- Also, NOC, pronounced as "knock," an acronym for "nonofficial cover." Primarily a CIA term used where one is operating without cover of diplomatic protection or US government employment. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

> *Case officers that have no visible affiliation with the U.S. government. NOCs, as they are called, might typically operate as business executives, students, writers, or in some other nongovernmental capacity. They perform those jobs in addition to doing their espionage. If they are caught in the act of spying, they do not have diplomatic immunity and are subject to the full force of the local law, including prosecution for espionage and imprisonment. NOCs usually receive less scrutiny and surveillance from the local authorities than their official colleagues.*
>
> -- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)

> According a Congressional Research Service report, placing U.S. intelligence officials in foreign countries under "nonofficial cover" (NOC) in businesses or other private capacities is possible, but it presents significant challenges to U.S. agencies. Administrative mechanisms are vastly more complicated [than those] for officials formally attached to the embassy; special arrangements have to be made… The responsibilities of operatives under nonofficial cover to the parent intelligence agency have to be reconciled with those to private employers, and there is an unavoidable potential for conflicts of interest…
>
> -- CRS Report RL33539, *Intelligence Issues for Congress*, 14 Sep 2011, p. 6

Non-Permissive Environment. An operational environment in which host government forces, whether opposed to or receptive to operations that a unit intends to conduct, do not have effective control of the territory and population in the intended operational area (Uncertain Environment); or an operational environment in which hostile forces have control as well as the intent and capability to oppose or react effectively to the operations a unit intends to conduct (Hostile Environment). (National Military Strategy to Combat Weapons of Mass Destruction, Feb 2006)

Non-Title 50 (NT50). Refers to those federal departments and organizations whose authorities derive from portions of United States Code other than Title 50, which addresses U.S. intelligence activities. NT50s are involved in many activities that affect national security, such as conducting foreign affairs; combating pandemic diseases; halting illicit trafficking; conducting scientific and medical research; regulating finance, commerce, and transportation; and protecting food, water and nuclear infrastructures.

Notice of Intelligence Potential (NIP). A document alerting consumers of a potential collection opportunity involving sources, It is often associated with travel by the source or attendance at some event. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Notional. Fictitious; most commonly used to refer to a nonexistent agent but also used to refer to fictitious organizations, individuals, or sources of information. (FBI FCI Terms)

-- Also, fictitious, imaginary, existing only in the perception of the target. Antonym of real, true, genuine, or legitimate. (CIA, D&D Lexicon, 1 May 2008)

-- Also, Notionals: fictious [sic], private commercial entities which exist on paper only. They serve as the ostensible employer of intelligence personnel, or as the ostensible sponsor of certain activities in support of clandestine operations. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Notorious Individual. Someone who is widely known and has an unfavorable public reputation. (DoDD S-5200.37, Management and Execution of Defense HUMINT (U), 9 Feb 2009 w/. chg 2)

O ==========

OFCO. Acronym, see *Offensive Counterintelligence Operation*.

Offensive Counterintelligence Operation (OFCO). A clandestine CI activity conducted for military, strategic, DoD, or national CI and security purposes against a target having suspected or known affiliation with FISS [Foreign Intelligence & Security Service], international terrorism, or other foreign persons or organizations, to counter terrorism, espionage, or other clandestine intelligence activities that threaten the security of the Department or the United States. The two types of OFCO are double agent operations and Counterintelligence Controlled Source Operations (CSO). (DoDI S-5240.09, OFCO, 29 Oct 2008)

If defensive counterintelligence is checkers, then offensive counterintelligence is chess.

-- Steven Aftergood, "DIA Takes on Offensive Counterintelligence," *Secrecy News* (12 Aug 2008)

An ideal counterintelligence system anticipates the enemy's move, notionally satisfies his needs, and indeed operates a notional intelligence service for him.

-- Eric W. Timm, "Countersabotage--A CI Function" *Studies in Intelligence*, V7:2 (Spring 1963), p. 67

Offensive CI operations – CI folks call OFCO – are clandestine CI activities run in support of DoD military national security objectives and programs against individuals known or suspected to be foreign intelligence officers with connections to foreign intelligence or international terrorist activities. And they're run to counter the foreign intelligence operations, espionage, against DoD national activities and, of course, terrorist operations against DOD or national. These are very tightly controlled departmental activities run by a small group of specially selected people within DoD. There are only four organizations in the department that can run these operations – Army Counterintelligence, Naval Criminal Investigative Service, Air Force Office of Special Investigations, and now DIA with the center [Defense CI & HUMINT Center].

-- Toby Sullivan, Director of Counterintelligence for USD/I, 5 Aug 2008;
see Federal News Service transcript at <http://www.fas.org/irp/news/2008/08/dia-dchc.pdf>

Offensive counterintelligence could exploit knowledge of secret adversary infrastructures to keep adversaries off-balance and to force them to divert critical resources to defend against the offensive thrusts of well-informed enemies. Offensive counterintelligence can also deceive and manipulate the leaders of hostile coalitions, as Western governments did repeatedly in WWII, and in the Gulf War.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence*, with new introduction by the author (paperback 2001), p. xxx

---

For detailed information concerning DoD OFCO see DoDI S-5240.09, *OFCO (U),* 29 Oct 2008

Many… offensive operations have changed history, but remain a misunderstood, and even unappreciated, CI penetration methodology.

-- CI Centre (www.cicentre.com)

-- Also (previously defined in DoDD O-5240.02, dated 20 Dec 2007), an approved CI operation involving a formally recruited human source conducted for DoD or national purposes against a target having suspected or known foreign intelligence and security services affiliation, international terrorist affiliation, or other foreign persons or organizations, to counter terrorism, espionage, or other clandestine intelligence activities that threaten the security of the Department and/or the United States. *Note: this definition was deleted from DoDD O-5240.02 with change 1 dated 30 Dec 2010*.

Offensive Cyber Operations (OCO). Cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 1-02 and JP 3-12, Cyberspace Operations, 5 Feb 2013)

-- Also, includes all US Government programs and activities that, through the use of cyberspace, 1) actively gather information from computers, information systems or networks or 20 manipulate, disrupt, deny, degrade, or destroy targeted adversary computers, information systems, or networks. (NSPD-38)

-- Also, offensive operations to destroy, disrupt, or neutralize adversary cyberspace capabilities both before and after their use against friendly forces, but as close to their source as possible. The goal of Offensive Cyberspace Operations (OCO) is to prevent the employment of adversary cyberspace capabilities prior to employment. This could mean preemptive action against an adversary. (DSS Glossary)

Official Information. Information that is owned by, produced for or by, or is subject to the control of the United States Government. (JP 1-02 and JP 3-61, Public Affairs, 25 Aug 2010)

Office of Foreign Missions (OFM). An office in the Department of State, Bureau of Diplomatic Security that has three missions: 1) Protecting the interests of the US and its citizens from foreign diplomats' abuses of privileges and immunities; 2) Improving the treatment of US· personnel assigned abroad by imposing reciprocal treatment on foreign diplomats assigned to the US; and 3) Services to the foreign diplomatic community in a variety of areas. Programs include the review of all notifications by foreign missions of any intent to acquire property in the US and monitoring of foreign diplomatic travel.

Office of the National Counterintelligence Executive (ONCIX). [The U.S. Government agency] charged with integrating the activities of all CI programs to make them coherent and efficient, coordinating CI policy and budgets to the same end, and evaluating the performance of the CI community against the [National CI] strategy. (National Intelligence: A Consumer's Guide - 2009) Also see *National Counterintelligence Executive.*

-- Also, ONCIX provides effective leadership and support to the counterintelligence and security activities of the US Intelligence Community, the US Government, and US private sector entities who are at risk of intelligence collection or attack by foreign adversaries. (www.ncix.gov; accessed 9 Jun 2014)

> The ONCIX is part of the Office of the Director of National Intelligence and is staffed by senior counterintelligence (CI) and other specialists from across the national intelligence and security communities. The ONCIX develops, coordinates, and produces:
> - Annual foreign intelligence threat assessments and other analytic CI products
> - An annual national CI strategy for the US Government
> - Priorities for CI collection, investigations, and operations
> - CI program budgets and evaluations that reflect strategic priorities
> - In-depth espionage damage assessments
> - CI awareness, outreach, and training standards policies.
>
> -- www.ncix.gov (accessed 9 Jun 2014)

Office of Special Investigations (OSI). See Air *Force Office of Special Investigations* (AFOSI).

One-Time Pad (OTP). Sheets of paper or silk printed with random five-number group ciphers to be used to encode and decode enciphered messages. (CI Centre Glossary)

-- Also, groups of random numbers or letters arranged in columns, used for encoding and decoding messages. Since the codes are only used once, a properly employed OTP is theoretically unbreakable. (Spycraft)

-- Also, sheets of randomly generated numbers, usually formatted into four- or five-digit groups. Each party to the secret communication… uses the same one-time pad. By a simple process of alphabetic substitution, along with "false subtraction" and "false addition," the two sides can securely communicate with each other. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

-- Also, manual one-time cryptosystem produced in pad form. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

An unbreakable cipher when used properly

One-time pad (OTP), also called Vernam-cipher or the perfect cipher, is a crypto algorithm where plaintext is combined with a random key. It is the only known method to perform mathematically unbreakable encryption. See <http://users.telenet.be/d.rijmenants/en/onetimepad.htm>

One-Time Source. A source who, may not reasonably be expected to provide information on a regular or continuing basis by reason of limited knowledgeability or circumstances of contact. (HDI Lexicon, April 2008)

-- Also, a source of information of value that was, and will be, encountered only once. (US Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

A one-time source cannot be tasked to collect information, but can be sensitized to information in which the collector is interested.

For more information see: <http://users.telenet.be/d.rijmenants/en/onetimepad.htm>

One-Way Radio Link (OWRL). The method of transmitting over radio (by voice, key, or impulses) messages to intelligence personnel who, by prearrangement, are in possession of a time schedule, signal, code, or cipher that enables them to receive and decipher messages. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

One-Way Voice Link (OWVL). One-way radio link that transmits a coded voice message to intelligence personnel who, by prearrangement, are in possession of a time schedule, signal, code, or cipher that enables them to receive and decipher messages. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, shortwave radio link used to transmit prerecorded enciphered messages to an operative, who is usually working in place in a hostile area. (CI Centre Glossary)

Open. Not classified or concealed. (CIA, D&D Lexicon, 1 May 2002)

Open Source. Any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure. (Army Techniques Publication 2-22.9, Open-Source Intelligence, 10 Jul 2012)

Open Source Acquisition. The act of gaining possession of, or access to open source information synonymous with "open source collection." The preferred term is acquisition because by definition, open sources are collected and disseminated by others[,] open source exploiters acquire previously collected and publicly available information second-hand. (ICD 301, National Open Source Enterprise, 11 Jul 2006) Also see *open source information* and *open source intelligence*.

Open Source Center (OSC). Advances the Intelligence Community's exploitation of openly available information to include the Internet, databases, press, radio, television, video, geospatial data, photos and commercial imagery; functions include collection, analysis and research, training and information technology management to facilitate government-wide access and use. The Director CIA will administer the Center on behalf of the DNI. (ODNI News Release 6-05, 8 Nov 2005)

-- Also, the OSC acts as a service of common concern to advance the IC's exploitation of open source material and nurtures acquisition, procurement, analysis, dissemination, and sharing of open source information, products, and services throughout the USG; established at CIA and builds on the former Foreign Broadcast Information Service and will include personnel from across the IC and other USG organizations; Dir CIA serves as the DNI's Executive Agent for the Center. (ICD 310, National Open Source Enterprise, 11 Jul 2006)

Open Source Collection. See *Open Source Acquisition*.

Open Source Information. Publicly available information which anyone can lawfully obtain by request or observation. (ICD 301, National Open Source Enterprise, 11 Jul 2006)

-- Also, information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access. (JP 2-0, Joint Intelligence, 22 Oct 2013)

We have no need for spies. We have the Times.
-- Tsar Nicholas I cited in Haswell, *Spies and Spymasters* (1977)

Open Source Intelligence (OSINT). Intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (PL109-163 § 931 and ICD 1, 1 May 2006)

"Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond."
-- Lieutenant General Samuel V. Wilson, USA (Ret.), Former Director, Defense Intelligence Agency

-- Also, relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, publicly available information appearing in print or electronic form, including information from radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings used to enhance intelligence analysis and reporting. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to intelligence requirements. (Army FM 2-22.9, Open Source Intelligence, Dec 2006)

-- Also, the discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (Army FM 2-0, Intelligence, 23 Mar 2010)

OSINT generally falls into four categories: 1) widely available data and information; 2) targeted commercial data; 3) individual experts; and 4) "gray" literature, which consists of written information produced by the private sector, government, and academe that has limited availability, either because few copies are produced, existence of the material is largely unknown, or access to information is constrained.

OSINT can include: media such as newspaper, magazines, radio, television, and computer-based information; public data such as government reports, and official data such as budgets and demographics, hearings, legislative debates, press conferences, and speeches; information derived from professional and academic sources such as conferences, symposia, professional associations, academic papers, dissertations and theses, and experts; commercial data such as commercial imagery; *gray literature* such as trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, and market surveys; and information, which although unclassified, could be considered company proprietary, financially sensitive, legally protected, or personally damaging, as well as information derived from Internet blogs.

-- CRS Report RL34270, 5 Dec 2007

Clandestine technical and humint sources can be used to confirm this kind of special take from open sources—and open sources can be used to confirm the information from clandestine sources.

-- Roy Godson*, Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 204

Operation Order (OPORD). A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Operation Plan (OPLAN). 1) Any plan for the conduct of military operations prepared in response to actual and potential contingences; 2) A complete and detailed joint plan containing a full description of the concept of operations, all annexes applicable to the plan, and a time-phased force and deployment data. (JP 5-0, Joint Operation Planning, 11 Aug 2011)

Operational Control (OPCON). The authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Operational Cycle (Ops Cycle). See *recruitment cycle*.

Operational Environment. A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Operational Intelligence. Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *strategic intelligence; tactical intelligence*.

Operational Interest (OI). [Within HUMINT usage] exclusive contact with a source, as established by a HUMINT organization. Within DoD, established for all sources upon IDSRS Deconfliction and assignment of a NFN. Between DoD and other national agencies, granted for clandestine leads and sources by the Interagency Source Registry (ISR). (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, see classified definition in AR 381-20, Army CI Program (U), 25 May 2010.

Operational Level of War. The level of war at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *tactical level of war; strategic level of war*.

Operational Proposal. A formal document prepared by DoD collection elements to outline a proposed activity or operation. (HDI Lexicon, April 2008)

Operational Testing. A continuing process of evaluation that may be applied to either operational personnel or situations to determine their validity or reliability. (JP 1-02)

-- Also, any means or process employed to establish authenticity, reliability, or control. (HDI Lexicon, April 2008)

Operational Warning. A warning to theater level or equivalent decision makers of developing situations or ongoing event which may initiate operational planning or trigger the execution or change in status of standing operations or contingency plans. (DoDD 3115.16, The Defense Warning Network,5 Dec 2013)

Operations Officer - CIA. A career track within the *Core Collector* profession of the National Clandestine Service (NCS), Central Intelligence Agency (CIA). Operations Officers (OO's) are focused full time on clandestinely spotting, assessing, developing, recruiting, and handling individuals with access to vital foreign intelligence on the full range of national security issues. OO's use their sound judgment, high integrity, strong interpersonal skills, and ability to assess the character and motivations of others to establish strong human relationships and trust that provides the foundation needed to acquire high-value intelligence from foreign sources. An OO's career can include assignments in the NCS's three key areas of activity—human intelligence collection, counterintelligence, and covert action—on issues of highest interest to US national security, such as international terrorism, weapons proliferation, international crime and narcotics trafficking, and capabilities and intentions of rogue nations. Operations Officers serve the bulk of their time in overseas assignments that range typically from 2-3 years. (CIA; see <https://www.cia.gov/careers/jobs/view-all-jobs/core-collector.html>; accessed 19 Mar 2009)

Operations Security (OPSEC). A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level. (DoDD 5205.02E, DoD OPSEC Program, 20 Jun 2012)

-- Also, a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) identify those actions that can be observed by adversary intelligence systems; b) determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02 and JP 3-13.3, Operations Security, 4 Jan 2012)

OPSEC's most important characteristic is that it is a process and not a collection of specific rules and instructions that can be applied to every operation or activity

Although good operational security (Opsec) does not guarantee the success of any intelligence operation, faulty Opsec almost surely guarantees worse than failure.

-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), p. 33

OPSEC… is a systematic and proved process… [to] deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.

-- NSDD 298, *National Operations Security Program*, 22 Jan 1988, p.1

[T]here is a clear and compelling need for operational security in a military environment and in the conduct of sensitive operations.

-- Joint Security Commission, *Redefining Security*, 28 Feb 1994, p. 66

Director, DIA provides intelligence and counterintelligence threat analysis to support OPSEC planning to all DoD Components. .

– DoDD 5205.02E, *DoD OPSEC Program*, 20 Jun 2012, p. 5

National OPSEC Program

In 1988, President Ronald Reagan signed *National Security Decision Directive 298* (NSDD 298). This directive established the "National Operations Security Program" as a means to identify, control, and protect unclassified information and evidence associated with U.S. national security programs and activities.

NSDD 298 named the Director, National Security Agency, as the Executive Agent for interagency OPSEC training and included in his responsibilities the establishment and maintenance of the **Interagency OPSEC Support Staff (IOSS).**

The primary responsibility of the IOSS is to act as a consultant to other U.S. government departments or agencies by providing technical guidance and assistance that will result in self-sufficient OPSEC Programs for the protection of U.S operations. Members of the IOSS staff assess OPSEC programs, assist in OPSEC program development, conduct surveys, assessments and provide OPSEC training.

See IOSS web site at: <https://www.iad.gov/ioss/>

Operations Security Assessment (OPSEC Assessment). An evaluative process, usually exercise, or support function to determine the likelihood that critical information can be protected from the adversary's intelligence. (JP 1-02 and JP 3-13.3, Operations Security, 4 Jan 2012)

Operations Security Countermeasures (OPSEC Security Countermeasures). Methods and means to gain and maintain essential secrecy about critical information. (JP 1-02 and 3-13.3, Operations Security, 4 Jan 2012)

Operations Security Indicators (OPSEC Indicators). Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (JP 1-02 and JP 3-13.3, Operations Security, 4 Jan 2012)

Operations Security Process (OPSEC Process). A process that examines a complete activity to determine what, if any, exploitable evidence of classified or sensitive activity may be acquired by adversaries. It is an analytical, risk-based process that incorporates five distinct elements: 1) critical information identification; threat analysis; 3) vulnerability analysis; 4) risk assessment; and 5) OPSEC countermeasures. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

The operations security process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate countermeasures.
-- NSDD 298, *National Operations Security Program*, 22 Jan 1988

Operations Security Survey (OPSEC Survey). An application of the OPSEC process by a team of subject matter experts to conduct a detailed analysis of activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries. (DoDD 5205.02E, DoD OPSEC Program, 20 Jun 2012)

-- Also, a collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence processes. (JP 1-02 and JP 3-13.3, Operations Security, 4 Jan 2012)

Operations Security Vulnerability (OPSEC Vulberability). A condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decisionmaking. (JP 1-02 and JP 3-13.3, Operations Security, 4 Jan 2012)

Operations Support Element (OSE). An element that is responsible for all administrative, operations support and services support functions within the counterintelligence and human intelligence staff element of a joint force intelligence directorate. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) [Normally in the J2X]

OPSEC, See *Operations Security*,

Organized Cyber Intruders/Attackers. Those individuals, groups or organizations who violate international law or conventions relating to computer networks or who otherwise use the cyberspace domain to interfere with, disrupt, or deny computer network services. (OSD, *Guidance for Employment of the Force*)

Original Classification Authority (OCA). An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to initially classify information. (DoD IG Evaluation Guide, 22 Jan 2013)

-- Also, an individual authorized in writing, either by the United States (U.S.) President, or by agency heads or other officials designated by the President, to classify information in the first instance. OCAs must receive training to perform this duty. (DSS Glossary)

> *OCAs and other individuals delegated declassification authority in writing by the head of the IC element may declassify information within their purview pursuant to EO 13526 and 32 CFR Part 2001 guidelines. Only the DNI may declassify space-based national imagery, pursuant to EO 12951.*
>
> -- ICD 710, *Classification Management and Control Markings System*, 21 Jun 2013

Other Government Agency (OGA). Within the context of interagency coordination, a non Department of Defense agency of the United States Government. (JP 1-02)

Overhead Reconnaissance. Activities carried out by space-based capabilities whose principal purpose is conducting and/or enabling intelligence collection. These activities are comprised of associated R&D, acquisition, test and evaluation, and system operations performed on or by satellites, communications, and facilities for data processing as well as command and control of spacecraft and payloads. (DoDD 5105.23, NRO, 28 Jun 2011)

Overt. Activities that are openly acknowledged by or readily attributable to the US Government, and include activities designed to acquire information through legal and open means without concealment. Overt information may be collected by observation, elicitation, or from knowledgeable human sources. (ICD 304, HUMINT, 6 Mar 2008; DoDD S-5200.37, 9 Feb 2009; JP 1-02; and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, refers to being in the open, without any attempt to deceive or mislead, with full knowledge of coordinating units or agencies; activity done without attempt to conceal it. (CI Community Lexicon)

-- Also, methods of conducting DoD activities that may be acknowledged by or attributable to the U.S. Government. (HDI Lexicon, April 2008)

Overt Collection. Intelligence activities with the ultimate goal of intelligence information collection which are not designed or executed to conceal sponsorship, collection activity, identity of operators, or methodologies employed. (Previously in DoDI S-5240.17, CI Collection, 12 Jan 2009) Also see *open source intelligence.*

-- Also, the acquisition of intelligence information in the public domain. (CI Community Lexicon)

> ***"While the importance of clandestine collection should not be underestimated, many of the pieces of the jigsaw puzzle which is 'finished foreign intelligence' can be overtly collected by a well-organized information gathering system."***
>
> -- Rockefeller Commission Report (June 1975), p. 209

Overt Intelligence. Information collected openly from public or open sources. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Overt Operation. An operation conducted openly, without concealment. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Overt [HUMINT] Operations. Openly acknowledged by, or are readily attributable to, the US Government. Overt HUMINT methods include: debriefing, interrogation, elicitation, and observation. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

P ==========

Packet Sniffer. Software that observes and records network traffic. (NIST, Glossary of Key Information Security Terms, May 2013)

Parallel Investigative Jurisdiction. One or more agencies with differing objectives having simultaneous authority to investigate a matter or incident. An example would be a criminal matter that has a national security implication, which might require investigation by both a CI organization and a criminal investigative organization. (AR 381-20, Army CI Program, 25 May 2010)

Paramilitary Forces. Forces or groups distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission. (JP 1-02 and JP 3-24, Counterinsurgency, 22 Nov 2013)

Parole. A prearranged verbal exchange used for recognition and identification between intelligence personnel. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, a prearranged verbal exchange used by intelligence personnel to identify themselves to each other. (FBI FCI Terms)

Passive Source. An individual recruited by a military CI agency to act as a listening post for CI purposes in a location associated with the individual's job or social status. This source undertakes no actions unless associated with such status. A passive source is recruited or placed in an area that foreign intelligence would consider a priority target and there is evidence of foreign intelligence spotting, assessing, or recruiting activities. (AFOSI Manual 71-119, CI Investigations, 27 Oct 2009)

Pattern Recognition. An inductive process of recognizing a commonality or trend in an aggregate of indications from which as plausible explanation or model can be developed. (Word of Intelligence, 2nd Edition, 2011)

Patterns. [In CI usage,] …repeated incidents that may be similar in nature or dissimilar events that occur in a specific location or time span that may indicate potential FISS and ITO [international terrorist organization] targeting or information exploitation. (Army FM 2-22.2, CI. Oct 2009)

Patriot Act (aka USA Patriot Act). The official title is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." An act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes. (PL 107-56, 26 Oct 2001; codified as amended at 50 USC § 1861)

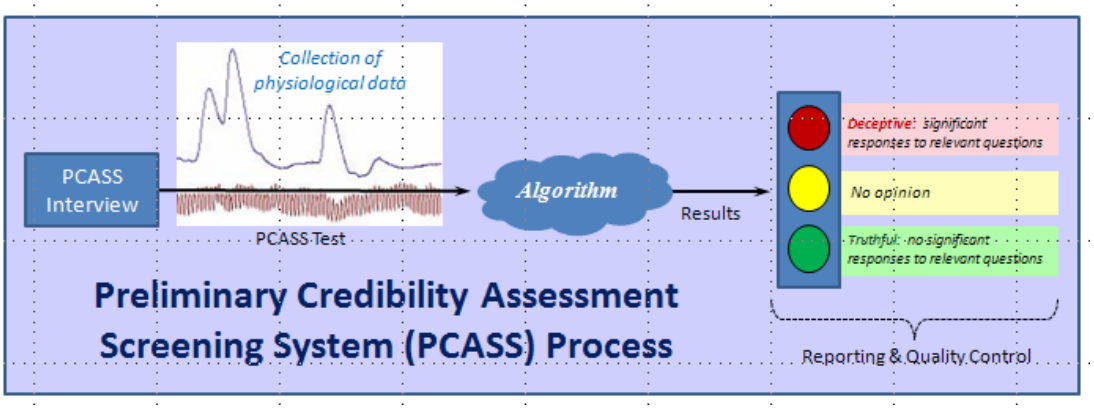
> The Patriot Act substantially expanded the authority of U.S. law enforcement agencies for the stated purpose of fighting terrorism in the United States and abroad. Among its provisions, the Act:
> -- increased the ability of law enforcement agencies to search telephone and e-mail communications and medical, financial and other records;
> -- eased restrictions on foreign intelligence gathering within the United States;
> -- expanded the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and
> -- enhanced the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts.
>
> The act also expanded the definition of terrorism to include "domestic terrorism," thus enlarging the number of activities to which the Patriot Act's expanded law enforcement powers can be applied.

The Patriot Act made a number of changes to U.S. law. Key acts changed were the Foreign Intelligence Surveillance Act of 1978 (FISA), the Electronic Communications Privacy Act of 1968 (ECPA), the Money Laundering Control Act of 1986, and Bank Secrecy Act (BSA), as well as the Immigration and Nationality Act.

Additional information on the Patriot Act available on NCIX website at: <http://www.ncix.gov/publications/law/index.html>

PCASS. Acronym for "Preliminary Credibility Assessment Screening System." (DoDI 5210.91, Polygraph and Credibility Assessment Procedures, 12 Aug 2010 with change 1 dated 15 Oct 2013) Also see *PCASS Instrument; polygraph examination*.

PCASS Instrument. A diagnostic instrument used during an interview capable of monitoring, recording, and/or measuring electrodermal and vasomotor activity. The PCASS instrument uses an algorithm to evaluate the physiological responses recorded by the two components. (DoDI 5210.91, Polygraph and Credibility Assessment Procedures, 12 Aug 2010 with chg 1 dated 15 Oct 2013) See *PCASS*.



The PCASS shall only be used as a field-expedient tool to screen persons of interest for intelligence and security purposes. Only certified personnel may conduct PCASS examinations.

Per DoD policy, the PCASS will not be used to test U.S. persons (however does not apply to PCASS examinations conducted for training); see Enclosure 5, DoD Instruction 5210.91.

Peace Operations (PO). A broad term that encompasses multiagency and multinational crisis response and limited contingency operations involving all instruments of national power with military missions to contain conflict, redress the peace, and shape the environment to support reconciliation and rebuilding and facilitate the transition to legitimate governance. Peace operations include peacekeeping, peace enforcement, peacemaking, peace building, and conflict prevention efforts. (JP 3-07.3 Peace Operations, 17 Oct 2007)

Peace Building. Stability actions, predominately diplomatic and economic, that strengthen and rebuild governmental infrastructure and institutions in order to avoid a relapse into conflict. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Peace Enforcement. Application of military force, or the threat of its use, normally pursuant to international authorization, to compel compliance with resolutions or sanctions designed to maintain or restore peace and order. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Peacekeeping. Military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (cease fire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Peacemaking. The process of diplomacy, mediation, negotiation, or other forms of peaceful settlements that arranges an end to a dispute and resolves issues that led to it. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Pen Register. A device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider, or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any devise used by a provider, or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business; see 18 USC §3127(3). (AR 381-10, US Army Intelligence Activities, 3 May 2007) Also see *trap and trace*.

-- Also, [a device that] records or decodes dialing, routing addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided that such information must not include the contents of any communication. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

> A *pen register* captures all outgoing phone numbers a particular telephone has called. A *trap and trace device* identifies all incoming phone numbers to a particular telephone.
>
> *Pen register and trap and trace (PR/TT) devices enable the prospective collection on non-content traffic information associated with wire and electronic communications, such as: the phone numbers dialed from or to a particular telephone, including electronic communications; messages sent from or to a particular telephone; or the internet protocol (IP) address of communications on the Internet and other computer networks.*
>
> -- FBI Domestic Investigations and Operations Guide, 15 Oct 2011, p. 18-123

Penetration. [In intelligence usage,] the recruitment of agents within or the infiltration of agents or technical monitoring devices in an organization or group for the purpose of acquiring information or of influencing its activities. (ICS Glossary)

> *Note: This term was previously in JP 1-02, however rescinded by JP 2-01.2, 16 Mar 2011.*

-- Also, the recruitment of agents within, or the planting of agents or technical monitoring devices within, a target organization to gain access to its secrets or to influence its activities. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- Also, a principal counterintelligence objective is penetration of an adversary, and this can be achieved by the recruitment of a key source within an opponent's organization. Ideally, the penetration will be the recruitment of a senior figure with sufficient access to compromise all the service's operations, but lower-level penetrations, such as the management of a double agent, may be sufficient to reveal the identities of case officers and their operational premises. (*Historical Dictionary of Cold War Counterintelligence*, 2007)

> ***The best way to catch a spy is to recruit a spy***
>
> -- Counterespionage Maxim
>
> (cited in Stuart A. Herrington, *Traitors Among US: Inside the Spy Catcher's World*, 1999, p. 255)

Penetration – a time-honored espionage practice
…oh what a tangled web we weave

The key to CI success is penetration. For every American spy, there are several members of the opposition service who know who he or she is. No matter what it takes, we have to have penetrations.

-- James M. Olson, "The Ten Commandments of Counterintelligence," *Studies in Intelligence*, Vol. 54 No. 5; see <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol45no5/html/v45i5a08p.htm>

_____

Almost every spy that we have found, both in the CIA and FBI, has been found with the aid of recruited sources of our own on other hostile intelligence services.

-- William Webster, Former FBI Director and DCI, in Senate testimony (9 Apr 2002)

_____

If the purpose of counterespionage is to manipulate enemy intelligence, as it is, then to have controlled agents in the staff of an enemy service is the most important objective of counterintelligence.

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

_____

…[C]ounterespionage has one purpose which transcends all others in importance: ***penetration.*** *The only way to be sure that an enemy has been contained is to know his plans in advance and in detail. Moreover, only a high-level penetration of the opposition can tell you whether your own service is penetrated.*

…Conducting CE without the aid of penetrations is like fighting in the dark. Conducting CE with penetrations can be like shooting fish in a barrel. The famous case of Col. Oleg Penkovskiy… illustrates the great value of penetrations. There can never be enough of them.

-- Austin B. Matschulat, "Coordination and Cooperation in Counterintelligence," *Studies in Intelligence*, V13: 2 (Spring 1969), pp. 29-30.

_____

Penetrating an adversary's intelligence service, especially the counterintelligence units, is one of the most valuable counterintelligence techniques. Often it is also notoriously difficult.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 207

_____

All countries… strive hard to secure penetration agents; and they constitute the counter-intelligence officer's worst nightmare.

-- Chapman Pincher. *Traitors: The Anatomy of Treason*, First U.S. Edition (1987), p. 29

_____

Penetrations - selected examples:

-- Colonel L Oleg V. Penkovsky was a British-US penetration of Soviet military intelligence (GRU).
-- Harold A.R. "Kim" Philby was a Soviet penetration of British intelligence.
-- Aldrich "Rick" Ames was a Soviet/Russian penetration of the CIA.
-- Robert (Bob) Hanssen was a Soviet/Russian penetration of the FBI.

Penetration Operation. The recruitment of agents within, the infiltration of agents, or the introduction of technical monitoring devices into an organization or physical facility to acquire information or influence the organization's activities. (AR 381-47, OFCO, 17 Mar 2006) Also see *recruitment-in-place*.

Penetration Testing. [In computer usage] a test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Pentagon Force Protection Agency (PFPA). [DoD agency that] provides force protection, security, and law enforcement to safeguard personnel, facilities, infrastructure, and other resources for the Pentagon Reservation and designated DoD facilities within the National Capital Region (NCR). (DoDD 5105.68, PFPA, 5 Dec 2013)

Perception Management. *Within DoD: None -- term removed from JP 1-02.*

Periodic Reinvestigation (PR). An investigation conducted every 5 years for the purpose of updating a previously completed background or special background investigation. The scope consists of a personal interview, National Agency Check (NAC), Local Agency Check (LAC), credit bureau checks, employment records, employment references, and developed character references, and normally will not exceed the most recent 5-year period. (DSS Glossary)

Permissive Environment. Operational environment in which host country military and law enforcement agencies have control as well as the intent and capability to assist operations that a unit intends to conduct. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

PERSEREC. See *Defense Personnel Security Research Center*.

Persistent Conflict. The protracted confrontation among state, nonstate, and individual actors that are increasingly willing to use violence to achieve their political and ideological ends. (Army FM 3-0, Operations, Feb 2008)

Persistent Surveillance. *Within DoD: None -- term removed from JP 1-02.*

> Previously defined in JP 1-02 and JP 2-0, Joint Intelligence (22 Jun 2007) as: a collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in near or real-time. Persistent surveillance facilitates the prediction of an adversary's behavior and the formulation and execution of preemptive activities to deter or forestall anticipated adversary courses of action

Persona. The social façade or image a person projects in public. A persona may be true or false. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

Persona Non Grata (PNG). An international diplomatic term meaning "person who is not acceptable or not welcome." It is a legal status applied to diplomats who have been caught by the host country in espionage or other unlawful activities and are expelled and thereafter denied access to the host country. (CI Community Lexicon)

> Latin for "unwelcome person." The provision for declaring a person *persona non grata* is codified in international law; see Article 9 of the Vienna Convention on Diplomatic Relations of 1961.

-- Also, a diplomatic expulsion by flag accrediting country. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, the official act of declaring a foreign national unwelcome in this country. (FBI FCI Terms)

-- Also, in diplomatic usage and under international law, the official act of declaring a foreign national, usually an official of a foreign government, as no longer welcome and forcing his/her expulsion. In tradecraft terminology, the undesirable individual is *PNG'd*. The most common use of *PNG* is for foreign diplomatic or official personnel caught in the act of engaging in illegal espionage activities. (*The CIA Insider's Dictionary*, 1996)

Personal Meeting (PM). Face-to-face contact between a handler and a lead or asset. (HDI Lexicon, April 2008)

-- Also, a clandestine meeting between two operatives, always the most desirable but a more risky form of communication. (CI Centre Glossary)

> *Personal meetings may be held to give an agent his next assignment and instructions for carrying it out, to train him in tradecraft or the use of technical or communications equipment, to transmit documents, reports, technical equipment, money, or other items, or to fulfill several of these purposes. In actual practice several purposes are usually served by a meeting. In addition to its particular objectives more general needs can be filled. A meeting held for training purposes may be a means for clarifying biographic data on the agent or his views on various subjects. At every meeting with an agent one should study him and obtain new data on his potential and talents, thereby providing a better basis for judging his sincerity and deciding how much trust to place in him.*
>
> -- L.K. Berrenev, 'Operational Contacts," *Studies in Intelligence*, Vol 9, Winter 1965, p.64 [declassified 18 Sep 1995; originally classified SECRET].

Personal Protective Security Detail. Security personnel assigned to protect individuals who, by their grade, assignment, symbolic value, or relative isolation, are likely attractive or accessible terrorist targets. These trained and armed personnel are capable of providing continuous protection for designated individuals. (DoDD 5105.68, PFPA, 5 Dec 2013)

Personally Identifiable Information (PII). Information which can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual. Includes information about an individual that identifies, links, relates, or is unique to, or describes him or her (e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home or office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc). (DoDD 5400.11, DoD Privacy Program, 8 May 2007)

-- Also, information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. (DSS Glossary)

Personnel Security. The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions. (DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012, w/ chg 1)

-- A security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information. (IC Standard 700-1, 4 Apr 2008)

-- Also, [with US Army] the application of standards and criteria to determine whether or not an individual is eligible for access to classified information, qualified for assignment to or retention in sensitive duties, and suitable for acceptance and retention in the total Army consistent with national security interests. (AR 380-67, Personnel Security Program, 24 Jan 2014)

> *The essence of personnel security is to determine that those who have access to secrets as a result of their jobs are people of sufficient probity and responsibility who will safeguard that data.*
>
> -- Frederick L. Wettering, "Counterintelligence: The Broken Triad." *International Journal of Intelligence and Counterintelligence* 13 (Fall 2000), pp. 265-299.
>
> ---
>
> ***Personnel Security—The First and Best Defense***
>
> *The personnel security system is a the very heart of the government's security mission. …{The main purpose of personnel security programs is to protect the national security interests of the United States by insuring the reliability and trustworthiness of those whom information vital to those interests is entrusted.*
>
> -- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, p. 39
>
> ---

For additional information see -- Personnel Security References

EO 12968, *Access to Classified Information*

EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*

DoD 5200.2-R, *Personnel Security Program*

For Army policy see: AR 380-67, *Personnel Security Program*

Personnel Security Investigation (PSI). An inquiry into the activities of an individual, designed to develop pertinent information pertaining to trustworthiness and suitability for a position of trust as related to loyalty, character, emotional stability, and reliability. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

DoD generates 90% of the security investigation requirements in the Executive Branch….
-- Security and Suitability Process Reform: Strategic Framework, Feb 2010

_____

A PSI is an inquiry into an individual's loyalty, character, trustworthiness, and reliability to ensure that he/she is eligible to access classified information, or for an appointment to a sensitive position or position of trust. DoD uses PSIs to determine an individual's eligibility for a security clearance.

In 2005, DoD transferred most of its PSI workload to U.S. Office of Personnel Management (OPM). All PSIs are conducted by the designated investigative service provider. In the case of DoD, OPM is the designated investigative service provider.

The types of PSIs vary based on the level of security clearance necessary for a given sensitive position. The personnel security clearance process is governed primarily by EO 12968 (Access to Classified Information), EO 13467 (Reforming Processes Related to Suitability for Government Employment) and the Federal Investigative Standards. DoD Regulation 5200.2-R, "Personnel Security Program," outlines criteria for sensitive positions and the corresponding clearance levels.

-- Also, any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DoD, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations…conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position. (AR 380-67, Personnel Security Program, 24 Jan 2014)

Pharming. Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential data, e.g., mimicking bank websites.
(FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

Phishing. Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, usually an email that looks like it is from a legitimate organization or person, but is not and contains a link or file with malware. Phishing attacks typically try to snag any random victim. Spear phishing attacks target a specific person or organization as their intended victim. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

-- Also, a form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. (McAfee.com; accessed 15 Nov 2010)

-- Also, Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. (Words of Intelligence, 2nd Edition, 2011)

Phreaking. Gaining unauthorized access to telecommunication systems. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

Physical Search. Any intrusion upon a person or a person's property or possessions to obtain items of property or information. The term does not include examination of areas that are in plain view and visible to the unaided eye if no physical trespass is undertaken, and does not include examinations of abandoned property left in a public place. (DoD 5240.1-R, Dec 1982) Also see *search*.

Types include consented physical search, plain view search, search incident to a lawful apprehension, and nonconsensual physical search. See USC §1821(5).

For DoD CI see Chapter 7, Procedure 7-Physical Searches, DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 7 Dec 1982

Physical Security. The security discipline concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012 w/ chg 1 dated 24 Apr 2013)

The physical protection of information, assets and personnel is fundamental to nay security system.
-- Joint Security Commission Report, *Redefining Security*, 28 Feb 1994, p. 56

-- That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 1-02 and JP 6-0, Joint Communications Systems, 10 Jun 2010)

-- Also, the security discipline concerned with physical measures designed to: protect personnel; prevent unauthorized access to facilities, equipment, material, and documents; and defend against espionage, terrorism, sabotage, damage, and theft. (IC Standard 700-1, 4 Apr 2008)

Physical Security Investigation. All inquires, inspections, or surveys of the effectiveness of controls and procedures designed to provide physical security; and all inquires and other actions undertaken to obtain information pertaining to physical threats to DoD personnel or property. (JP 1-02)

Physical Surveillance. A systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance. (DoD 5240.1-R, Dec 1982) Also see *surveillance*.

Surveillance, the job of following and observing designated persons without being noticed, is intrinsic to counterintelligence.
-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

For DoD CI see Chapter 9, Procedure 9 - Physical Surveillance, DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 7 Dec 1982

-- Also, physical surveillance (not requiring a court order): the deliberate observation… of persons, places, or events, on either a limited or continuous basis, in areas where there may or may not be a reasonable expectation of privacy. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

-- Also, physical surveillance (with a warrant or court order): a physical search constitutes any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in the seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011, p. 18-152)

Piracy. An illegal act of violence, depredation (e.g., plundering, robbing, or pillaging), or detention in or over international waters committed for private ends by the crew or passengers of a private ship or aircraft against another ship or aircraft or against persons or property on board such ship or aircraft. (JP 1-02)

Pitch. [In intelligence usage] the effort made to recruit a source. (HDI Lexicon, April 2008)

Placement. An individual's proximity to information of intelligence interest. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *access; placement & access.*

-- Also, the rationale for a HUMINT source or operational asset's presence in an operational area. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

Placement and Access (P&A). An individual's proximity to and ability to collect information of intelligence interest. (HDI Lexicon, April 2008) Also see *access.*

Plain Text. Unencrypted information. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Planned Target. Target that is known to exist in the operational environment, upon which actions are planned using deliberate targeting, creating effects which support commander's objectives. (JP 3-60, Joint Targeting, 13 Apr 2007)

Planning. The ability to establish a framework to employ resources to achieve a desired outcome or effect. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

-- Also, the process by which commanders (and the staff, if available) translate the commander's visualization into a specific course of action for preparation and execution, focusing on the expected results. (Army FM 3-0, Operations, Feb 2008)

Planning and Direction. In intelligence usage, the determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Planning Order (PLANORD). A planning directive that provides essential planning guidance and directs the initiation of execution planning before the directing authority approves a military course of action. (JP 5-0, Joint Operation Planning, 11 Aug 2011) Also see *execute order (EXORD).*

Plant. [In intelligence usage,] 1) to insert information into a target's intelligence channel; 2) an individual infiltrated into a foreign organization (a penetration); 3) a forged document provided to a foreign organization. (CIA in D&D Lexicon, 1 May 2002)

Planted Information. False or misleading information that the target has been permitted or helped to collect. (CIA in D&D Lexicon, 1 May 2002)

Platform. In collection parlance, the conveyance for collection sensors.

Plausible Denial. Official disclaimer supported by a believable cover story. (CIA in D&D Lexicon, 1 May 2002) Also see *plausible deniability*.

Plausible Deniability. The concept that allows the United States government, specifically the U.S. president himself, to claim no knowledge of or involvement in a covert action that goes public, particularly if it has gone badly. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Pocket Litter. The usual litter found in pockets: coins, tickets, keys, etc. In this case, pocket litter is planted so that if the agent is caught, incidental-looking items will reinforce his cover story. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

Police Information. All available information concerning known and potential enemy and criminal threats and vulnerabilities collected during police activities, operations, and investigations. Analysis of police information produces police intelligence. (ATTP 3-39.20, Police Intelligence Operations, Jul 2010)

Police Intelligence. Police intelligence results from the application of systems, technologies, and processes that analyze applicable data and information necessary for situational understanding and focusing policing activities to achieve social order. (ATTP 3-39.20, Police Intelligence Operations, Jul 2010)

Political Intelligence. Intelligence concerning foreign and domestic policies of governments and the activities of political movements. (JP 1-02)

Polygraph and Credibility Assessment (PCA). The overarching term covering programs, research, training, and procedures that employ technologies to assess an individual's truthfulness with the aid of technical devices that measure physiological data or behavioral activity. (DoDI 5210.91, PCA Procedures, 12 Aug 2010 with chg 1 dated 15 Oct 2013) Also see *polygraph examination*.

Polygraph Examination. A process that encompasses all activities that take place between a polygraph examiner and examinee during a specific series of interactions. (DoDD 5210.48, PCA Program, 25 Jan 2007 with change 2 dated 15 Nov 2013) Also see *credibility assessment; polygraph instrument*.

-- Also, a highly structure technique conducted by specialty trained CI personnel certified by proper authority as polygraph examiners. (Army FM 2-22.2, CI, Oct 2009)

Polygraph – Greek for "many writings"

The most significant contribution of the polygraph is its success in eliciting information and its value as a deterrent; however, the polygraph should be one of several investigative tools.

-- Webster Commission Report (*A Review of FBI Security Programs*), March 2002 (p. 68)

The polygraph is a multichannel instrument that records changes in respiration, cardiovascular activity, and skin resistance in response to questions. According to polygraph theory, when a subject gives a false response to a relevant question…, the physiological reaction will be greater than the reaction to others questions (control or irrelevant questions). However, contrary to popular belief, there is no physiological response that is unique to deception. The reactions measured by the polygraph can be caused by a variety of emotions. This fact underlies much of the controversy surrounding the polygraph. […]

Two types of polygraphs are currently used in personnel security screening the counterintelligence-scope(CI-scope) polygraph and the full-scope polygraph. The CI-scope polygraph focuses on espionage, sabotage, terrorism, mishandling classified information, and unauthorized contacts with representatives of foreign governments. […] Screening polygraphs arguably have a deterrent effect.

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, pp.61-70

The evidence is overwhelming that the polygraph, in the hands of a skilled examiner, is a very useful tool to elicit information from an applicant or an employee that might otherwise be obtained only after lengthy and costly investigation—or not at all.

-- DCI's Blue Ribbon Panel on the Polygraph, *CIA's Use of Polygraph in Personnel Screening*, Redacted Copy approved for public release 29 May 2012. Copy available at:
<http://www.nationalsecuritylaw.org/files/received/CIA/Poly_Use_of_Polygraphy_in_Personnel_Screening.pdf>

For additional information, see --

"Your Polygraph Examination" at:
<http://www.cdse.edu/multimedia/polygraph_videos/polygraph.pdf>

Committee to Review the Scientific Evidence on the Polygraph, *The Polygraph and Lie Detector (Washington,* DC: National Academies Press, 2003).

Ken Alder, *The Lie Detector: The History of an American Obsession* (New York: Free Press, 2007)

John F. Sullivan, *Gatekeeper: Memories of a Polygraph Examiner* (Washington, DC: Potomac Books, 2007)

Also see the American Polygraph Association (APA) web site at <http://www.polygraph.org/>

Polygraph Instrument. A diagnostic instrument to measure and record respiration, electrodermal, blood volume, and heart rate responses to verbal or visual stimuli. (DoDI 5210.91, Polygraph and Credibility Assessment Procedures, 12 Aug 2010 with chg 1 dated 15 Oct 2013) Also see *polygraph examination*.

PORTICO. The nickname for the DoD Counterintelligence Community's enterprise information capability that promotes information sharing and provides standardized CI activity reporting across the Department. PORTICO operates in a secure network environment and facilitates standardization of DoD CI business processes by providing a common interface for shared results of core CI functions (i.e., collection, investigations, analysis & production, operations, and functional services).

Port Security. The safeguarding of vessels, harbors, ports, waterfront facilities, and cargo from internal threats such as destruction, loss, or injury from sabotage or other subversive acts; accidents; thefts; or other causes of similar nature. (JP 1-02 and JP 3-10, Joint Security Operations in Theater, 3 Feb 2010)

Positive Intelligence. A term of convenience sometimes applied to foreign intelligence to distinguish it from foreign counterintelligence. (ICS Glossary, 1978)

-- Also, information gathered concerning a foreign power that is significant to national security, foreign relations, economic interest, and other plans and policies of a government. (CI Community Lexicon)

In the early 1900's military intelligence consisted of two separate fields of endeavor: positive intelligence and negative intelligence. Positive intelligence focused on "seeking information on our enemies or potential enemies" and negative intelligence focused on "preventing enemies or potential enemies from acquiring information of value about the United States." Following World War I, the term *negative intelligence* was replaced by *counterintelligence*.

-- Source: Bruce W. Bidwell, *History of the MI Division… Army General Staff: 1775 - 1941* (1986)

Posse Comitatus Act. Prohibits search, seizure, or arrest powers [by] US military personnel [in civilian law enforcement matters in the US unless authorized by legislation]. Amended in 1981 under Public Law 97-86 to permit increased DoD support of drug interdiction and other law enforcement activities [Title 18, USC § 1385]. (JP 1-02)

Posse Comitatus Act (PCA) places strict limits on the use of federal military personnel for law enforcement. Enacted in 1878, PCA prohibits the willful use of the US Army (and later, the US Air Force) to enforce laws, except as authorized by the Congress or the US Constitution. Although the PCA, by its terms, refers only to the Army and Air Force, DoD policy extends the prohibitions of the Act to the US Navy and Marine Corps, as well.

Specifically prohibited activities include: interdiction of a vehicle, vessel, aircraft, or similar activity; search and/or seizure; arrest, apprehension, "stop-and-frisk" detentions, and similar activities; and use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators. Additionally, federal courts have recognized exceptions to the PCA. These common law exceptions are known as the "military purpose doctrine" and the "indirect assistance" exceptions.

Exceptions and/or circumstances not falling under PCA include:
1) Actions that are taken for the primary purpose of furthering a military or foreign affairs function of the United States;
2) Federal troops acting pursuant to the President's Constitutional and statutory authority to respond to civil disorder;
3) Actions taken under express statutory authority to assist officials in executing the laws, subject to applicable limitations; and
4) Civil Disturbance operations authorized by statute.

The PCA does not apply to National Guard forces operating in state active duty or Title 32 USC status, nor to the USCG, which operates under Title 14 USC authority.

For an overview of the Posse Comitatus Act, see CRS Report R42659, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law* (16 Aug 2012), by Charles Doyle and Jennifer K. Elsea; copy available at: <http://www.fas.org/sgp/crs/natsec/R42659.pdf>

Also see Craig T. Trebilcock, *The Myth of Posse Comitatus*, October 2000; copy available at: < http://www.homelandsecurity.org/journal/articles/trebilcock.htm>

Also see DoDI 3025.21, *Defense Support of Civilian Law Enforcement Agencies*, 27 Feb 2013.

Preliminary Credibility Assessment Screening System (PCASS) Instrument. A diagnostic instrument used during an interview capable of monitoring, recording, and/or measuring electrodermal and vasomotor activity. The PCASS instrument uses an algorithm to evaluate the physiological responses recorded by the two components. (DoDI 5210.91, PCA Procedures, 12 Aug 2010 with change 1 dated 15 Oct 2013)

Only certified personnel may conduct PCASS examinations. Also IAW current DoD policy the PCASS will not be used to test U.S. persons.

Preliminary Inquiry. An unobtrusive review of the facts and circumstances of an incident or allegation to determine if the preliminary information or circumstances is sufficient to warrant the initiation of an investigation or referral to an investigative entity. The limited objective will be determined by the policy of individual agencies and may include the collection of information from other agencies and/or other records such as travel, financial, HR, security, and badgeing [sic], etc.; which may be used to make an informed determination if the incident involved is part of a pattern. (ONCIX Insider Threat Detection – Glossary) Also see *counterintelligence investigation*, *counterintelligence inquiry*, *investigation; preliminary counterintelligence investigation; Section 811 referral*.

Within DoD the proper term of use is *Counterintelligence Inquiry* or *CI Inquiry*; see DoDI O-5240.21, Counterintelligence Inquiries, 14 May 2009 with change 2 dated 15 Oct 2013.

Preliminary Investigation [counterintelligence related]. A limited scope inquiry into the circumstances surrounding a reported incident or matter of potential CI interest to determine if there are specific facts giving reason to believe that a threat to national security may exist or if a full field CI investigation is warranted. (AR 381-20, Army CI Program, 25 May 2010)

Preparation of the Environment (PE). An umbrella term for operations and activities conducted by selectively trained special operations forces to develop an environment for potential future special operations. (JP 3-05, Special Operations, 18 Apr 2011)

President's Daily Brief (PDB). An all-source, analytic document produced for the President of the United States and members of his/her Cabinet and senior staff. Production is overseen by the ODNI with contributions from the Intelligence Community.

Preventive Deployment. The deployment of military forces to deter violence at the interface or zone of potential conflict where tension is rising among parties. Forces may be employed in such a way that they are indistinguishable from a peace operations force in terms of equipment, force posture, and activities. (JP 3-07.3, Peace Operations, 17 Oct 2007)

Prisoner of War (POW or PW). A detained person (as defined in Articles 4 and 5 of the Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949) who, while engaged in combat under orders of his or her government, is captured by the armed forces of the enemy. (JP 1-02 and JP 3-50. Personnel Recovery, 20 Dec 2011)

Private Information. Data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization. (Army Techniques Publication 2-22.9, Open-Source Intelligence, 10 Jul 2012)

Private Sector. An umbrella term that may be applied in the United States and in foreign countries to any or all of the nonpublic or commercial individuals and businesses, specified nonprofit organizations, most of academia and other scholastic institutions, and selected nongovernmental organizations. (JP 3-57, Civil Military Operations, 8 Jul 2008)

Privacy Act. The Privacy Act of 1974 (5 U.S.C. 552a) establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by an individual's name or by some other identifier assigned to the individual. The Privacy Act requires that agencies provide public notice of their systems of records through publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a system of records absent the written consent of the individual who is the subject of the information search, unless the disclosure is pursuant to one of 12 statutory exceptions. The Privacy Act also provides individuals with a means by which to seek access to and amend their records and sets forth various agency record-keeping requirements. (ODNI, U.S. National Intelligence – An Overview 2011)

> For DoD policy see DoD Regulation 5400.11-R, DoD Privacy Act Program.
>
> The Privacy Act regulates the way certain types of information may be acquired and used by the Federal Government and provides certain rights to individuals whose information is acquired by the government.
>
> A 240-page overview of the Act can be found at: <http://www.justice.gov/opcl/1974privacyact.pdf>

Proactive TSCM. CI-focused TSCM targeting using a risk-based approach with the goal of identifying and exploiting technical collection efforts targeting DoD interests. (DoDI 5240.05, TSCM, 3 Apr 2014)

Probable Cause. Would a prudent individual believe that a fact is probably true. (Congressional Research Memorandum, Subject: Probable Cause, Reasonable Suspicion, and Reasonableness Standards in the Context of the Fourth Amendment and the Foreign Intelligence Surveillance Act, 30 Jan 2006; at <http://www.fas.org/sgp/crs/intel/m013006.pdf>) Also see *reasonable belief*.

-- Also, 1) To search: A reasonable belief that a crime has been committed and that the person, property, or evidence sought in connection with the crime is located in the place or on the person to be searched; and/or 2) To apprehend: A reasonable belief that a crime has been committed and that the person to be apprehended committed it. (AR 190-20, Military Police Investigations, 1 Nov 2005)

Probable Cause / Reasonable Belief

The facts and circumstances are such that a trained and experienced reasonable person would hold the belief.

- Fact Specific / Situation Dependant
- Must be based on facts and circumstances that can be articulated
- Can be based on experience, training and knowledge as it applies to the facts and circumstances
- "Hunches" and "intuitions" don't count
- Often requires education of non-intelligence personnel

-- Briefing, *Legal Fundamentals for Counterintelligence Professionals*, Staff Judge Advocate, US Army Intelligence and Security Command, nd. circa 2012

Probe. In information operations, any attempt to gather information about an automated information system or its on-line users. (JP 3-13, Information Operations, 13 Feb 2006) Also see *information operations*.

-- Also, [In computer usage / information operations] a technique that attempts to access a system to learn something about the system. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Processing. A system of operations designed to convert raw data into useful information. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Processing and Exploitation. In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Production. The preparation of reports based on analysis of information to meet the needs of intelligence users (Consumer's) within and outside the Intelligence Community. (CIA, *A Consumer's Guide to Intelligence*, July 1995) Also see *intelligence production*.

-- Also, conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of data from all available sources and the preparation of intelligence products in support of known or anticipated user requirements. (AR 381-20, Army CI Program, 25 May 2010)

Production results in the creation of intelligence, that is, value-added actionable information tailored to a specific customer. In government parlance, the term 'finished intelligence" is reserved for products issued by analysts responsible for synthesizing all available sources of intelligence, resulting in a comprehensive assessment of an issue or situation, for use by senior analysts or decision makers.

-- DIA, *Intelligence Essentials for Everyone*, June 1999

Production is the development of intelligence through the analysis of collected information and existing intelligence. Analysts create intelligence products, conclusions, or projections regarding threats and relevant aspects of the operational environment to answer known or anticipated requirements in an effective format.

-- ADRP 2-0, Intelligence, Aug 2012, p. 3-7

Production Requirement (PR). A customer's formal request for analytic support, identifying the topic or issue of interest, type of information or analysis required, date required, preferred format, and classification. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

-- Also, an intelligence requirement that cannot be met by current analytical products resulting in tasking to produce a new product that can meet this intelligence requirement. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Proliferation. The transfer of weapons of mass destruction, related materials, technology, and expertise from suppliers to hostile state or non-state actors. (JP 1-02 and JP 3-40, Combating WMD, 10 Jun 2009)

Program Protection Plan (PPP). A risk-based, comprehensive, living plan to protect CPI that is associated with an RDA program. (DoDI 5200.39, CPI Protection within the DoD, 16 Jul 2008 with change 1 dated 28 Dec 2010) Also see *counterintelligence support plan (CISP); critical program information (CPI)*.

Note: DoDI 5200.39 is under revision. A proposed *draft* definition for PPP: a risk-based, comprehensive, living plan to identify and protect CPI and mission-critical functions and components associated with an RDA program.

Program Protection is the integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle.

The **purpose of the PPP** is to help programs ensure that they adequately protect their technology, components, and information. The PPP is used to develop tailored protection guidance for dissemination and implementation throughout the program for which it is created. The layering and integration of the selected protection requirements documented in a PPP provide for the integration and synchronization of CPI protection activities throughout DoD.

Once a PPP is in place, it should guide program office security measures and updated as threats and vulnerabilities change or are better understood. Appendix B to the PPP is the **Counterintelligence Support Plan (CISP),** which should be cited/referenced here.

See "Program Protection Plan Outline & Guidance," Version 1.0, July 2011; copy available on line at: < http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf >

Prominent Individual. Someone who is widely known and has a favorable public reputation. (DoDD S-5200.37, Management & Execution of Defense HUMINT, 9 Feb 2009)

Propaganda. Any form of adversary communication, especially of a biased or misleading nature, designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. (JP 1-02 and JP 3-13.2, Psychological Operations, 7 Jan 2010)

Proprietaries. A term used… to designate ostensibly private commercial entities capable of doing business which are established and controlled by intelligence services to conceal governmental affiliation of intelligence personnel and/or governmental sponsorship of certain activities in support of clandestine operations. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Protection. The ability to prevent, mitigate adverse effects of attacks on personnel (combatant /non-combatant) and physical assets of the United States, allies, and friends. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

-- Also, preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Protective Service Detail. Trained and armed protective security officials capable of providing continuous protection for a designated individual. (DoDI 2000.12, DoD AT Program, 1 Mar 2012 w/ change 1 dated 9 Sep 2013)

Protective Intelligence (PI). CRIMINT [criminal intelligence] used to identify, analyze, and provide leads for investigation into various direct and indirect threats to DoD personnel and property. It may provide further details about persons who may have the interest, motive, intention, and capability of mounting attacks against the DoD and its personnel. Additionally, it can aid DoD LEAs in gauging the potential threat to and vulnerability of a targeted individual or property and may be used in determining or preventing violence. (DoDI 5525.18, Law Enforcement Criminal Intelligence in DoD 18 Oct 2013)

Protective Measures. Those actions, procedures, or designs implemented to safeguard protected information. (DSS Glossary)

Provocation. Activity designed to induce an individual, organization, intelligence service, or governments to take action damaging to itself. (FBI FCI Terms) Also see *dangle; double agent.*

-- Also, activity intended to cause an individual, organization, intelligence service, or government to take actions that can cause damage to itself. (Spy Book)

Provocation [aka *Dangle*]

"A *provocation* is an agent deployed by you to be recruited by an opponent and to perform his or her secret work *under your control* as a channel to and weapon against your opponent."

-- William R. Johnson, *Thwarting Enemies at Home and Abroad*, Georgetown University Press (2009), p.98

Prudent Risk. A deliberate exposure to potential injury or loss when the commander judges the outcome in terms of mission accomplishment as worth the cost. (ADRP 6-0, Mission Command, May 2012)

Pseudonym. A code name assigned to an individual, place, or activity to enhance operational, administrative, and communication security. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, an assigned identity that is used to protect an individual's true identity. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Psychological Operations (PSYOP). *Within DoD: None -- term rescinded.* See *Military Information Support Operations (MISO).*

Term changed to MISO IAW SECDEF Memo dated 3 Dec 2010.

Public Affairs (PA). Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. (JP 1-02 and JP 3-61, Public Affairs, 25 Aug 2010)

Public Diplomacy. 1). Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. 2). In peace building, civilian agency efforts to promote an understanding of the reconstruction efforts, rule of law, and civic responsibility through public affairs and international public diplomacy operations. Its objective is to promote and sustain consent for peace building both within the host nation and externally in the region and in the larger international community. (JP 1-02 and JP 3-07.3, Peace Operations, 17 Oct 2007)

Public Domain. In open view; before the public at large and not in private or employing secrecy or other protective measures. (DSS Glossary)

Public Information. Within public affairs, that information of a military nature, the dissemination of which is consistent with security and approved for release. (JP 1-02 and JP 3-61, Public Affairs, 25 Aug 2010)

Publicly Available Information. Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could lawfully be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any vent that is open to the public. (Attorney General Guidelines for National Security Investigations and Foreign Intelligence Collection, 31 Oct 2003)

--Also, data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public. (Army Techniques Publication 2-22.9, Open-Source Intelligence, 10 Jul 2012)

Q ==========

Questionable Intelligence Activity. An intelligence activity, as defined in EO 12333, that may be unlawful or contrary to E.O., Presidential directive, or applicable DoD policy governing that activity. (DoDD 5148.11, ATSD/IO, 24 Apr 2013) Also see *intelligence oversight*.

> DoD Policy: See DoD 5240 1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,* 7 Dec 1982.
>
> Also see DTM 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*, 17 Jun 2009 with chg 4 dated 21 Aug 2013; copy at <http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-052.pdf>

Quit Claim. A document in which an asset acknowledges that all commitments due have been met by the handler's organization. (HDI Lexicon, April 2008)

R ==========

Rabbit. [Tradecraft jargon] The target in a surveillance operation. (CI Centre Glossary)

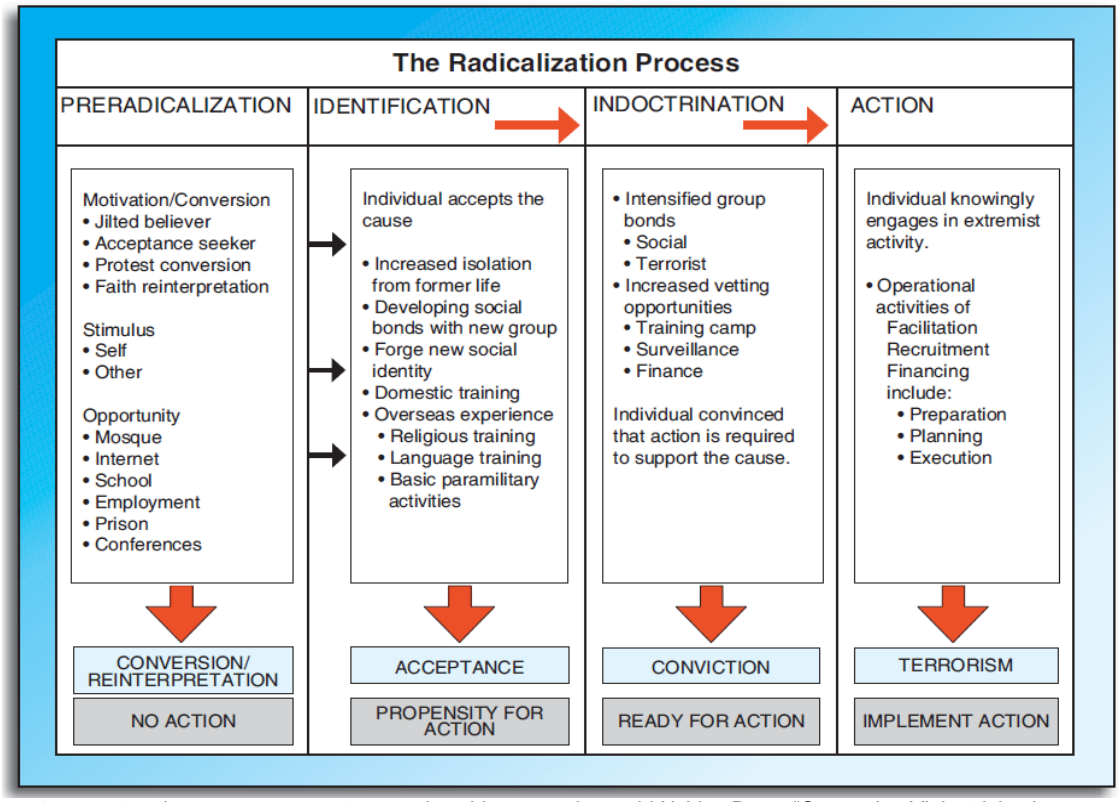
Radiogram. Coded bursts of data sent by a radio transmitter that can be picked up by a radio receiver that has been set to the proper frequency; as transmitted, radiograms generally sound like the transmission of Morse code. (FBI Affidavit, 25 June 2010)

Radicalization. The process of acquiring and holding radical or extremist beliefs. (Congressional Research Service Report R42553, *Countering Violent Extremism in the United States,* 19 Feb 2014) Also see *self-radicalization*; *violent extremism, violent radicalization*.

-- Also, the social and behavioral process whereby people adopt and embrace extremist attitudes, values or behaviors. It is a risk factor for involvement in terrorism, but involvement in terrorism does not always result from radicalization. JP1-02 does not include a definition for radicalization. (Defense Science Board Report, *Predicting Violent Behavior*, Aug 2012, citing Horgan's *The Psychology of Terrorism 2nd Edition*, 2012)

Radicalization Process

The FBI model describes the radicalization process – the "way stations" – as four incremental stages of development: 1) Preradicalization, 2) Identification, 3) Indoctrination, and 4) Action. Each one is distinct, and a radicalized individual may never reach the final stage.
See chart—*The Radicalization Process*—below…



Source: Carol Dyer, Ryan E. McCoy, Joel Rodriguez, and Donald N. Van Duyn, "Countering Violent Islamic Extremism: A Community Responsibility, *FBI Law Enforcement Bulletin*, Vol 76, No 12, Dec 2007*

* Copy available at <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2007-pdfs/dec07leb.pdf>

-- Also, the process by which an individual, group, or mass of people undergoes a transformation from participating in the political process via legal means to the use or support of violence for political purposes. (Army Tactical Reference Guide, Radicalization into Violent Extremism – A Guide for Military Leaders, April 2011

The growth in social media and the terrorist use of chat rooms, Facebook, Twitter, YouTube, and other sites has facilitated radicalization inside the United States.

-- Seth G. Jones, The RAND Corporation, "The Extremist Threat to the U.S. Homeland," Testimony Before the Committee on Homeland Security United States House of Representatives, 15 January2014 (This testimony available at <http://www.rand.org/pubs/testimonies/CT403.html>)

There is no easily identifiable terrorist-prone personality, no single path to radicalization and terrorism. Many people may share the same views, and only a handful of the radicals will go further to become terrorists. The transition from radical to terrorist is often a matter of happenstance. It depends on whom one meets and probably on when that meeting occurs in the arc of one's life.

-- Brian M. Jenkins*

* Brian Michael Jenkins, *Would Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001* (Santa Monica, CA: The RAND Corporation, 2010), p. 7.

Studies by the Department of Homeland Security's Office of Intelligence and Analysis indicate that the radicalization dynamic varies across ideological and ethno-religious spectrums, different geographic regions, and socio-economic conditions. Moreover, there are many diverse "pathways" to radicalization and individuals and groups can radicalize or "de-radicalize" because of a variety of factors.

-- U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, Written Testimony of Charles E. Allen, Assistant Secretary of Intelligence and Analysis and Chief Intelligence Officer, Department of Homeland Security, "Threat of Islamic Radicalization to the Homeland," 110th Cong., 1st sess., March 14, 2007, p. 5.

Also see US Army Asymmetric Warfare Group, Tactical Reference Guide, *Radicalization into Violent Extremism, A Guide for Military Leaders, August 2011*—copy available at: <http://www.wired.com/images_blogs/dangerroom/2012/10/Radicalization-FINAL090911.pdf>

Raid. An operation to temporarily seize an area in order to secure information, confuse an adversary, capture personnel or equipment, or to destroy a capability culminating with a planned withdrawal. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Rapport Building. Establishing a sense of connection between the interviewer and the interviewee to facilitate communication and information sharing. (Keats, 1993)

Raw Data. Bits of collected data that individually convey little or no useful information and must be collated, aggregated, or interpreted to provide meaningful information. (ODNI, U.S. National Intelligence – An Overview 2011)

Raw Intelligence. A colloquial term meaning collected intelligence information that has not yet been converted into finished intelligence. (ODNI, U.S. National Intelligence – An Overview 2011)

Reachback. The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 1-02 and JP 3-30, Command and Control for Joint Air Operations, 12 Jan 2010)

Reactive Operation. An operation initiated in response to a FIS personal contact. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Real Time. Pertaining to the timeliness of data or information which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays. (Previously in JP 2-0, Joint Intelligence) Also see *near real time*.

Reasonable Belief. A reasonable belief arises when the fact and circumstances are such that a reasonable person would hold the belief. Reasonable belief must rest on the facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. Reasonable belief can be based on experience, training, and knowledge in foreign intelligence or counterintelligence work applied to facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not. (DoD 5240.1-R, December 1982) Also see *probable cause*; *reasonable suspicion.*

Reasonable Expectation of Privacy. In U.S. constitutional law the expectation of privacy is a legal test which is crucial in defining the scope of the applicability of the privacy protections of the Fourth Amendment to the United States Constitution.

> The extent to which a reasonable person in the particular circumstances involved is entitled to believe his or her actions are not subject to outside observations. Must be both objectively and subjectively reasonable [as well as] very fact specific. (SJA Office, USAINSCOM)
>
> _____
>
> As a general matter the Supreme Court has held that there may be circumstances in which a government employee has a legitimate expectation of privacy in the contents of governmental property that the employee uses or controls at work, such as an office or a locked desk drawer. See: O'Connor, 480 U.S. at 716-19 (1987) (plurality) (public employee has a reasonable expectation of privacy in personal items, papers, and effects in office, desk, and file cabinets provided by public employer); see id. at 730-31 (Scalia, J., concurring) (government employee has a legitimate expectation of privacy in the contents of his office).
>
> Instead, whether, in a particular circumstance, a government employee has a legitimate expectation of privacy in his use of governmental property at work is determined by "[t]he operational realities of the workplace" and "by virtue of actual office practices and procedures, or by legitimate regulation." See: O'Connor, 480 U.S. at 717 (plurality); see United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) ("[O]ffice practices, procedures, or regulations may reduce legitimate privacy expectations.").

Reasonable Suspicion. Specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch of criminal activity. (United States v. Mason, 628 F.3d 123, 128 – 4th Cir. 2010 [quoting United States v. Branch, 537 F.3d 328, 336 – 4th Cir. 2008])

Recognition Signal. Any prearranged signal by which individuals or units may identify each other. (JP 1-02 and JP 3-50. Personnel Recovery, 20 Dec 2011)

-- Also, prearranged visual indicator used for recognition and identification between intelligence personnel. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, prearranged visual signal used by intelligence personnel to identify each other. (FBI FCI Terms)

Reconnaissance (RECON). A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Records Check. The process whereby a Special Agent obtains relevant information about Sources or Subjects from the records and information holdings of military, civilian or government agencies, as well as certain commercial companies and vendors, during the conduct of an investigation or operation. Types include military agency checks (MACs), local agency checks (LACs) and national agency checks (NACs).

-- *Military Agency Check* (MAC): a records or files check conducted at any military agency within the jurisdiction of the CI element conducting the check.

-- *Local Agency Check* (LAC): a records or files check of official or publically available information retained by any local office or government agency within the jurisdiction of the CI element conducting the check. Records may include holdings and databases maintained by local and state law enforcement agencies, local courts, local offices of federal agencies, etc.

-- *National Agency Check* (NAC): formal requests to federal agencies for searches of their records and supporting databases and files for information of investigative or operational interest. NACs include DoD agencies, as well as other federal agency holdings, e.g., FBI, CIA, DHS, ICE, IRS, OPM, State Department, FINCEN, etc.

Recovery Operations. Operations conducted to search for, locate, identify, recover, and return isolated personnel, human remains, sensitive equipment, or items critical to national security. (JP 1-02 and JP 3-50, Personnel Recovery, 5 Jan 2007)

Recruitment. The deliberate and calculating effort to gain control of an individual and to induce him or her to furnish information or to carry out intelligence tasks for an intelligence or CI service. (DoDI S-5240.17, CI Collection Activities, 14 Mar 2014)

-- Also, authorized personnel establishing control over an foreign individual who, witting or unwitting of USG involvement, accepts tasking as a result of the established relationship; authorized personnel establishing control over a U.S. person who, fully aware of USG involvement, accepts tasking as a result of the established relationship. (DoDI S-5200.42, Defense HUMINT and Related Activities (U), 8 Dec 2009 w/ chg 1 dated 16 Aug 2010)

-- Also, the acquisition of an individual's services who, witting or unwitting of U.S. Government involvement, accepts directions and control thus obligating both parties to an act in a prescribed manner. (HDI Lexicon, April 2008)

-- Also, the establishment of a degree of control over an individual who, witting or unwitting of U.S. Government involvement accepts tasking as a result of the relationship established. (Army TC 2-22.307, Aug 2009)

-- Also, the process of enlisting an individual to work for an intelligence or counterintelligence service. (FBI FCI Terms)

-- Also, term for the tradecraft process of enlisting a target individual to work for an intelligence or security service. (*The CIA Insider's Dictionary*, by Leo D. Carl, 1996)

-- Also, the tradecraft process of enlisting a target individual to work for an intelligence service—in most cases against his own country. The process includes spotting, assessing, developing, and recruitment. Motivation may be ideological, financial, or other, such as revenge. (A Spy's Journey)

Recruitment… is a process of salesmanship, almost of seduction.
-- SSCI Report 99-522 (1986)

Agent recruiting is the most important task of both strategic and operational intelligence. No real problems can be solved without agent penetration in basic government, military and technological centres of the enemy.

-- Victor Suvorov, *Inside Soviet Military Intelligence* (1984); see Chapter 4 - Agent Recruiting.

Agent recruitment is a tedious process with a low rate of success and a high rate of return. Of every ten agents recruited, eight will fall by the wayside because they lose their access or they tire of the commitment, one will be a problem—mainly of security—and one will work as a productive agent, perhaps for decades.

-- Joseph W. Wippl (35 year CIA career with the National Clandestine Service), "The Qualities That Make a Great Case Officer," *International Journal of Intelligence and Counterintelligence*, Vol 25 No 3 (Fall 2012), p. 602

Recruitment… is an art form

How do you do recruitment? *"How do you sell anything in life? You have to have a product, you have to develop a relationship, and in that relationship you have to be able to identify people's strengths and weaknesses. And then you have to be able to ask that tough question: Will you help me? There is a sense of timing in it. It's an art form, very frankly."*

-- Jack Devine, 32-year CIA veteran in "Ten Questions," *Time* Magazine, Vol. 183 No. 23, 16 June 2014. p. 60

Recruitment Cycle. The… process by which intelligence services recruit agents (aka the agent acquisition process). (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

"The recruitment cycle is the essence of spying"

Seven steps of the recruitment cycle: 1) Spotting; 2) Assessing; 3) Developing; 4) Pitching; 5) Formalizing; 6) Producing; and 7) Terminating.

-- James M. Olson (CIA Retired), Former Chief CIA Counterintelligence

-- Also, *Agent Recruitment Cycle* (ARC): the systematic method for acquiring agents HUMINT sources) who will satisfy intelligence collection requirements and meet intelligence needs.

*The **Agent Recruitment Cycle** consists of six steps:*

+ *Spotting (or identifying) individuals who can meet intelligence needs as identified by analyst or policymakers.*
+ *Assessing whether the spotted individuals have the placement and access to provide the desired information as well as beginning the process of determining their motivations, vulnerabilities, and suitability.*
+ *Developing a relationship with the individual to further assess the factors above and to explore whether they will be responsive to initial tasking for intelligence information.*
+ *The actual recruitment.*
+ *Training and handling meetings with the agent, including taskings and debriefings.*
+ *Either turning an agent over to another case officer or terminating the relationship.*

-- Randy Burkett, "An Alternative Framework for Agent Recruitment: From MICE to RASCALS," *Studies in Intelligence*, Vol 57, No 1 (March 2013), p. 55

Seven basic areas: 1) Spotting; 2) Evaluation; 3) Recruiting; 4) Testing; 5) Training; 6) Handling; and 7) Termination.

+ *Spotting: the process of identifying foreigners or other persons who might be willing to spy…*
+ *Evaluation: a thorough review of all information available…*
+ *Recruiting: the recruitment "pitch".… People volunteer or agree to spy on their governments for many reasons. It is the task of the recruiter to determine what reason—if one exists—is most likely to motivate the potential agent.*
+ *Testing: [testing the asset's] loyalty and reliability …*

+ Training: [tradecraft training] instructed in one of several methods of covert communications… learn the use of clandestine contacts. And… will be given training on security precautions, such as the detection and avoidance of surveillance.
+ Handling: Successful handling of an agent hinges on the strength of the relationship that the case officer is able to establish with the agent. ….a good case officer must combine the qualities of a master spy, a psychiatrist, and a father confessor. …One of the biggest problems in handling an agent is caused by the changeover of case officers.
+ Termination: All clandestine operations ultimately come to an end. …[need for] resettlement

-- Victor Marchetti and John D. Marks, *The CIA and the Cult of Intelligence*, 2nd Edition (1980), pp 215-228

Agent recruitment [cycle]: 1) Spot; 2) Assess; 3) Develop & Recruit; 4) Test; 5) Train; 6) Handle; and 7) Terminate.

-- Jefferson Mack, *Running a Ring of Spies* (1996)

Recruitment-in-Place (RIP). An official who overtly continues to work for his government and clandestinely provides information of intelligence value to a foreign government; will in many instances be connected with a foreign government's intelligence service. (CI Community Lexicon) Also see *penetration; penetration operation*.

-- Also, a person who agrees to become an agent and retain his position in his organization or government while reporting on it to an intelligence or security organization of a foreign country. (ICS Glossary)

-- Also, inducement of a person to become an informant or agent of an intelligence service while he or she remains in the same position and status. This term applies to personnel of foreign establishments, diplomatic or other, who continue to occupy their regular posts instead of defecting. (AFOSI Instruction 71-101, 6 Jun 2000)

-- Also, a foreign national who overtly continues to work for his government and covertly provides the U.S. with information of intelligence value. (FBI FCI Terms)

Recruitment-in-place, one of the most difficult and sensitive activities in counterintelligence.

-- William H. Webster, Director FBI, Speech on 22 March 1986

Recruiting anybody to be a spy is an act of seduction. Recruiting hostile intelligence officers amounts to seducing seducers—an art in itself.

-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), p. 337

A recruitment who stays on the job… is the ultimate prize, the crown jewel of any counterintelligence operation. At great personal risk, a recruitment in place is in a position to provide continuous and up-to-date information. By contrast, a defector, while usually welcome, is of less value. Once debriefed of the information he or she knows, and with no further access to secrets, a defector has diminished worth.

-- David Wise, *Tiger Trap: America's Secret Spy War with China* (2011), p. 177

It is axiomatic in intelligence work that 'there is no better counterintelligence than recruiting the other side's intelligence officers.'

-- James M. Olson (CIA Retired), Former Chief CIA Counterintelligence

Reconstitution. The process of restoring critical assets and their necessary infrastructure support systems (or their functionality) to pre-incident operational status. (DoDI 3020.45, DCIP Management, 21 Apr 2008)

RED. In cryptographic systems, refers to information or messages that contain sensitive or classified information that is not encrypted. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) Also see *BLACK*.

RED EYE. The RED EYE Task Force, hosted by AFMC [Air Force Material Command] and sponsored by Region 1 [AFOSI] is a multi-agency operation consisting of nine federal law enforcement and intelligence agencies working together to identify, exploit, neutralize and mitigate threats of illicit procurement and illegal export of sensitive U.S. technology to foreign adversaries. (AFOSI 2012 Fact Book)

Red Team. An organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *red team analysis*.

> A "CI Red Team" is a simulation of a foreign intelligence collection activities of a specified friendly/Blue target, such as a RDA project/program, installation, military operation, etc. May include the identification of physical, electronic, acoustic, or visual patterns of the supported activity/agency as may be seen through the eyes of ad adversary.

Red Team Analysis. Models the behavior of an individual or group by trying to replicate how an adversary would think about an issue. (CIA, *A Tradecraft Primer: Structured Analytical Techniques for Improving Intelligence Analysis*, June 2005) Also see *red team*.

> Red Team analysis tries to consciously place the analyst in the same cultural, organizational, and personal setting -- "putting them in their shoes" -- in which the target individual or group operates. Red Team analysis is not easy to conduct. It requires significant time to develop a team of qualified experts who can think like the adversary.
>
> ***Contrarian methods and "Red Teams" should be a routine part of the analytical process.***
> -- Jeffrey R, Cooper, *Curing Analytical Pathologies*, Center for the Study of Intelligence (Dec 2005), p. 43

Redaction. For purposes of declassification, the removal of exempted information from copies of a document. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012)

Refugee. A person who owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his or her nationality and is unable or, owing to such fear, is unwilling to avail himself or herself of the protection of that country. See also *dislocated civilian; displaced person; evacuee; expellee; stateless person*. (JP 1-02 and JP 3-29, Foreign Humanitarian Assistance, 17 Mar 2009)

Regional Security Officer (RSO). A security officer responsible to the chief of mission (ambassador), for security functions of all US embassies and consulates in a given country or group of adjacent countries. (JP 1-02 and JP 3-10, Joint Security Operations in Theater, 3 Feb 2010)

-- Also, Diplomatic Security Special Agents of the U.S. Department of State (DoS), assigned to U.S. diplomatic missions overseas as the personal advisor to the ambassador or chief of mission on all security issues and coordinate all aspects of a mission's security program. They develop and implement effective security programs to protect DoS employees from terrorist, criminal, and technical attack both at work and at home. The RSO serves as the primary liaison with foreign police and security services overseas in an effort to obtain support for U.S. law enforcement initiatives and investigations. (DoS)

> See Department of State website at: <http://www.state.gov/m/ds/protection/c8756.htm>

Reid Technique. A method of questioning subjects and assessing their credibility. The technique consists of a non-accusatory interview combining both investigative and behavior-provoking questions. If the investigative information indicates that the subject committed the crime in question, the *Reid Nine Steps of Interrogation* are utilized to persuade the subject to tell the truth about what they did. The Reid technique involves three different components — factual analysis, interviewing, and interrogation. (Wikipedia; accessed 21 Aug 2013)

> The term *"Reid Technique"* is a registered trademark of the firm John E. Reid and Associates, which offers training courses in the method they have devised. The technique is widely used by numerous law-enforcement agencies. For more information see: <http://www.reid.com/>

Remediation. Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, the act of mitigating a vulnerability or a threat. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Rendition. An extra-territorial activity to apprehend and return a person to the US or another country, with or without permission from the country in which the subject is apprehended. (National HUMINT Glossary)

> *The term "rendition" in the counterterrorism context means nothing more than moving someone from one country to another, outside the formal process of extradition.*
>
> -- Daniel Benjamin, Former Director for Counterterrorism, National Security Council
>
> ---
>
> For additional information see CRS Report (RL32890) *Renditions: Constraints Imposed by Laws on Torture,* 8 Sep 2009; copy available at: <http://www.fas.org/sgp/crs/natsec/RL32890.pdf>

Repatriate. A person who returns to his or her country or citizenship, having left said native country either against his or her will, or as one of a group who left for reason of politics, religion, or other pertinent reasons. (JP 1-02)

Repatriation. 1) The procedure whereby American citizens and their families are officially processed back into the United States subsequent to an evacuation. (JP 3-68, Noncombatant Evacuation Operations, 23 Dec 2010); and 2) The release and return of enemy prisoners of war to their own country in accordance with the 1949 Geneva Convention Relative to the Treatment of Prisoners of War. (JP 1-0, Personnel Support to Joint Operations, 16 Oct 2006)

Report of Investigation (ROI). An executive summary of all results of investigative activity conducted in an investigation. (902d MIG Investigations Handbook, updated 17 Oct 2012) .

Reportable Incident. Any suspected or alleged violation of Department of Defense policy or of other related orders, policies, procedures or applicable law, for which there is credible information. (JP 1-02 and JP 3-63, Detainee Operations, 30 May 2008)

Request For Assistance (RFA). A request based on mission requirements and expressed in terms of desired outcome, formally asking for assistance.

Request For Information (RFI). 1) Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. 2) A term used by the National Security Agency/Central Security Service to state ad hoc signals intelligence requirements. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Research, Development, and Acquisition (RDA). All activities associated with research and engineering, acquisition, international transfers of technology, and disposal of defense-related technology. (DoDI O-5240.24,CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013)

Residency. An office or location in a country used by foreign intelligence officers from which to plan, coordinate, and execute intelligence activities. Also refers to the number of foreign intelligence agents present in a given area. (AR 381-20, Army CI Program, 25 May 2010)

Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (PPD-21, 2013)

Resiliency. The characteristic or capability to maintain functionality and structure (or degrade gracefully) in the face of internal and external change. (DoDI 3020.45, DCIP Management, 21 Apr 2008)

Resistance Movement. An organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability. (JP 1-02 and JP 3-05, Special Operations, 18 Apr 2011)

Responsible Analytical Center (RAC). The Intelligence organization that has responsibility for providing integrated all-source analysis, or application of analysis, to produce an intelligence product to answer a specific COCOM Intelligence Task List (ITL) task or sub-task. DoD organizations that qualify as RACs include: DIA analytical offices [including DAC-1C] and Intelligence Centers, the COCOM Joint Intelligence Operations Centers (JIOCs), and the Service intelligence production centers (MCIA, NASIC, NGIC, and ONI). (CJCSM 3314.01, Intelligence Planning, 28 Feb 2007)

Restraint. In the context of joint operation planning, a requirement placed on the command by a higher command that prohibits an action, this restricting freedom of action. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Restricted Area. An area (land, sea or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation/activity commander/director, properly posted, and shall employ physical security measures. Additionally, Controlled Areas may be established adjacent to Restricted Areas for verification and authentication of personnel. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, 1) An area (land, sea, or air) in which there are special restrictive measures employed to prevent or minimize interference between friendly forces; and 2) An area under military jurisdiction in which special security measures are employed to prevent unauthorized entry. (JP 1-02)

Restricted Target. A valid target that has specific restrictions placed on actions authorized against it due to operational considerations. Also see *restricted target list*. (JP 3-60, Joint Targeting, 13 Apr 2007)

Restricted Target List (RTL). A list of restricted targets nominated by elements of the joint force and approved by the joint force commander. This list also includes restricted targets directed by higher authorities. Also see *restricted target*. (JP 3-60, Joint Targeting, 13 Apr 2007)

Returnee. A displaced person who has returned voluntarily to his or her former place of residence. (JP 3-29, Foreign Humanitarian Assistance, 17 Mar 2009)

Revolution. The overthrow or renunciation of one government or ruler and the substitution of another by the governed. (Army FM 3-24-2, Tactics in Counterinsurgency, April 2009)

Risk. Probability and severity of loss linked to threats or hazards and vulnerabilities. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, probability and severity of loss linked to hazards (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

-- Also, a measure of consequence of peril, hazard or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability). (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, a measure of the potential degree to which protected information is subject to loss through adversary exploitation. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (DHS, National Infrastructure Protection Plan - 2009)

When you hear "calculated risk," don't ask to see the calculations.

-- Dr. Gus Weiss, Former Assistant Secretary of Defense for Space Policy
(quoted in *Intelligence Analysis: A Target-Centric Approach*)

Risk, in the context of critical infrastructure and terrorism, can be defined as the potential consequence associated with a particular kind of attack or event against a particular target, discounted by the likelihood that such an attack or event will occur (threat) and the likelihood that the target will sustain a certain degree of damage (vulnerability).

Threat includes not only the identification of specific adversaries, but also their intentions and capabilities (both current and future). Consequences include lives and property lost, short term financial costs, longer term economic costs, environmental costs, etc.

Given this definition, risk is not threat, nor vulnerability to a threat, nor the estimated consequences associated with a specific attack, but some integration of the three.

-- CRS Report, RL30153, 8 Jan 2007

Risk Avoidance. A security philosophy which postulates that adversaries are all-knowing and highly competent, against which risks are avoided by maximizing defenses and minimizing vulnerabilities. (DSS Glossary) Also see *risk management*.

Risk Analysis. A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios in order to determine the likelihood of compromise of critical information. (DSS Glossary)

-- Also, examination of information to identify the risk to an information system. See risk assessment. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Risk Assessment. A systematic examination of risk using disciplined processes, methods, and tools. A risk assessment provides an environment for decision makers to evaluate and prioritize risks continuously and to recommend strategies to remediate or mitigate those risks. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, the identification and assessment of hazards (first two steps of risk management process). (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

-- Also, a process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, a defined process used to fuse the procedures of analyzing threat, risks, and vulnerabilities, into a cohesive, actionable product. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, the process of evaluating security risks based on analyses of threats, vulnerabilities, and probable adverse consequences to a facility, system, or operation. (IC Standard 700-1, 4 Apr 2008)

Risk Assessment

The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).

-- CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010

Risk Management (RM). The process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

*The basic concept for a cost effective security system is **risk management** rather than the unattainable and unaffordable goal of risk avoidance.*

-- Joint Security Commission II Report, 24 August 1999, p.12

-- Also, a process by which decision makers accept, reduce, or offset risk and subsequently make decisions that weigh overall risk against mission benefits. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, process and resultant risk of systematically identifying, assessing and controlling risks. Commanders/Directors are required to identify critical assets and their subsequent protection requirements, including future expenditures required for the protection requirements. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, the process of selecting and implementing security countermeasures to accept or mitigate the risk of a known or suspected threat to an acceptable level based on cost and effectiveness. (IC Standard 700-1, 4 Apr 2008)

-- Also, *Antiterrorism (AT) Risk Management*: the process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance possible adverse outcomes with mission benefits. AT risk management is one of the five minimum elements of an AT program. The end products of the AT program risk management process shall be the identification of DoD elements and personnel that are vulnerable to the identified threat attack means. From the assessment of risk based upon the three critical components of AT risk management (threat assessment, criticality assessment, and vulnerability assessment), the commander or DoD civilian manager must determine which DoD elements and personnel are at greatest risk and how best to employ given resources and FP measures to deter, mitigate, or prepare for a terrorist incident. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013)

Risk Mitigation. Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/ countermeasures recommended from the risk management process. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Risk Response. Actions taken to remediate or mitigate risk, or to reconstitute capability in the event of loss or degradation. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Romeo Spies. Men whose task is to seduce women who have access to confidential material, in the hope that through pillow talk the women will reveal secrets. (Encyclopedia of Cold War Espionage, Spies, and Secret Operations, 3rd revised edition 2012)

Rolling Car Pickup. A clandestine car pickup executed so smoothly that the car hardly stops at all and seems to have kept moving forward. (CI Centre Glossary) Also see *car pick-up*.

Rule of the Least Intrusive Means. The collection of information by a DoD intelligence component must be accomplished by the **least intrusive means** or lawful investigative technique reasonably available. (DIA Intelligence Law Handbook, Sep 1995)

> This rule prescribes a hierarchy of collection techniques which must be considered before an intelligence component engages in collection of information about US persons. The methodologies below become progressively more intrusive as one proceeds through this hierarchical framework:
>
> -- First, to the extent feasible, information must be collected from publically available materials, or with the consent of the person or persons concerned.
>
> -- Second, if collection from these sources is not feasible, then cooperating sources may be used.
>
> -- Third, if neither publically available information nor cooperating sources are sufficient or feasible, and then collection may be pursued using other lawful investigative techniques that require neither a judicial warrant nor the approval of the Attorney General of the United States.
>
> -- Finally, when none of the first three approaches has been sufficient or feasible, then the collecting intelligence component may seek approval for use of one of the techniques that require a warrant or approval of the Attorney General.
>
> DoD Policy: see DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, 7 Dec 1982 (para C2.4.2, page 18).

Rules of Engagement (ROE). Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. (JP 1-02 and JP 1-04, Legal Support to Military Operations, 17 Aug 2011)

Ruse. In military deception, a trick of war designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary's intelligence collection system. (JP 1-02 and JP 3-13.4, Military Deception, 13 Jul 2006)

S ==========

Sabotage. An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, the willful destruction of government property with the intent to cause injury, destruction, or defective production of national defense or war materials by either an act of commission or omission. (IC Standard 700-1, 4 Apr 2008)

Sabotage is a violation of Title 18 USC, §§ 2151-2156.

———————————

[S]abotage is the destruction of material by covert means in order to destroy the capability of a country to pursue its policies.

-- Tucker, David. *Illuminating the Dark Arts of War*, New York: Continuum International Publishing Group, 2012, p. 136

Safe House. An innocent-appearing house or premises established by an organization for the purpose of conducting clandestine or covert activity in relative security. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

-- Also, a facility use to afford security for operations. (HDI Lexicon, April 2008)

-- Also, house or premises controlled by an intelligence service that affords at least temporary security for individuals engaged in intelligence operations. (CI Community Lexicon)

-- Also, any house, apartment, office, or other building or quarters used to afford security for persons engaged in clandestine activities or for intelligence collection purposes. Safe houses may be used as refuge for or holding of agents or defectors; lodging and feeding of couriers, escapees, or evaders; lodging and working space for agents; rendezvous training, briefing, or questioning; or storage of supplies and equipment. (National HUMINT Glossary)

-- Also, a location controlled by an intelligence service that provides a secure place for individuals engaged in intelligence operations to meet. (FBI FCI Terms)

-- Also, a secure facility, unknown to adversary intelligence and security services, used for agent meetings, defector housing or debriefing, and similar support functions. (CIA in D&D Lexicon, 1 May 2002)

-- Also, [safehouse] a secure location used by intelligence services to meet with agents or for other clandestine purposes. The renter or purchaser of a safehouse is usually a cutout, someone who has no visible connection with intelligence work or with any official organization. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

-- Also, [safehouse] a sterile location, normally a house or apartment—but could be a hotel room as well—used to meet agents securely. (A Spy's Journey)

Safeguarding. Measures and controls that are prescribed to protect classified information. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012)

Sanction Enforcement. Operations that employ coercive measures to control the movement of certain types of designated items into or out of a nation or specified area. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Sanitization. The editing of intelligence to protect sources, methods, capabilities, and analytical procedures to permit wider dissemination (IC Standard 700-1, 4 Apr 2008)

Sanitize. To revise a report or other document in such a fashion as to prevent identification of sources, or of the actual persons and places with which it is concerned, or of the means by which it was acquired. Usually involves deletion or substitution of names and other key details. (JP 1-02)

Sanitizing. The removal of information from the media or equipment such that data recovery using any known technique or analysis is prevented. Sanitizing shall include the removal of data from the media, as well as the removal of all classified labels, markings, and activity logs. Properly sanitized media may be subsequently declassified upon observing the organization's respective verification and review procedures. (DSS Glossary)

Satellite Reconnaissance Advanced Notice (SATRAN) Program. Advanced warning of reconnaissance satellite orbits so military commanders can take appropriate action. (Center for Army Lessons Learned, http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=26671, accessed 4 Mar 2014)

> *In response to the intelligence threat from Soviet imagery satellites, the United States initiated the Satellite Reconnaissance Advanced Notice (SATRAN) program… in 1966.*
>
> -- Jeffrey T. Richelson, *The US Intelligence Community* (2012, Sixth Edition), pp. 270-271

> *The mission of the SATRAN Program is to provide the US military, US Government agencies… with warning of periods where their equipment or activities are vulnerable to reconnaissance by foreign spacecraft. The SATRAN program provides accurate overflight information in a timely manner so that foreign spacecraft are denied the opportunity to collect useful intelligence data.*
>
> -- Intellipedia (accessed 4 Mar 2014)

SATRAN. Acronym, see *Satellite Reconnaissance Advanced Notice Program* above.

Scams. [Cyber usage] Fake deals that trick people into providing money, information, or service in exchange for the deal. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

Scattered Castles. The IC [Intelligence Community] security clearance repository and the Director of National Intelligence's authoritative source for clearance and access information for all IC, military services, DoD civilians, and contractor personnel. DoD information is furnished by JPAS. (IC Standard 700-1, 4 Apr 2008)

Scientific and Technical Intelligence (S&TI). The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information that covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development related thereto; and the production methods employed for their manufacture. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Scientific Method. [One of the four basic types of reasoning applied to intelligence analysis, it] combines deductive and inductive reasoning: induction is used to develop the hypothesis, and deduction is used to test it. (DIA, *Intelligence Essentials for Everyone*, June 1999) Also see *abduction; deduction; induction.*

> For additional information see *Knowledge Management in the Intelligence Enterprise* by Edward Waltz (2003).

Screening. In intelligence, [the] evaluation of an individual; or a group of individuals to determine their potential to answer collection requirements or to identify individuals who match a predetermined source profile coupled with the process of identifying and assessing the areas of knowledge, cooperation, and possible approach techniques for an individual who has information of intelligence value. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> For additional information see Chapter 6 "Screening," FM 2-22.3, *Human Intelligence Collection Operations*.

SCRM. See *Supply Chain Risk Management*.

Search. An examination, authorized by law, of a specific person, property, or area for specified property or evidence, or for a specific person for the purpose of seizing such property, evidence, or person. (AR 190-20) Also see *physical search*, *search warrant*, *seizure*.

Search Warrant. An express authorization to search and seize issued by competent civilian authority. (AR 190-20) Also see *search, seizure*.

> A search warrant is a court order authorizing law enforcement to search a specified location and seize evidence. Under the Fourth Amendment, searches must be reasonable and specific.
>
> The Fourth Amendment prohibits unreasonable searches and seizures (U.S. Constitution. Amendment. IV). Searches and seizures are presumptively unreasonable, unless they are conducted pursuant to a warrant issued by a neutral magistrate upon a sworn showing of probable cause (*Terry v. Ohio*, 393 U.S. 1, 20, 1968).

Sector-Specific Agency. Federal departments and agencies identified in Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," 7 December 2003 as responsible for CI/KR [critical infrastructure and/or key resource] protection activities in specified national CI/KR sectors. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, a Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (PPD-21, 2013)

> PDD 21 identifies 16 critical infrastructure sectors and designates associated Federal SSAs. For the critical infrastructure sector "Defense Industrial Base" the Department of Defense is the designated SSA by PDD 21.

Secret, Security classification that shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe. (EO 13526) Also see *security classification*.

SECRET Internet Protocol Router Network (SIPRNet). The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010)

Secret Writing (SW). Invisible writing. (FBI FCI Terms)

-- Also, any tradecraft technique employing invisible messages hidden in or on innocuous materials. This includes invisible inks and microdots, among many other variations. (CI Centre Glossary)

-- Also, tradecraft term that describes the act of using special inks or special carbons papers (impregnated with chemicals) to write messages clandestinely. The utilization of special inks is known as the "wet system." The utilization of special carbon papers is known as the "dry system." (*Encyclopedia of the CIA*, 2003]

The simplest secret writing uses organic inks: milk, vinegar, lemon juice, even urine. These inks dry invisibly and can be developed by applying heat. Espionage agencies have produced many inks made of chemicals that could be developed only by a specific chemical.

-- Spy Book

The chief difficulty with secret inks was their inability to handle great volume of information that spies had to transmit in a modern war.

-- David Kahn, *The Codebreakers* (1967)

The techniques of secret writing are the same the world over. First the spy writes his cover letter. Then he writes the secret message on top, using a special sheet of carbon paper treated with a colorless chemical. Tiny particles of the chemical; are transferred to the letter, which can then be developed by the recipient. Most developing agents make the chemical traces grow, so that the message becomes legible, and unless the correct agent is known, the message remains undetectable.

-- Peter Wright, *Spy Catcher* (1987), p.119

For an explanation of secret inks, see Robert Wallace and H. Keith Melton, *Spycraft: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda* (2008), pp. 427-437.

Section 603 Referral. Section 603 of the "Intelligence Authorization Act for FY 1990" states: "Subject to the authority of the Attorney General, the FBI shall supervise the conduct of all investigations of violations of the espionage laws of the United States by persons employed by or assigned to United States diplomatic missions abroad. All departments and agencies shall report immediately to the FBI any information concerning such a violation. All departments and agencies shall provide appropriate assistance to the FBI in the conduct of such investigations. Nothing in this provision shall be construed as establishing a defense to any criminal, civil, or administrative action." (Public Law 101-193, 30 Nov 1989) Also see *Section 811 Referral*.

See <http://www.intelligence.senate.gov/laws/pl101-193.pdf>

Section 811 Referral. Section 811 of the Intelligence Authorization Act of 1995 (50 USC 402a) is the legislative act that governs the coordination of counterespionage investigations between Executive Branch agencies and departments and the FBI. Section 811 referrals are the reports – made by the Executive Branch agencies or departments to the FBI under Section 811(c)(1)(a) – that advise the FBI of any information, regardless of origin, which may indicate that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power. (CI Community Lexicon)

Section 811 was enacted in response to the damage to US national security caused by the Aldrich Ames espionage case. The Ames case led to a legislative call for agencies to share data in counterespionage investigations and for the FBI to be involved earlier in the process of evaluating information concerning the possible compromise of classified information.

Within DoD, all *811 Referrals* are considered "significant CI activities" and as such must also be reported to DIA Office of Counterintelligence - Counterespionage Division (OCI-2)

See <http://www.intelligence.senate.gov/laws/pl103-359.pdf>

"811" referrals… allow our operational counterintelligence sections to concentrate solely on detecting and countering foreign intelligence operations, focus on emerging strategic threats, and protecting United States secrets from compromise.

-- Robert S. Muller, III, Director FBI
Before the Senate Committee on the Judiciary (6 June 2002)

Security. Proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences. (DoDD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012 w/ chg 1 dated 24 Apr 2013) Also see *operational security (OPSEC); security disciplines; security profession, security professional.*

DoD Policy

Security is a mission critical function of the DoD and its proper execution has a direct impact on all DoD missions and capabilities and on the national defense.

Security is the personal responsibility of all DoD personnel….

-- DoD 5200.43, Management of the Defense Security Enterprise, 1 Oct 2012

-- Also, 1) Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. 2) A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. 3) With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. (JP 1-02; JP 2-0, Joint Intelligence, 22 Oct 2013; and JP 3-10, Joint Security Operations in Theater, 3 Feb 2010)

-- Also, the protection of information to assure it is not accidentally or intentionally disclosed to unauthorized personnel. (DSS Glossary)

Security is not counterintelligence – counterintelligence is not security.

"People like to confuse counterintelligence (CI) with security. In practice, the two are related but not identical."

-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

"…[C]ounterintelligence measures deal directly with foreign intelligence service activities, while security programs are indirect defensive actions that minimize vulnerabilities."

-- SSCI Report 99-522 (1986)

"Counterintelligence investigates the enemy, or if you will in the modern world, the opposition, to learn their capabilities, intentions, methods and focus. ***It is not security work. Security protects. It does not attack.*** *[Emphasis added] CI attacks the actor. It attacks the opposition intelligence structures. It is not speculative. CI feeds security because it helps them focus on meaningful measures and safeguards. Using CI to help security is just smart security."*

-- Robert P Hanssen (Soviet Spy, Former FBI Agent and current Federal inmate) as quoted in "Diary of a Spy" by Paul M. Rodriquez, *Insight on the News*, 16 July 2001.

Security *vs.* Counterespionage -- *"[T]he security effort seeks primarily to protect its assigned material against compromise, deliberate or accidental, while the counter-espionage effort operates actively to identify, thwart. mislead, and destroy an opposing espionage capability."*

-- George P. Morse, *America Twice Betrayed: Reversing Fifty Years of Government Security Failure* (1995), p. 50

"Counterintelligence… is often confused with security—that is, merely with protecting secrets and protecting against subversion. Yet whereas the objective of security is to cut and prevent all contacts between hostiles and those who are to be protected the objective of CI is to engage hostile intelligence, control what it knows, and if possible control what it does. In principle, neither security people nor CI people deny the validity of the others approach, but CI people think of security as flatfooted cops, and the latter think of the former as game-playing spooks."

-- Angelo Codevilla, *Informing Statecraft: Intelligence for a New Century* (1992), p. 26

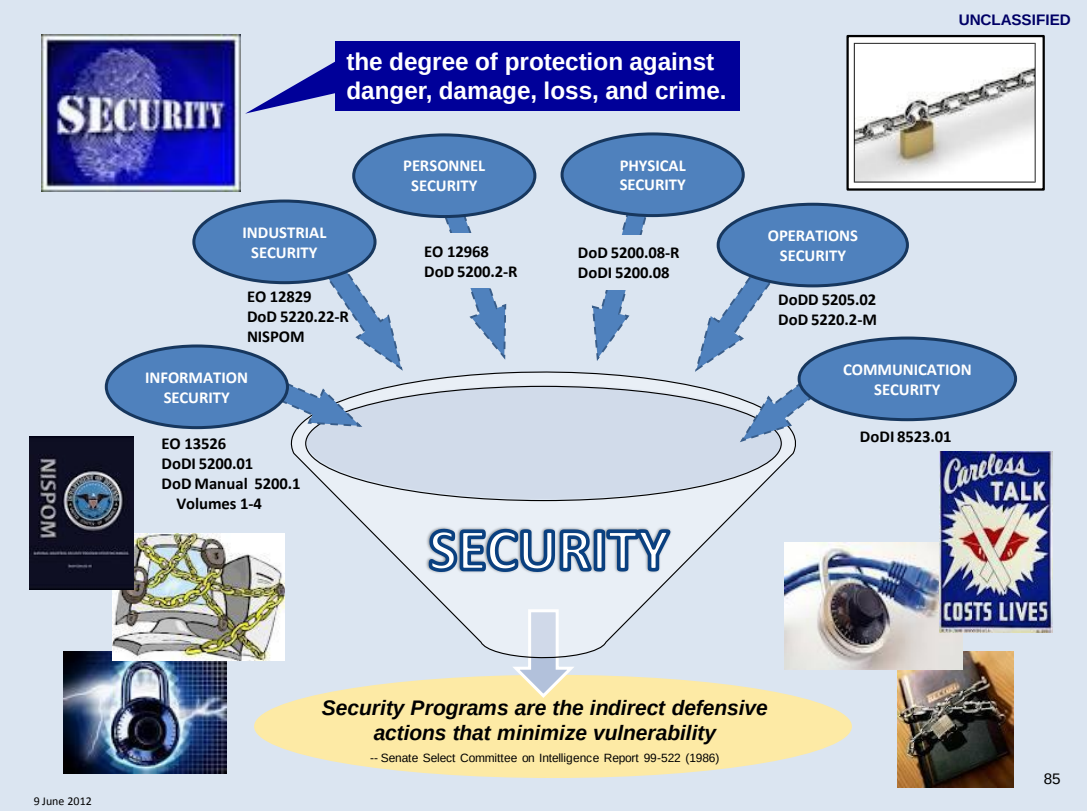
"Security is a dimension of clandestinity in espionage, counterespionage, counterintelligence, adultery, and poker. It is to these activities what style is to a writer, an athlete, or a musician, but it is not itself a work, a game, or a performance. Its purpose is prophylactic: it excludes toxic and infectious organisms and conserves vital fluids."

-- William R. Johnson, "Clandestinity and Current Intelligence." *Studies in Intelligence*, vol 20, no. 3, (Fall 1976), pp. 15-69. Originally classified "Secret / No Foreign Dissem" [declassified].

"CI and security shall be regarded as interdependent and mutually supportive disciplines with shared objectives and responsibilities associated with the protection of secrets and assets."

"Security programs establish appropriate personnel, physical, information, operations, industrial and technical security, safeguards, and countermeasures to protect information and information systems, personnel, operations, resources, technologies, and facilities from threats."

-- ICD 700, Protection of National Intelligence, 7 Jun 2012



"Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness."

-- President Ronald Reagan, NSDD-145, 17 Sep 1984

General functions and responsibilities performed by security professionals, including communications security, counterintelligence awareness, security systems, international programs, operations security, research and technology protection, sensitive compartmented information security, special access program security, and security program policy.

-- DoDI 3305.13, DoD Security Education, Training, and Certification, 13 Feb 2014

Security--Four Basic Principles

According to the Joint Security Commission, security is a dynamic and flexible system guided by four basic principles:

1) Security policies and services must be realistically matched to the threats we face. The processes we use to formulate policies and deliver services must be sufficiently flexible to facilitate their evolution as the threat changes.

2) Security policies and practices must be consistent and coherent across the Defense and Intelligence Communities, thereby reducing inefficiencies and enabling us to allocate scare resources efficiently.

3) Security standards and procedures must result in the fair and equitable treatment of the members of our communities upon whom we rely to guard the nation's security.

4) Security policies, practices, and procedures must provide the security we need at a price we can afford.

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, p. 3

Security is a highly decentralized government function. […] Effectively addressing security generates costs that must be balanced against risk and threats. Security, as a discipline, has historically been dominated by "police" type management, processes, and enforcement approaches. Although the police function is still required, today's security vulnerabilities are increasingly technical in nature and related to information technology systems, software, and hardware.

-- WMD Report (31 March 2005), p. 545

Security Classification. A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required. (JP 1-02)

There are three categories of security classification:

1) ***Top Secret***--National security information or material that requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

2) ***Secret***--National security information or material that requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

3) ***Confidential***--National security information or material that requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

For additional information see website at: <http://www.archives.gov/isoo/policy-documents/>

Security Classification Guide (SCG). A documentary form of classification guidance issued by an OCA [original classification authority] that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element. (DoD Manual 5200.01-Vol 1, DoD Information Security Program, 24 Feb 2012)

Security Clearance. An administrative determination by competent authority that an individual is eligible, from a security stand-point, for access to classified information. (JP 1-02)

> Within DoD, a security clearance is a determination that a person is eligible under DoD policy for access to classified information. Clearances allow personnel to access classified information categorized into three levels: top secret, secret, and confidential. The damage to national defense and foreign relations that unauthorized disclosure could reasonably be expected to cause ranges from "exceptionally grave damage" for top secret information to "damage" for confidential information.
>
> _____
>
> *The security clearance process is designed to determine the trustworthiness of an individual prior to granting him or her access to classified national security information. The process has evolved since the early 1950s, with antecedents dating to World War II.*
>
> *A security clearance is a determination that an individual—whether a direct federal employee or a private contractor performing work for the government—is eligible for access to classified national security information.*
>
> *A security clearance alone does not grant an individual access to specific classified materials. Rather, a security clearance means that an individual is eligible for access. In order to gain access to specific classified materials, an individual should also have a demonstrated "need to know" the classified information for his or her position and policy area responsibilities. In addition, prior to accessing classified information, an individual must sign an appropriate nondisclosure agreement.*
>
> -- CRS Report R43216, *Security Clearance Process: Answers to Frequently Asked Questions*, 9 Sep 2013 *
>
> * Copy available at: <http://www.fas.org/sgp/crs/secrecy/R43216.pdf>

Security Clearance Investigation. An inquiry into an individual's loyalty, character, trustworthiness and reliability to ensure that he or she is eligible for access to national security information. (ONCIX, <http://www.ncix.gov/SEA/reform/secvssuit.php>; accessed 18 Sep 2012) Also see *suitability investigation*.

> "*The Director of National Intelligence shall serve as the **Security Executive Agent**. As the Security Executive Agent the Director of National Intelligence shall direct the oversight of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position made by any agency; shall be responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position."*
>
> – EO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, 2 Jul 2008

Security Compromise. The disclosure of classified information to persons not authorized access thereto. (DSS Glossary)

Security Countermeasures (SCM). Actions, devices, procedures, and/or techniques to reduce security risks. (IC Standard 700-1, 4 Apr 2008)

-- Also, those protective activities required to prevent espionage, sabotage, theft, or unauthorized use of classified or controlled information, systems, or material of the Department of Defense. (JP 1-02; and in previous edition JP 2-01.2, dated 13 Jun 2006)

Security Detainee. Those detainees who are not combatants, but who may be under investigation or pose a threat to US forces if released. (Army FM 2-22.3, HUMINT Collector Operations, Sep 2006)

Security Disciplines. Core functions and responsibilities performed by security professionals with a concentration in personnel, physical, information, and industrial security. (DoDI 3305.13, DoD Security Education, Training, and Certification, 13 Feb 2014) Also see *security; security professional*.

Security Environment Threat List. A list of countries with United States Diplomatic Missions that is compiled by the Department of State and updated semi-annually. The listed countries are evaluated based on: transnational terrorism; political violence; human intelligence; technical threats; and criminal threats [and rated via] four threat levels: Critical, High, Medium and Low. (DSS Glossary)

> Four Threat Levels:
>
> ***Critical*** – defined as a definite threat to United States assets based on adversary's capability, intent to attack, and targeting conducted on a recurring basis;
>
> ***High*** – defined as a credible threat to United States assets based on knowledge of an adversary's capability, intent to attack, and related incidents at similar facilities;
>
> ***Medium*** – defined as a potential threat to United States assets based on knowledge of an adversary's desire to compromise the assets and the possibility that the adversary could obtain the capability to attack through a third party who has demonstrated such a capability; and
>
> ***Low*** – defined as little as no threat as a result of the absence of credible evidence of capability, intent, or history of actual or planned attack against United States assets.

Security Executive Agent (SecEA). The Director of National Intelligence shall serve as the Security Executive Agent. (EO 13467, 30 Jun 2008)

> For additional information see Security Executive Agent Directive 1 "Security Executive Agent Authorities and Responsibilities," 13 Mar 2012.
>
> Copy at: <http://www.ncix.gov/SEA/docs/2012-03-13_SEAD-1_Directive.pdf>

Security Incident. A security compromise, infraction, or violation. (DSS Glossary)

Security In-Depth. A concept of security calling for layered and complementary controls sufficient to detect and deter infiltration and exploitation of an organization, its information systems and facilities. (IC Standard 700-1, 4 Apr 2008)

-- Also, a combination of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the installation and/or facility and the ability to delay and respond with force. Examples include the use of perimeter fences, employee and visitor entry and/or exit controls, sensors and intrusion detection systems, closed circuit video monitoring, security patrols during working and non-working hours, or other safeguards that mitigate vulnerabilities. (DTM 09-012, 8 Dec 2009, w/ chg 2 dated 9 Sep 2012)

-- Also, an array of security measures which, considered as a whole, provide a level of security greater that that by any one measure individually. Includes identification checks, perimeter fences, police patrols, motion detectors, and other security measures. (DoD Manual S-5240.09, OFCO Procedures and Security Classification Guide, 13 Jan 2011 w/ change 1 dated 16 Oct 2012)

Security Infraction. A security incident that is not in the best interest of security and does not involve the loss, compromise, or suspected compromise of classified information. (DSS Glossary)

Security Measures: [Actions] taken by the government and intelligence departments and agencies, among others, for protection from espionage, observation, sabotage, annoyance, or surprise. With respect to classified materials, it is the condition which prevents unauthorized persons from having access to official information which is safeguarded in the interests of national defense. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Security Profession. An occupation dedicated to the protection of people, facilities, information, operations, and activities. (DoDI 3305.13, DoD Security Education, Training, and Certification, 13 Feb 2014) Also see *security; security disciplines; security professional*.

Security Professional. An individual who is educated, trained, and experienced in one or more security disciplines and provides advice and expertise to senior officials on the effective and efficient implementation, operation, and administration of the organization's security programs. (DoDI 3305.13, DoD Security Education, Training, and Certification, 13 Feb 2014) Also see *security; security profession*.

Security Service. Entity or component of a foreign government charged with responsibility for counterespionage or internal security functions. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; and CI Community Lexicon)

Sedition. Willfully advocating or teaching the duty or necessity of overthrowing the US government or any political subdivision by force or violence. (JP 1-02; also in previous edition JP 2-01.2, dated 13 Jun 2006)

> Sedition and criminal subversion of military forces are violations of Title 18 USC, §§ 2384-2390 and is a punishable offense under UCMJ Article 94. It is a term of law which refers to overt conduct that is deemed by the legal authority as tending toward insurrection against the established order. It is the crime of creating a revolt, disturbance, or violence against lawful civil authority with the intent to cause its overthrow or destruction. Sedition often includes subversion of a constitution and incitement of discontent (or resistance) to lawful authority. A seditionist is one who engages in or promotes the interests of sedition.
>
> The difference between sedition and treason consists primarily in the subjective ultimate object of the violation to the public peace. Sedition does not consist of levying war against a government nor of adhering to its enemies, giving enemies aid, and giving enemies comfort. Nor does it consist, in most representative democracies, of peaceful protest against a government, nor of attempting to change the government by democratic means (such as direct democracy or constitutional convention).
>
> Sedition is the stirring up of rebellion against the government in power. Treason is the violation of allegiance to one's sovereign or state, giving aid to enemies, or levying war against one's state. Sedition is encouraging one's fellow citizens to rebel against their state, whereas treason is actually betraying one's country by aiding and abetting another state.

Seizure. The taking or dispossession of property from the possessor by an authorized person or the restriction of the freedom of movement of an individual against his or her will by an agent of the Government. (AR 190-20) Also see *search*.

Self-radicalization. Significant steps an individual takes in advocating or adopting an extremist belief system for the purpose of facilitating ideologically-based violence to advance political, religious, or social change. The self-radicalized individual has not been recruited by and has no direct, personal influence or tasking from other violent extremists. The self-radicalized individual may seek out direct or indirect (through the Internet for example) contact with other violent extremists for moral support and to enhance his or her extremist beliefs. (DoDD 5240.06, CIAR, 17 May 2011 with change 1 dated 30 May 2013) Also see radicalization; violent radicalization.

-- Also, the process whereby people seek out opportunities for involvement in terrorist activity absent a formal involvement in a terrorist group and/or recruitment by others. (DSB Report, *Predicting Violent Behavior*, Aug 2012, citing Horgan's *The Psychology of Terrorism 2nd Edition*, 2012)

-- Also, *self radicalization*: a phenomenon in which individuals become terrorists without joining an established radical group, although they may be influenced by its ideology and message. (DSB Report, *Predicting Violent Behavior*, Aug 2012)

Senate Select Committee on Intelligence (SSCI). Created pursuant to Senate Res. 400, 94th Congress: to oversee and make continuing studies of the intelligence activities and programs of the United States Government, and to submit to the Senate appropriate proposals for legislation and report to the Senate concerning such intelligence activities and programs. Provides legislative oversight over US intelligence activities to assure that such activities are in conformity with the Constitution and laws of the United States. (www.intelligence.senate.gov)

> The 1980 Intelligence Oversight Act charged the SSCI and the House Permanent Select Committee on Intelligence (HPSCI) with authorizing the programs of US intelligence agencies and overseeing their activities.
>
> *It is IC policy that IC elements shall, in a timely manner, keep the Congressional intelligence committees fully informed, in writing, of all significant anticipated intelligence activities, significant intelligence failures, significant intelligence activities, and illegal activities.*
>
> -- ICD 112, *Congressional Notification*, 16 Nov 2011
>
> See an interested article entitled "Congressional Oversight of Intelligence: One Perspective," by Mary Sturtevant, Senate Committee Staff, in *American Intelligence Journal*, Summer 1992; copy available on line at: <http://www.fas.org/irp/eprint/sturtevant.html>

Senior Defense Official / Defense Attaché (SDO/DATT). Principal DoD official in a U.S. embassy, as designated by the Secretary of Defense. (DoDD 5105.75, DoD Operations at Defense Embassies, 21 Dec 2007) Also see *Defense Attaché Office*.

> The SDO/DATT is the Chief of Mission's (COM's) principal military advisor on defense and national security issues, the senior diplomatically accredited DoD military officer assigned to a US diplomatic mission, and the single point of contact for all DoD matters involving the embassy or DoD elements assigned to or working from the embassy.
>
> All DoD elements assigned or attached to or operating from U.S. embassies are aligned under the coordinating authority of the SDO/DATT. See DoD Directive 5105.75, DoD Operations at U.S. Embassies.

Sensitive. Requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power. May be applied to an agency, installation, person, position, document, material, or activity. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Sensitive Activities [within DoD]. Operations, actions, activities, or programs that are generally handled through special access, compartmented, or other sensitive control mechanisms because of the nature of the target, the area of operation, or other designated aspects. Sensitive activities also include operations, actions, activities, or programs conducted by any DoD Component that, if compromised, could have enduring adverse effects on U.S. foreign policy, DoD activities, or military operations; or cause significant embarrassment to the United States, its allies, or the DoD. (DoDI O-5100.94, Oversight, Coordination, Assessment, and Reporting of DoD Intelligence and Intelligence-Related Sensitive Activities, 27 Sep 2011 w/ change 1 dated 15 Oct 2013)

Sensitive Compartmented Information (SCI). All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

-- Also, classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the DNI. (National Intelligence: A Consumer's Guide – 2009).

-- Also, classified national intelligence information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the DNI. (DoDI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information, 9 Oct 2008 w/ chg 1)

Sensitive Compartmented Information Facility (SCIF). An accredited area, room, group of rooms, or installation where sensitive compartmented information (SCI) may be stored, used, discussed, and/or electronically processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

-- Also, a subset of CNI [Classified National Intelligence] concerning or derived from intelligence sources, methods or analytical processes that is required to be protected within formal access control systems established by the DNI [Director of National Intelligence]. (ICD 703, Protection of Classified National Intelligence, Including Sensitive Compartmented Information, 21 Jun 2013)

-- Also, an accredited area where Sensitive Compartmented Information may be stored, used, discussed, and/or processed. Only those Intelligence Community Agencies with SCIF Accreditation Authority may officially accredit facilities to handle, process, and store SCI materials. (National Intelligence: A Consumer's Guide - 2009).

> For additional information on SCIFs see *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, IC Standard Number 705-1, 17 Sep 2010, and *Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information*, IC Standard Number 705-2, 17 Sep 2010.

Sensitive Information. Information that the loss, misuse, unauthorized access, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code, but that has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of National defense or foreign policy. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Sensitive Site. A geographically limited area that contains, but is not limited to, adversary information systems, war crimes sites, critical government facilities, and areas suspected of containing high value targets. (JP 1-02 and JP 3-31, Command and Control for Joint Land Operations, 29 Jun 2010)

-- Also, a designated, geographically limited area with special diplomatic, informational, military, and economic sensitivity for the United States. This includes factories with technical data on enemy weapon systems, war crimes sites, critical hostile government facilities, areas suspected of containing persons of high rank in a hostile government or organization, terrorist money-laundering areas, and document storage areas for secret police forces. (Army FM 2-0, Intelligence, 23 Mar 2010)

Sensitive Site Exploitation (SSE). *Within DoD, term rescinded.* See *site exploitation*.

> This term was previously defined in JP 1-02 as: a related series of activities inside a captured sensitive site to exploit personnel documents, electronic data, and material captured at the site, while neutralizing any threat posed by the site or its contents.
>
> Note: Army Tactics, Techniques and Procedures (ATTP) 3-90.15 [FM 3-90.15] (8 Jul 2010) also rescinded *"sensitive site exploitation"* as a doctrinal term.

Sensitive Sources and Methods. A collective term for those persons, organizations, things, conditions, or events that provide intelligence information and those means used in the collection, processing, and production of such information which, if compromised, would be vulnerable to counteraction that could reasonably be expected to reduce their ability to support US intelligence activities. (ICS Glossary)

Sensemaking. A set of philosophical assumptions, substantive propositions, methodological framings, and methods. (*Sensemaking: A Structure for an Intelligence Revolution* by David T. Moore) Also see *sensemaking*. Also see *intelligence sensemaking*.

> Sensemaking goes beyond analysis, a disaggregative process, and also beyond synthesis, which meaningfully integrates factors relevant to an issue. It includes an interpretation of the results of that analysis and synthesis. It is sometimes referred to as an approach to creating situational awareness "in situations of uncertainty."
>
> Copy of *Sensemaking: A Structure for an Intelligence Revolution* by David T. Moore available at <http://ni-u.edu/ni_press/pdf/Sensemaking.pdf>

Serials. Individual items of evidence in a counterintelligence case are known as serials. They may not necessarily reach a standard required for a criminal prosecution but the objective is not necessarily to achieve a public trial and conviction, but to develop an investigation to the point where some advantage can be achieved. While serials may include entirely circumstantial evidence, unsubstantiated allegations, and coincidence, until verified or dismissed through inquiry and research, they remain valid and may stay in a dossier for decades. (Historical Dictionary of Cold War Counterintelligence, 2007)

Shape. The ability to conduct activities to affect the perceptions, will, behavior, and capabilities of partner, competitor, or adversary leaders, military forces, and relevant populations to further U.S. national security or shared global security interests. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Shielded Enclosure. Room or container designed to attenuate electromagnetic radiation, acoustic signals, or emanations. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Short-Range Agent Communication (SRAC). A device that allows agent and [case] officer to communicate clandestinely over a limited distance. (Spycraft)

Signal. A prearranged visual or audio sign that a dead drop has been filled or emptied or that an emergency meeting is needed. (FBI FCI Terms) Also see *signals*.

-- Also, prearranged visual or audio indicator having a designated significance for intelligence personnel involved. For example, to signify that a dead drop has been filled or emptied or to call an emergency or unscheduled personal meeting. (AFOSI Manual 71-142, OFCO, 9 June 2000)

Signal Flags. The IC [Intelligence Community] database containing information used to assist security and counterintelligence professionals conducting National Agency Checks on individuals applying for positions with IC organizations. (IC Standard 700-1, 4 Apr 2008)

Signal Security (SIGSEC). A generic term that includes both communications security and electronics security. (JP 1-02) Also see *security*.

Signal Site. A prearranged fixed location, usually in a public place, on which an agent or intelligence officer can place a predetermined mark in order to alert the other to operational activity. Such a mark may be made by, for example, chalk or a piece of tape. (FBI -- Affidavit: USA vs. Robert Philip Hanssen, 16 Feb 2001)

> *The operational activity signaled may be the fact that a dead drop has been "loaded" and is ready to be "cleared." A call-out signal may be used to trigger a contact between an agent and an intelligence officer.*
>
> – FBI: Affidavit USA vs. Robert Philip Hanssen, 16 Feb 2001)

-- Also, a covert means of communications using a nonalerting signal, such as a chalk mark on a lamppost, to either initiate or terminate a clandestine act, (Spycraft) Also see *signals*.

Signals. Any form of clandestine tradecraft using a system of marks, signs, or codes for signaling between operatives. (CI Centre Glossary) Also see *signal site*.

Signals Intelligence (SIGINT). 1) A category of intelligence comprising either individually or in combination all communications intelligence [COMINT], electronic intelligence [ELINT], and foreign instrumentation signals intelligence [FISINT], however transmitted. 2) Intelligence derived from communications, electronic, and foreign instrumentation signals. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

For DoD policy see DoDI O-3115.07, Signals Intelligence (SIGINT), 15 Sep 2008

-- Also, intelligence gathered from data transmissions [signals intercepts], including Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT). SIGINT includes both raw data [collection] and the analysis of that data to produce intelligence. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, information derived from intercepted communications and electronic and data transmissions. (WMD Report, 31 Mar 2005)

The collection of signals intelligence is necessary for the United States to advance its national security and foreign policy interests and to protect its citizens and the citizens of its allies and partners from harm.

-- PDD-28 Signals Intelligence Activities, 17 Jan 2014

The Intelligence Community refers to the collection and exploitation of signals transmitted from communication systems, radars, and weapon systems as signals intelligence or SIGINT. SIGINT consists of Communications Intelligence (COMINT) – technical and intelligence information derived from intercept of foreign communications; Electronic Intelligence (ELINT) – information collected from systems such as radars and other weapons systems; and Foreign Instrumentation Signals Intelligence (FISINT) – signals detected from weapons under testing and development.

SIGINT is collected in a variety of ways depending on the type of signal targeted. The National Security Agency (NSA) collects the raw SIGINT and then NSA translators, cryptologists, analysts, and other technical experts turn the raw data into something that an all-source analyst can use. Once the NSA has collected, processed, and analyzed SIGINT, it is passed on to CIA and Intelligence Community analysts who use it to complement information from other sources to produce finished intelligence.

The volume and variety of today's signals adds challenges to the timely production of finished intelligence for policymakers. It is a lot of work to track and analyze all the SIGINT collected.

-- www.cia.gov (accessed, 30 Nov 2010)

Signals Intelligence (SIGINT): The interception of signals, whether between people, between machines, or a combination of both. The National Security Agency (NSA) is responsible for collecting, processing, and reporting SIGINT. Within the NSA, the National SIGINT Committee advises the Director, NSA, and the Director of National Intelligence (DNI) on policy issues and manages the SIGINT requirements system.

-- www.intelligence.gov (accessed 13 Aug 2012)

Signals Intelligence (SIGINT)… comprises Communications Intelligence (COMINT) and Electronic Intelligence (ELINT) , and activities pertaining thereto….

-- NSCID 6, Signals Intelligence, 17 Feb 1972 (redacted copy, complete original version is TOP SECRET)
Available at: <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/docs/doc05.pdf>

Signature. A recognizable, distinguishing pattern. See also attack signature or digital signature. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Signatures. [In CI usage,] indicators of potential FISS and ITO [international terrorist organizations] methods of operations, including static surveillance of U.S. forces [and] installations…. (Army FM 2-22.2, CI, Oct 2009)

Sign-of-Life Signal. A signal emitted periodically to signify that an agent is safe. (FBI FCI Terms)

Silver Triangle. The South American region consisting of Peru, Bolivia, and Colombia that is historically known to be a major illegal drug production area. (JP 3-07.4**,** Joint Counterdrug Operations, 13 Jun 2007)

Single Scope Background Investigation (SSBI). Investigation for individuals requiring a top secret clearance or working in a critical sensitive position; normally covers a 5-year period and consists of a subject interview, NAC, credit checks, character references, and employment records checks and references.

-- Also, a personnel security investigation consisting of all the elements prescribed in Standard B of ICPG 704.1. The period of investigation for a SSBI varies, ranging from the immediate preceding 3 years for neighborhood checks to immediately preceding 10 years for local agency checks. (IC Standard 700-1, 4 Apr 2008)

Singleton. Intelligence operations conducted by a single intelligence officer or agent. These operations include intelligence collection, servicing agents, and courier services. (Spy Book)

Site Exploitation. A series of activities to recognize, collect, process, preserve, and analyze information, personnel, and/or materiel found during the conduct of operations. (JP 1-02 and JP 3-31, Command and Control for Joint Land Operations, 29 Jun 2010)

-- Also, systematically searching for and collecting information, material, and persons from a designated location and analyzing them to answer information requirements, facilitate subsequent operations, or support criminal prosecution. (Army Tactics, Techniques & Procedures 3-90.15 [FM 3-90.15], Site Exploitation Operations, 8 Jul 2010)

Situation Report (SITREP). A report giving the situation in the area of a reporting unit or formation. (JP 1-02 and JP 3-50, Personnel Recovery)

Situational Awareness. Immediate knowledge of the conditions of the operation, constrained geographically and in time. (Army FM 3-0, Operations, Feb 2008)

Slammer. Project Slammer was an Intelligence Community sponsored study of espionage to determine the motivation of the convicted spies and to learn the methods by which they committed their crimes.

> In 1985 U.S. intelligence agencies embarked on a 10-year benchmark study named Project Slammer, which was focused on interviewing incarcerated spies. It examined “espionage by interviewing and psychologically assessing actual espionage subjects Additionally, persons knowledgeable of subjects were contacted to better understand the subjects' private lives and how they are perceived by others while conducting espionage.” Project Slammer sought to understand of the dynamics of espionage and to incorporate of that enhanced understanding into government and industry security programs.
>
> Project Slammer research endeavor consisted of voluntary interviews with incarcerated spies and subsequent analysis of the data. The effort was essentially de-funded in the early nineties and consequently lost impetus. Nevertheless, there are currently extant several Slammer papers and tapes which are used throughout the security community. Those analyses deal with the essential and multi-faceted motivational patterns underlying espionage.
>
> Although dated, the study's findings remain significant, and the conclusions included: No offender entered a position of trust with the intent to betray; and there were two prevalent sets of personality traits: 1) highly manipulative, dominant, and self-serving; and 2) passive, easily influenced, and lacking self-esteem.

Sleeper. [Tradecraft jargon] an illegal; or agent in a foreign country who does not engage in intelligence activities until told to do so. (FBI FCI Terms)

-- Also, a spy placed in a target area but does not engage in espionage until he or she is activated at a future time. (Spy Book)

-- Also, an illegal or agent residing in a foreign country under orders to engage in no intelligence activities. The inactive status, which can endure for a considerable time, serves to strengthen the legend and permit access by a foreign power to an individual in position to be ready for action under certain circumstances should a specific need arise. (Word of Intelligence, 2nd Edition, 2011)

SMADS. See *Strategic Mission Assurance Data System*.

Social Engineering, An attempt to trick someone into revealing information (e.g., a password) that can be used to attack an enterprise. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. (The Ultimate Guide to Social Engineering, undated)

Copy of "The Ultimate Guide to Social Engineering" available on line at: <http://assets.csoonline.com/documents/cache/pdfs/Social-Engineering-Ultimate-Guide.pdf>

Social Networking. Web-based services that allow individuals to create a public profile, to create a list of users with whom to share connection, and view and cross the connections within the system. (Wikipedia)

Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as, mobile connectivity, photo/video/sharing and blogging. Social networking sites allow users to share ideas, pictures, posts, activities, events, and interests with people in their network.

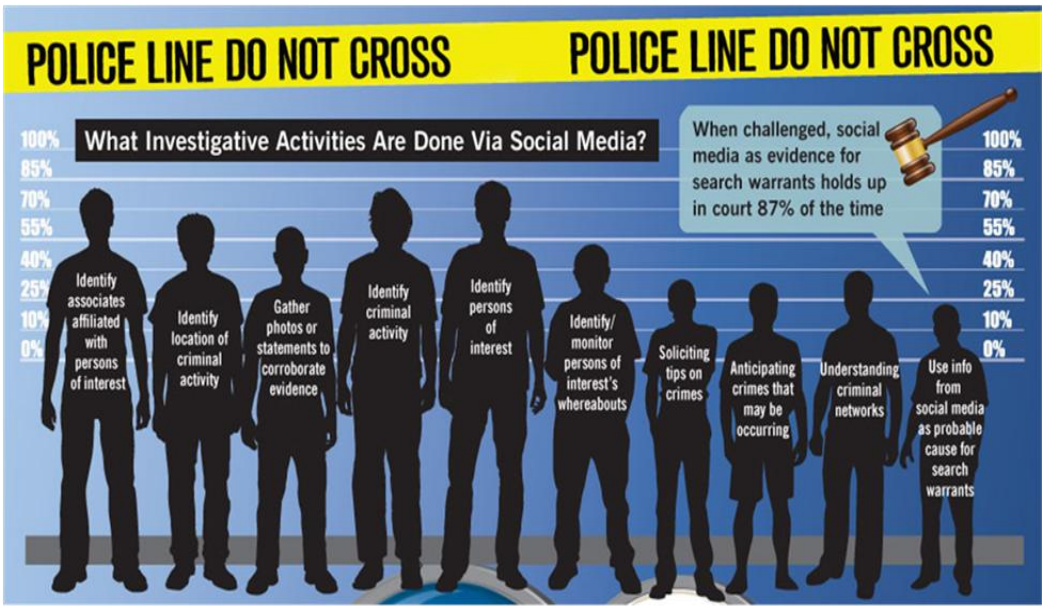
The main types of social networking services are those that contain category places (such as former school year or classmates), means to connect with friends (usually with self-description pages), and a recommendation system linked to trust. Popular methods now combine many of these, with American-based services such as *Facebook, Google+, YouTube, LinkedIn, Instagram, Pinterest, Tumblr* and *Twitter* widely used worldwide*; Nexopia in Canada; Badoo, Bebo, VKontakte (Russia), Delphi* (also called *Delphi Forums*), *Draugiem.lv* (mostly in Latvia), *Hi5* (Europe), *Hyves* (mostly in The Netherlands*), iWiW* (mostly in Hungary), *Nasza-Klasa*, *Soup* (mostly in Poland), *Glocals* in Switzerland, *Skyrock, The Sphere, StudiVZ* (mostly in Germany), *Tagged, Tuenti* (mostly in Spain), and *XING* in parts of Europe; *Hi5* and *Orkut* in South America and Central America; *Mxit* in Africa; and *Cyworld, Mixi, Orkut, renren, weibo* and *Wretch* in Asia and the Pacific Islands.

Social networking services are increasingly being used in legal and criminal investigations. Information posted on sites such as *MySpace* and *Facebook* has been used by police (forensic profiling), probation, and university officials to prosecute users of said sites. In some situations, content posted on *MySpace* has been used in court

-- Wikipedia at <http://en.wikipedia.org/wiki/Social_networking> (accessed 11 Mar 2014)

See "Social Media: Establishing Criteria for Law Enforcement Use" by Robert D. Stuart, M.S., in FBI, *Law Enforcement Bulletin*, Feb 2013. Article available at: <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/2013/february/social-media-establishing-criteria-for-law-enforcement-use>

"Under Investigation: Social Media Use by Law Enforcement"



-- http://www.lexisnexis.com/government/investigations/ (accessed 11 Mar 2014)

Socio-Cultural Dynamics. Information about the social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment. (DoDD 3600.01, Information Operations, 14 Aug 2006 with Chg 1, 23 May 2011)

Sociocultural Analysis (SCA). The analysis of adversaries and other relevant actors that integrates concepts, knowledge, and understanding of societies, populations, and other groups of people, including their activities, relationships, and perspectives across time and space at varying scales. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Sociocultural Factors. The social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment. (JP 1-02 and JP 2-01.3, Joint Intelligence Preparation of the Operational Environment)

Software Assurance. The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle. (DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012)

Source. A person, thing, or activity from whom information or services are obtained. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013, with chg 1 dated 13 Jun 2013) Also see *agent; asset, controlled source; human source; HUMINT source.*

-- Also, 1) A person, thing, or activity from which information is obtained; 2) In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes; or 3) In interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. In this context, a controlled source is in the employment or under the control of the intelligence activity and knows that the information is to be used for intelligence purposes. An uncontrolled source is a voluntary contributor of information and may or may not know that the information is to be used for intelligence purposes. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, a person from whom information or services are obtained. (DoDD S-5200.37, Management & Execution of Defense HUMINT, 9 Feb 2009 w/ chg 2)

-- Also, a person, device, system, or activity from which services or information are obtained. (Defense HUMINT Enterprise Manual 3301.02, Vol II Collection Operations, 23 Nov 2010)

-- Also, a person from whom information or services are obtained. (DoDD 3600.01, Information Operations, 14 Aug 2006 with Chg 1, 23 May 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, a document, interview, or other means by which information has been obtained. From an intelligence perspective, sources are individuals (or HUMINT) who collect or possess critical information needed for intelligence analysis. (ODNI, U.S. National Intelligence – An Overview 2011)

Source Directed Requirement (SDR). A HUMINT collection requirement based upon the placement and access of a source to collect and report on a specific person, place, thing, or event. (DHE-M 3301.001, DIA HUMINT Manual, Vol I, 30 Jan 2009 w/ chg 2)

Source Management. The process of registering and monitoring the use of sources involved in counterintelligence and human intelligence operations to protect the security of the operations and avoid conflicts among operational elements. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Source Registry. A source record/catalogue of leads and sources acquired by collectors and centralized for management, coordination and deconfliction of source operations. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Source Validation. Vetting to determine if a source is who he/she claims to be, is free of external control, is capable of behaving in a secure manner, and possesses placement and access consistent with tasking. (HDI Lexicon, April 2008) Also see *vetting* and *counterintelligence flags*.

> All DoD human sources are vetted in accordance with National HUMINT Manager Directive 001.08 (HUMINT Source Validation).
>
> For DoD policy see DoDI S-3325.07, *Guidance for the Conduct of DoD Human Source Validation (U),* 22 Jun 2009.

Special Access Program (SAP). A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

-- Also, a program activity which has enhanced security measures and imposes safeguarding and access requirements that exceed those normally required for information at the same level. Information to be protected within the SAP is identified by an SCG [security classification guide]. (DoDI 5205.11, Management, Administration, and Oversight of DoD Special Access Programs, 6 Feb 2013)

-- Also, a sensitive program, approved in writing by a head of agency with original top secret classification authority, that imposes need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information. The level of controls is based on the criticality of the program and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

> DoD SAPs are established and maintained only when absolutely necessary to protect the Nation's most sensitive capabilities; information; technologies; operations; and research, development, test and evaluation; or when required by statute pursuant to DoDD 5205.07, SAP Policy, 1 Jul 2010.
>
> _____

Acknowledged – Unacknowledged – Waived

Acknowledged SAP: A SAP whose existence is acknowledged, affirmed, or made known to others, but its specific details (technologies, materials, techniques, etc.,) are classified as specified in the applicable SCG.

Unacknowledged SAP: A SAP having enhanced security measures ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information.

Waived SAP: A SAP for which the Secretary of Defense has waived applicable reporting in accordance with DoD Manual 5200.01 following a determination of adverse effect to national security. An unacknowledged SAP that has more restrictive reporting and access controls than other unacknowledged SAPs.

Interestingly, the Joint Security Commission noted in its 1994 report (*Redefining Security*) that --

"Special Access Programs are used to compensate for the fact that the classification system is not trusted to protect information effectively and does not adequately enforce the 'need to know' principle."

Special Access Program Central Office (SAPCO). The office within a DoD Component or OSD PSA that, when directed, executes, manages, administers, oversees, and maintains records on the SAPs for which it has been assigned CA. Responsibilities may also include developing and implementing policies and procedures for oversight, management, execution, administration, SAP security, IA for SAP IS, and records management of SAPs under their cognizance, as directed. (DoDD 5205.07, Special Access Program Policy, 1 Jul 2010)

The DoD SAPCO is the office charged by the Deputy Secretary of Defense with responsibility as the designated proponent for developing and implementing policies and procedures for DoD SAP execution, management, and administration.

For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), these functions shall be exercised by the Director of National Intelligence.

-- EO 13526, *Classified National Security Information*, 29 Dec 2009

Special Actions. Those functions that due to particular sensitivities, compartmentation, or caveats cannot be conducted in normal staff channels and therefore require extraordinary processes and procedures and may involve the use of sensitive capabilities. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

Special Activities. Activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the U .S. Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence U .S. political processes, public opinion, policies, or media and do not include diplomatic activities, the collection and production of intelligence, or related support functions. (IC Standard 700-1, 4 Apr 2008) Also see *covert action.*

-- Also, *within DoD: None -- term rescinded by JP 3-05, Special Operations, 18 Apr 2011.*

As previously defined, it was a term synonymous with "covert action" -- see *covert action.*

Special Agent. *Within DoD: None -- term rescinded by JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011.* See *Counterintelligence Special Agent.*

Previously defined in JP 1-02 as: a person, either United States military or civilian, who is a specialist in military [law enforcement,] security or the collection of intelligence or counterintelligence information.

-- Also, a United States military or civilian who is a specialist in military security or in the collection of intelligence or counterintelligence information. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Special Area Clearance. The required concurrence granted to DoD personnel by the Department of State and the Office of the USD(P) for travel to certain overseas areas designated by the Department of State as special areas. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

Special Collection Service (SCS). [According to open source,*] a joint CIA-NSA signals intelligence collection organization.

-- Also, elite, highly secret U.S. electronic intelligence group that conducts eavesdropping operations in [foreign] countries. The service is controlled by the NSA… [also] CIA experts are often assigned. (Spy Book)

* See Jeffrey T. Richelson, *The US Intelligence Community*, Sixth Edition, 2012, pp. 224-226

_____

"According to a former high-ranking intelligence official, SCS was formed in the late 1970s after competition between the NSA's embassy-based eavesdroppers and the CIA's globe-trotting bugging specialists from its Division D had become counterproductive. While sources differ on how SCS works, some claim its agents never leave their secret embassy warrens where they perform close-quarters electronic eavesdropping, while others say agents operate embassy-based equipment in addition to performing riskier 'black-bag' jobs, or break-ins, for purposes of bugging…."

-- Jason Vest & W. Madsen , "A Most Unusual Collection Agency," *The Village Voice*, 24 Feb - 2 Mar 1999

Special Collection Techniques. Those lawful investigative techniques which are employed by a DoD intelligence component under the rule of the least intrusive means, after a determination has been made that the required information is not publicly available, available with the consent of the person or persons concerned, or available from cooperative sources. (DIA Intelligence Law Handbook, Sep 1995) Also see *rule of the least intrusive means*.

Special collection techniques -- also commonly referred to as "special investigative techniques" within CI channels -- are addressed in DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 7 Dec 1982,

Procedures 5-10:

* Procedure 5 - Electronic Surveillance
* Procedure 6 - Concealed Monitoring
* Procedure 7 - Physical Searches
* Procedure 8 - Searches and Examination of Mail
* Procedure 9 - Physical Surveillance
* Procedure 10 - Undisclosed Participation in Organizations

Special Communication. See definition provided in DTM 08-019, Establishment of the DoD Special Communication Enterprise Office (SCEO), 11 Jun 2008, marked FOUO.

Special Event. An international or domestic event, contest, activity, or meeting, which by its very nature, or by specific statutory or regulatory authority, may warrant security, safety, and/or other logistical support or assistance from the Department of Defense. (DODD 3025.18, Defense Support of Civil Authorities, 29 Dec 2010)

Special Event Management. Planning and conduct of public events or activities whose character may them attractive targets for terrorist attack. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

Special Information Operations (SIO). Information operations that by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. (JP 3-13, Information Operations, 13 Feb 2006) Also see *information operations*.

Special Investigative Inquiry (SII). A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination. (IC Standard 700-1, 4 Apr 2008)

Special Investigative Techniques. See *Special Collection Techniques*.

Special Limiting Criteria (SLC). [Term used in document/media exploitation activities]. A narrowly-defined set of criteria intended to restrict access to data that, if compromised, could imperil planned operations, contain evidence of espionage or counterintelligence operations, identify sources and methods, and[/or] contain illegal or inappropriate material. (National Media Exploitation Center)

Special Mission Unit (SMU). A generic term to represent a group of operations and support personnel from designated organizations that is task-organized to perform highly classified activities. (JP 1-02 and JP 3-05.1, Joint Special Operations Task Force Operations, 26 Apr 2007)

Special Operations (SO). Operations requiring unique modes of employment, tactical techniques, equipment and training often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk. (JP 3-05, Special Operations, 18 Apr 2011)

Special Operations Activities. Activities that include each of the following insofar as it relates to special operations: direct action, strategic reconnaissance, unconventional warfare, foreign internal defense, civil affairs, psychological operations, counterterrorism, humanitarian assistance, theater search and rescue, and such other activities as may be specified by the president or the Secretary of Defense. (DoDD S-3325.09, Oversight, Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013, with chg 1 dated 13 Jun 2013)

Special Reconnaissance (SR). Reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces. (JP 3-05, Special Operations, 18 Apr 2011)

Special Security Center. The Director of National Intelligence element responsible for developing, coordinating, and overseeing Director of National Intelligence security policies and databases to support Intelligence Community security elements. The Special Security Center interacts with other Intelligence Community security organizations to ensure that Director of National Intelligence equities are considered in the development of national level security policies and procedures. (DSS Security Glossary)

Specified Task. In the context of joint operation planning, a task that is specifically assigned an organization by its higher headquarters. (JP 1-02 and JP 5-0, Joint Operation Planning, 11 Aug 2011)

Spoofing. [Tradecraft jargon] A ploy designed to deceive the observer into believing that an operation has gone bad when, in fact, it has been put into another compartment. (Spy Dust)

-- Also, [cyber usage] deceiving computers or computer users by hiding or faking one's identity. Email spoofing utilizes a sham email address or simulates a genuine email address. IP spoofing hides or masks a computer's IP address. (FBI; see <http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1>)

Spot. [In intelligence usage,] to locate and recruit people demonstrated access to intelligence targets. (*TOP SECRET: The Dictionary of Espionage and Intelligence*, 2005)

-- Also, to identify for consideration potential sources as candidates for recruitment. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Spot Report. A non-standard DoD HUMINT report (not an IR) used to report on actionable/perishable HUMINT of a non-CRITIC nature. (DHE-M 3301.001, Vol I: Collection Requirement, Reporting, and Evaluation Procedures, 30 Jan 2009, w/ chg 2 dated 1 Feb 2012)

-- Also, a concise narrative report of essential information covering events or conditions that may have an immediate and significant effect on current planning and operations that is afforded the most expeditious means of transmission consistent with requisite security. Also called SPOTREP. (Note: In reconnaissance and surveillance usage, spot report is not to be used.) (JP 1-02 and JP 3-09.3, Close Air Support)

For CRITIC reporting see Chapter Three - Specialized Intelligence Reporting, DHE-M 3301.001, Vol I: *Collection Requirement, Reporting, and Evaluation Procedures* (U), 30 Jan 2009, w/ chg 2, dated 1 Feb 2012.

Spotter. In intelligence, an agent or illegal assigned to locate and assess individuals in positions of value to an intelligence service. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; and CI Community Lexicon) Also see *spotter / assessor.*

-- Also, an agent or illegal assigned to locate and assess individuals who might be of value to an intelligence service. (FBI FCI Terms)

Spotter / Assessor. An asset assigned to locate and/or assess individuals of intelligence or operational interest. (HDI Lexicon, April 2008) Also see *spotter; spotter assessor operation*.

Spotter / Assessor Operation. Those actions taken to identify persons who may be in contact with or placed in contact with opposition intelligence and counterintelligence services, and to determine the potential value of these persons as intelligence or counterintelligence sources. (AR 381-47, OFCO, 17 Mar 2006)

Spy. A generic term that refers… to either a professional intelligence officer work works for an intelligence service, or to a foreign source or asset who steals secrets on behalf of that intelligence service. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

-- Also, a person employed by or in the service of a foreign government, either with or without pay, to secure information considered vital to the waging of a shooting or economic war against another country. (Committee on Un-American Activities, U. S. House of Representatives, April 1949)

[T]he spy is the greatest of soldiers. If he is the most detested by the enemy, it is only because he is the most feared.

– King George V (1865-1936)

A U.S, intelligence officer that handles clandestine human sources is normally referred to as a "case officer (C/O)" or "operations officer (OO)." The people that case officers or OOs recruit as penetrations of foreign governments and organizations are their "agents." Agents have access to important information and pass that information secretly to their case officers/OOs.

An army without secret agents is exactly like a man without eyes or ears.

-- Chia Lin, Chinese Strategist of the late eighth century

One spy in the right place is worth 20,000 men in the field.
-- Napoleon

_____

In the circumstances of espionage and betrayal,
one county's heroic spy is another's traitor.
-- Frederick P. Hitz, Former Inspector General of the CIA (1990 - 1998)

_____

"What do you think spies are: priests, saints, and martyrs?
They're a squalid procession of vain fools, traitors too, yes;
pansies, sadists and drunkards, people who play
cowboys and Indians to brighten their rotten lives…"
-- Alec Leamas, the protagonist in LeCarre's *The Spy Who Came in From the Cold*.

Spy Dust (also called METKA). Chemical marking compound developed by the KGB to keep tabs on the activities of a target officer. The compound is made of nitrophenyl pentadien (NPPD) and luminol. (Spy Dust)

Spying. Under Article 106, UCMJ, in time of war, the act of clandestinely or under false pretences, collecting or attempting to collect, information with the intent to convey it to a hostile party. (AR 381-20, Army CI Program, 25 May 2010)

Like war, spying is dirty business. Shed of its alleged glory, a soldier's job is to kill.
Peel away the claptrap of espionage and the spy's job is to betray trust.
-- William Hood, *Mole* (1993)

_____

Spying is a major weapon in the state's exercise of power, according to Machiavelli. In his "Art of War.' He provides amazingly modern and sophisticated instructions on how to prevent spying by the enemy (counterintelligence), how to deceive the enemy (covert action), and how to learn its intentions (espionage).*
-- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006), p. 23
* Niccolo Machiavelli (1469-1527), Florentine statesman and patriot.

Spyware. Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a wide range of unwanted programs that exploit infected computers for commercial gain. They can deliver unsolicited pop-up advertisements, steal personal information (including financial information such as credit card numbers), monitor web-browsing activity for marketing purposes, or route HTTP requests to advertising sites. (McAfee.com; accessed 15 Nov 2010)

Stability Operations. An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Staff Judge Advocate (SJA). A judge advocate so designated in the Army, Air Force, or Marine Corps, and the principal legal advisor of a Navy, Coast Guard, or joint force command who is a judge advocate. (JP 1-04, Legal Support to Military Operations, 17 Aug 2011)

Stake Out. Stationary surveillance of a person, site, or facility. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

-- Also, stakeout: a surveillance point or location that has been employed (or laid out) with the benefit of prior planning. Usually meant to be occupied for an extended period of time. (Words of Intelligence, 2nd Edition, 2011)

Standard Operating Procedure (SOP). A set of instructions covering those features of operations which lend themselves to a definite or standardized procedure without loss of effectiveness. The procedure is applicable unless ordered otherwise. (JP 1-02 and JP 3-31,Command and Control for Joint Land Operations, 29 June 2010)

Star-Burst Maneuver. A countersurveillance ploy in which more than one target car or target officer is being followed and they suddenly go in different directions, forcing the surveillance team to make instant choices about whom to follow. (CI Centre Glossary)

Statement Analysis (also called Scientific Content Analysis or SCAN and Investigative Discourse Analysis). A technique for analyzing the words people use. Proponents claim this technique can be used to detect concealed information, missing information, and whether the information that person has provided is true or false. (Wikipedia, accessed 5 Mar 2014)

Station. A CIA operational center overseas… usually, but not always, located under cover in a U.S. official installation. The senior officer in charge of a station is known as the chief of station, or COS. (James M. Olson, *Fair Play: The Moral Dilemmas of Spying*, 2006)

Status of Forces Agreement (SOFA). An agreement that defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to the local law or to the authority of local officials. (JP 1-02 and JP 3-16, Multinational Operations, 7 Mar 2007)

-- Also, an accord, either bilateral or multilateral, that defines the legal position of a visiting military force deployed in the territory of a friendly state, usually delineating matters affecting the relationship between the military force and the civilian authorities and population. (AR 381-20, Army CI Program, 25 May 2010)

Stay Behind [aka sleeper]. Agent or agent organization established in a given country to be activated in the event of hostile overrun or other circumstances under which normal access would be denied. (JP 1-02)

Steganography. The art, science, and practice of communicating in a way that hides the existence of the communication. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, the process of hiding information by embedding messages within other, seemingly harmless messages. The process works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images. (US Army TRADOC DCSINT Handbook 1.02, 15 Aug 2007)

-- Also, the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. (Wikipedia; accessed 4 April 2011)

> *Steganography (from the Greek root "staganos," meaning covered or secret), or stego, is the technique of hiding data in a host file. […] Simply put, stego is hiding* a covert message within another file so that only the sender and receiver can access it.
>
> -- Eric Cole, "Steganography: More than Meets the Eye, " in *Information Security*, November 2006 (pp. 32-37)

Steganography is the process of secreting data in an image. Moscow Center uses steganographic software that is not commercially available. The software package permits the SVR clandestinely to insert encrypted data in images that are located on publicly-available websites without the data being visible. The encrypted data can be removed from the image, and then decrypted, using SVR-provided software. Similarly, SVR-provided software can also be used to encrypt data, and then clandestinely to embed the data in images on publicly-available websites.

-- FBI Affidavit, 25 June 2010

_____

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

With the advent of digital media, steganography has come to include the hiding of digital information within digital files. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

-- Wikipedia (accessed 4 April 2011)

_____

For additional information also see -- <http://www.steganographypro.com/> and <http://www.citi.umich.edu/u/provos/papers/practical.pdf>

Sterilize. To remove from material to be used in covert and clandestine actions any marks or devices which can identify it as originating with the sponsoring organization or nation. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Strategic Communication. Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. (JP 1-02)

Strategic Debriefing. Debriefing activity conducted to collect information or to verify previously collected information in response to national or theater level collection priorities. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; and Army FM 2-22.3, HUMINT Collector Operations, 6 Sep 2006)

Sources for strategic debriefing operations include but are not limited to émigrés, refugees, displaced persons, defectors, and selected U.S. personnel.

Strategic Intelligence. Intelligence required for the formation of policy and military plans at national and international levels. Strategic intelligence and tactical intelligence differ primarily in level of application, but may also vary in terms of scope and detail. (JP 1-02) Also see *intelligence; operational intelligence; tactical intelligence.*

Sherman Kent defined *strategic intelligence* as “high-level foreign positive intelligence.”

Strategic Intelligence Interrogation. An intelligence interrogation of any person who is in the custody or under the effective control of the DoD or under detention in a DoD facility, conducted at a theater-level detention facility. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013) Also see *intelligence interrogation*.

Strategic Level of War. The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, and then develops and uses national resources to achieve these objectives. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see also *operational level of war; tactical level of war.*

Strategic Mission Assurance Data System (SMADS). A classified geospatially enabled Critical Infrastructure database with the capability to analyze potential national, strategic, and operational impacts resulting from the loss or disruption of Critical Infrastructure and Key Resources (CIKR).

> Strongly recommended that all DoD CI personnel providing CI support to DCIP obtain an SMADS account.
>
> SMADS is a restricted database accessible on SIPRNet at: <https://smads.stratcom.smil.mil> Access is only granted to end-users who have a valid user account (requires valid need-to-know). Permissions are granted based upon a user's mission and associated responsibilities.
>
> SMADS is managed and maintained by the U.S Strategic Command (USTRATCOM) Mission Assurance Division (MAD). It is the current Joint Staff program of record for Critical Infrastructure and Key Resources (CIKR).
>
> Refer to the *SMADS User Manual* which serves as a general reference for end-users; it provides a step-by-step guide to performing web-enabled database tasks, while incorporating some DCIP program information to help facilitate the completion of these tasks.
>
> For other DCIP tools see web site at: <http://dcip.dtic.mil/DCIPtools.html>

Strategy. A prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

-- *Military Strategy*. The art and science of employing the armed forces of a nation to secure the objectives of national policy by the application of force or the threat of force. (JP 1-02)

-- *National Military Strategy*. The art and science of distributing and applying military power to attain national objectives in peace and war; also called NMS. (JP 1-02)

-- *National Strategy*. The art and science of developing and using the diplomatic, economic, and informational powers of a nation, together with its armed forces, during peace and war to secure national objectives; also called national security strategy or grand strategy. (JP 1-02)

Structured Analysis. A distinct form of intelligence analysis methodology that provides a step-by-step process for analyzing the kinds of incomplete, ambiguous, and sometimes deceptive information that analysts must deal with.

> Structured analysis is a mechanism by which internal thought processes are externalized in a systematic and transparent manner so that they can be shared, built on, and easily critiqued by others. Structured analysis helps analysts ensure that their analytical framework—the foundation upon which they form their analytical judgments—is as solid as possible.
>
> For in-depth information on structured analysis see Richards J. Heuer, Jr. and Randolph H. Pherson, *Structured Analytical Techniques for Intelligence Analysis* (Washington, DC; CQ Press, 2011).

Subject. Person, place, or thing observed or under investigation. (AFOSI Manual 71-142, OFCO, 9 Jun 2000) Also see *suspect.*

-- Also, a person about whom probable cause exists to believe that the person committed a particular criminal offense. (AR 195-2, Criminal Investigation Activities, 15 May 2009)

Subject Interview. Interview with the subject of an investigation; it may be non-custodial or custodial.

> *Interviews of subjects of CI investigations are conducted to afford subjects the opportunity to refute, explain, clarify or mitigate allegations of espionage, terrorism, and other acts that may constitute threats to national security.*
> -- AR 381-20, *Army CI Program*, 25 May 2010

Subversion. Actions designed to undermine the military, economic, psychological, or political strength or morale of a governing authority. (JP 1-02 and JP 3-24, Counterinsurgency, 22 Nov 2013) Also see *subversive activity*.

-- Also, actions designed to undermine the military, economic, political, psychological, or moral strength of a nation or entity. It can also apply to an undermining of a person's loyalty to a government or entity. (Senate Report 95-755, Book I – Glossary, 26 Apr 1976)

-- Also, actively encouraging military or civilian personnel to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, or discipline of the US military forces. Lending aid, comfort, and moral support to individuals, groups, or organizations that advocate the overthrow of the U.S. Government. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, the crime of creating a revolt, disturbance, or violence against lawful civil authority with the intent to cause its overthrow or destruction. (Dictionary.com)

> Subversion refers to an attempt to overthrow structures of authority, including the state. It is an overturning or uprooting. Subversive activity is the lending of aid, comfort, and moral support to individuals, groups, or organizations that advocate the overthrow of incumbent governments by force and violence. All willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage are placed in the category of subversive activity.
>
> _____
>
> *In the context of DoD investigative policy, subversion refers only to such conduct as is forbidden by the laws of the United States. Specifically, this is limited to information concerning the activities of individuals or groups that involve or will involve the violation of Federal law, for the purpose of:*
> *1) Overthrowing the Government of the United States or the government of a State; and*
> *2) Substantially impairing for the purpose of influencing U.S. Government policies or decisions.*
> -- DoD 5200.2-R, *Personnel Security Program*, Jan 1987 (w. chg 3), p.22

Subversion of Department of Defense Personnel. Actions designed to undermine the loyalty, morale, or discipline of DoD military and civilian personnel. (JP 1-02)

-- Also, [previously defined in DoDI 5240.06, 7 Aug 2004] an act or acts inciting military or civilian personnel of the DoD to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, [or] discipline, of the Military Forces of the United States.

> Criminal subversion of military forces is a violation of Title 18 USC, §§ 2384-2390.

Subversive Activity. Anyone lending aid, comfort, and moral support to individuals, groups or organizations that advocate the overthrow of incumbent governments by force and violence is subversive and is engaged in subversive activity. All willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage will be placed in the category of subversive activity. (JP 1-02)

Suitability Investigation. An inquiry into a person's identifiable character traits and conduct sufficient to decide whether an individual's employment or continued employment would or would not protect the integrity or promote the efficiency of the service. (ONCIX, http://www.ncix.gov/SEA/reform/secvssuit.php; accessed 18 Sep 2012) Also see *security clearance investigation*.

> "*The Director of the Office of Personnel Management shall serve as the Suitability Executive Agent. As the Suitability Executive Agent, the Director of the Office of Personnel Management will be responsible for developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of suitability and eligibility for logical and physical access."*
>
> -- EO 13467 (30 June 2008)

Superencryption. Process of encrypting encrypted information. Occurs when a message, encrypted off-line, is transmitted over a secured, on-line circuit, or when information encrypted by the originator is multiplexed onto a communications trunk, which is then bulk encrypted. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Supply Chain. The linked activities associated with providing materiel from a raw materiel stage to an end user as a finished product. (JP 1-02 and JP 4-09, Distribution Operations, 5 Feb 2010) Also see *adversarial supply chain operations, supply chain attack, supply chain risk, supply chain risk management*.

-- Also, the linked activities associated with providing materiel from a raw materiel stage to an end user as a finished product or system. Including design, manufacturing, production, packaging, handling, storage, transport, mission operation, maintenance, and disposal. (DoDI 4140.67, DoD Counterfeit Prevention Policy, 26 Apr 2013)

-- Also, organizations, people, technology, information and associated resources involved in moving a product or service from supplier to customer. (National Counterintelligence Strategy of the United States of America, 2012)

-- Also, a system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

> *Supply Chain: 1) Starting with unprocessed raw materials and ending with the final customer using the finished goods, the supply chain links many companies together; 2) the material and informational interchanges in the logistical process stretching from acquisition of raw materials to delivery of finished products to the end user. All vendors, service providers, and customers are links in the supply chain.*
>
> -- CSCMP Glossary, Feb 2010, p. 179
>
> See *Supply Chain Management Terms and Glossary*, Feb 2010. Available online at: <http://cscmp.org/sites/default/files/user_uploads/resources/downloads/glossary.pdf>

Supply Chain Attack. Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Supply Chain Risk. The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, otherwise degrade the function, use or operation of the item or system. (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 w/ chg 1 and DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012) Also see *supply chain risk management; supply chain risk mitigation; supply chain vulnerabilities.*

-- Also, the risk that adversaries will insert malicious code into or otherwise subvert the design, manufacturing, production, distribution, installation, or maintenance of ICT components that may be used in DoD systems to gain unauthorized access to data, to alter data, to disrupt operations, or to interrupt communications. (DTM 09-016, SCRM to Improve the Integrity of Components Used in DoD Systems, 25 Mar 2010 w/ chg 3 dated 23 Mar 2012)

"*The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system."*

-- The Ike Skelton National Defense Authorization Act for Fiscal Year 2011, (Section 806)

The increased dependence of the United States on global inputs in the manufacturing and service sectors, especially relating to information technology, opens the door to greater supply-chain vulnerabilities. As international companies and foreign individuals play a greater role in the information-technology supply chain, the specter of persistent, stealthy subversion is raised—particularly by foreign intelligence and military services, as well as international terrorists and criminal groups.

– ONCIX website <http://www.ncix.gov/sections/carc/index.html>

Within DoD, see DoDI 52400.44 (Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012) which establishes policy to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components by foreign intelligence, terrorists, or other hostile elements.

DoD computing systems, are a constant target of foreign exploitation. A 2007 Defense Science Board report noted that the software industry has become increasingly and irrevocably global. Much of the code is now written outside the United States, some in countries that may have interests inimical to those of the United States. The combination of DoD's profound and growing dependence upon software and the expanding opportunity for adversaries to introduce malicious code into this software has led to a growing risk to the Nation's defense.

See report of the *Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software*, Sep 2007.

"A computer chip with a hidden, malicious flaw could sabotage a weapons system. And the compromised hardware is almost impossible to detect…. A chip might even be embedded with a 'kill switch,' allowing the weapon to be disabled by remote control. …only about 2 percent of the integrated circuits purchased every year by the military are manufactured in the United States."

-- David Wise, *Tiger Trap: America's Secret Spy War with China* (2011), p. 233

"The Defense supply chain is at risk: More than two-thirds of electronics in U.S. advanced fighter aircraft are fabricated in off-shore foundries."

-- Dr. Kaigham J. Gabriel, Acting Director DARPA, DoD
March 2012 – Testimony before the Senate Armed Services Committee hearing on Emerging Threats and Capabilities

---

"Interdependence of information technologies and integration of foreign technology in US information technology, telecommunications, and energy sectors will increase the potential scope and impact of foreign intelligence and security services' supply chain operations. The likely continued consolidation of infrastructure suppliers—which means that critical infrastructures and networks will be built from a more limited set of provider and equipment options—will also increase the scope and impact of potential supply chain subversions."

-- James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Committee on Armed Services, 18 April 2013

Counterfeit Electronic Parts in the DoD Supply Chain…

"In March 2001, the Senate Armed Services Committee initiated an investigation into counterfeit electronic parts in the Department of Defense (DOD) supply chain. The investigation uncovered overwhelming evidence of large numbers of counterfeit parts making their way into critical defense systems. … The investigation… found overwhelming evidence that companies in China are the primary source of counterfeit electronic parts in the defense supply chain."

-- Armed Services U.S. Senate Report 112-167, 21 May 2012; copy of full report at: <http://www.armed-services.senate.gov/Publications/Counterfeit%20Electronic%20Parts.pdf>

Supply Chain Risk Management (SCRM). The management of supply chain risk whether presented by the supplier, the supplied product and its sub-components, or the supply chain (e.g., packaging, handling, storage, and transport). (DoDI O-5240.24, CI Activities Supporting RDA, 8 Jun 2011 with change 1 dated 15 Oct 2013) Also see *adversarial supply chain operations*, *supply chain attack*, *supply chain risk; supply chain risk mitigation; supply chain vulnerabilities.*

-- Also, the systematic identification, assessment, and quantification of potential supply chain disruptions with the objective to control exposure to risk or reduce its negative impact on supply chain performance.(DoDI 4140.01, DoD Supply Chain Materiel Management Policy, 14 Dec 2011)

-- Also, a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD's "supply chain" and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal). (DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012)

-- Also, management of risk that an adversary may sabotage, malicious[ly] introduce unwanted functions, or otherwise subvert the design, manufacturing, production, distribution, installation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, otherwise degrade the function, use or operation of the item or system. (DoD FCIP Strategy FY 2013-2017)

-- Also, [within the Intelligence Community] the management of risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain. It addresses the activities of foreign intelligence entities and other adversarial attempts aimed at compromising the IC supply chain, which may include the introduction of counterfeit or malicious items into the IC supply chain. (ICD 731, Supply Chain Risk Management, 7 Dec 2013)

Supply chain risk management encompasses many disciplines and requires participation from subject matter experts in acquisition, counterintelligence, information assurance, logistics, program offices, analysis, security, and other relevant functions as necessary.

-- ICD 731, Supply Chain Risk Management, 7 Dec 2013

The President's Comprehensive National Cybersecurity Initiative (CNCI) 11 directs the implementation of SCRM in information and communications technology (ICT) acquisition.

Various SCRM References:

National Strategy for Global Supply Chain Security, White House, Jan 2012; copy available at www.whitehouse.gov

Committee on National Security Systems Directive (CNSSD) No. 505, *Supply Chain Risk Management* (U), 7 Mar 2012; available at www.cnss.gov

For SCRM policy within the IC see Intelligence Community Directive (ICD) 701, *Supply Chain Risk Management*, 7 Dec 2013.

"Supply Chain Risk Management Awareness" by J. Filsinger, B. Fast, D. Wolf, et al; copy available at: <http://www.afcea.org/committees/cyber/documents/Supplychain.pdf>

Supply Chain Risk Mitigation. A process to ensure software and hardware commodity items are not compromised by malicious actions that disrupt or endanger military operations or provided an entry point for gaining access or control of DoD systems. (DoD Strategy for Operating in Cyberspace, May 2011) Also see *supply chain risk; supply chain risk management; supply chain risk vulnerabilities.*

> ***Manage Supply Risk*** *– Identify, assess, and prioritize efforts to manage risk by utilizing layered defenses, and adapting our security posture according to the changing security and operational environment.*
>
> -- White House, *National Startegy for Global Supply Chain Security*, Jan 2012, p.1

Supply Chain Vulnerabilities. An assessment of the supply chain related to CPI [critical program information] to determine if an adversary has the capability and intent to affect it in a manner that compromises the military effectiveness of the given platform, weapon system, or network. (DoDI 5200.39, CPI within the DoD,16 Jul 2008 with change 1 dated 28 Dec 2010) Also see *supply chain risk; supply chain risk mitigation; supply chain risk management*.

Supplier Assurance. Evidence demonstrating the level of confidence that a supplier is free from vulnerabilities. (DoDI 5200.39, CPI within the DoD,16 Jul 2008 with change 1 dated 28 Dec 2010)

Support Agent. An agent recruited to do support work, such as finding and living in safehouses, serving as a courier, or any of the other activities required to support a spy in place. In many cases, this support agent is a local citizen of the country in which the CIA operates. (A Spy's Journey)

Support Asset. An asset who acquires, maintains, and/or provides services. (HDI Lexicon, April 2008)

Supported Commander. 1) The commander having primary responsibility for all aspects of a task assigned by the Joint Strategic Capabilities Plan or other joint operation planning authority. 2) In the context of joint operation planning, the commander who prepares operation plans or operation orders in response to requirements of the Chairman of the Joint Chiefs of Staff. 3) In the context of a support command relationship, the commander who receives assistance from another commander's force or capabilities, and who is responsible for ensuring that the supporting commander understands the assistance required. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *support; supporting commander*.

Supporting Commander. 1) A commander who provides augmentation forces or other support to a supported commander or who develops a supporting plan. Includes the designated combatant commands and Defense agencies as appropriate. 2) In the context of a support command relationship, the commander who aids, protects, complements, or sustains another commander's force, and who is responsible for providing the assistance required by the supported commander. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *support; supported commander*.

Suspect Counterfeit. Materiel, items, or products in which there is an indication by visual inspection, testing, or other information that it may meet the definition of counterfeit materiel provided herein. (DoDI 4140.67, DoD Counterfeit Prevention Policy, 26 Apr 2013) Also see *counterfeit material*.

Surreptitious Entry. Entry by stealth. (Spycraft)

-- Also, unauthorized entry in a manner which leaves no readily discernible evidence. (DSS Glossary and AR 381-14, Technical Counterintelligence, 30 Sep 2002)

-- Also, any entry into a guarded or locked area or container and a departure therefrom without leaving a trace that such entry was made. (FM 30-17, Counterintelligence Operations, Jan 1972)

Surreptitious Entry Unit. Unit in OTS [CIA's Office of Technical Service] whose specialty was opening locks and gaining access to enemy installations for the purpose of supporting bugging operations. (Spy Dust)

Surveillance. The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *counter surveillance*, *electronic surveillance*, *physical surveillance, surveillance detection*.

> ***"Surveillance is a valuable investigative tool [emphasis added]…."***
>
> *"Investigators always should assume that subjects engaged in operational, terrorist, or criminal activity will attempt to detect surveillance by employing a variety of methods and techniques…. During surveillances, participants must remain vigilant and alert to the possibility of countersurveillance techniques being employed against them."*
>
> -- John T. Nason, "Conducting Surveillance Operations" in *FBI Law Enforcement Bulletin*, May 2004

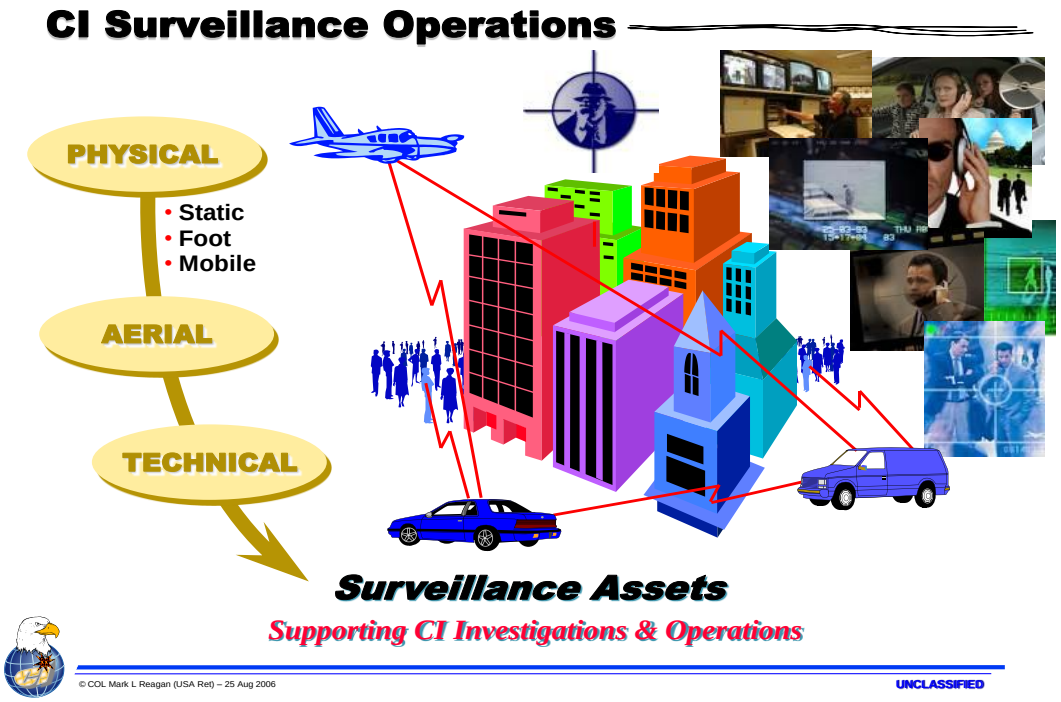
-- Also, systematic observation of a target. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

-- Also, the continuous watching or listening (overtly or covertly) of people, vehicles, places, or objects to obtain information concerning the activities and identities of individuals. (Peter Jenkins, *Surveillance Tradecraft: The Professional's Guide to Covert Surveillance Training*, 2010)

-- Also, the tradecraft of undetected observation. Surveillance can be physical, electronic, or acoustic. It may include audio or photographic observation and includes mail opening. (A Spy's Journey)

-- Also, actively but unobtrusively observing a subject to gather information about their activities and whereabouts. (Webster's New World Law Dictionary, 2010)

-- Also [as used within DoD concerning force protection], monitoring the activity of DoD personnel, facilities, processes, or systems including showing unusual interest in a facility, infrastructure, or personnel (e.g., observations through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit. (DTM 08-007, DoD Force Protection Threat Information, 22 Jul 2008)



Surveillance, by definition, is intrusion into the affairs of other people.
-- William R. Johnson, *Thwarting Enemies at Home and Abroad* (2009)

The word surveillance comes from the French *surveiller*, to watch over. The term is often used for all forms of observation or monitoring, not just visual observation.

In order to be effective, surveillance must go unnoticed and be undetected.

Surveillance can be used from a static point, on foot, from vehicle or by using technical devices. In most cases a combination of all four are used, with targets even often taking public transport and even attempting to detect or avoid surveillance.

-- Peter Jenkins in an introduction to *Surveillance Tradecraft* (2010)

Surveillance, physical: term for the universal tradecraft of undetected observation conducted by humans versus technical means.

Surveillance, technical: generic term for surveillance using various forms of visual, auditory and electronic aids in covering a designated target.

Surveillance, close: tradecraft jargon term for surveillance maintained where the prevention of loss of the subject is paramount.

Surveillance, discreet: tradecraft jargon term for surveillance maintained on a "loose" basis, the prevention of detection being paramount, even to the loss of the subject being tailed. Generally, the guiding rule is to discontinue surveillance rather than risk actions which make the subject aware of the surveillance.

Surveillance, fixed: tradecraft jargon term for a stationary or static surveillance. Also *stakeout*, tradecraft jargon for the static surveillance of a given target.

Surveillance, foot: tradecraft jargon term for, as the words imply, a surveillance conducted on foot.

Surveillance, mobile: tradecraft jargon term for surveillance conducted with the use of various mobile platforms, e.g., vehicles, aircraft, boats, etc.

-- Adapted from *The CIA's Insider's Dictionary* by Leo D. Carl (1996)

Surveillance… must be executed with maximum care lest its target become aware of it.
-- Allen W. Dulles, *The Craft of Intelligence* (2006), p. 124

Surveillance Detection. Measures taken to detect and/or verify whether an individual, vehicle, or location is under surveillance. (DoDI S-5240.15, FPRG, 20 Oct 2010 with change 1 dated 16 Oct 2013) Also see *counter surveillance*, *surveillance*.

-- Measures taken to determine if an individual is under surveillance. (HDI Lexicon, April 2008)

-- Also, self-initiated actions taken by a target/subject to identify surveillance. Conducted by taking advantage of screen and flow, couple with detailed route selection, and noting possible surveillance against time and distance relationships. (CI Community Lexicon)

Surveillance Detection Route (SDR). A carefully crafted route, of varying lengths and complexity depending on the operational environment, used by a case officer and/or agent to get to a meeting site, and after leaving the meeting site, [to] determine that the case officer and agent are not under surveillance before going to and after the ops meeting. (National HUMINT Glossary)

-- Also, a preplanned route used to determine if an individual is under surveillance. (HDI Lexicon, April 2008)

-- Also, a planned route taken by an agent or handler prior to conducting a clandestine act… designed to identify or elude surveillance. (Spycraft)

-- Also*, surveillance detection run*; a route designed to erode or flush out surveillance without alerting them to an operative's purpose. (CI Centre Glossary)

> *Professional case officers of all services, conduct lengthy SDRs before engaging in operational acts. A good SDR gives a case officer the opportunity to flush out surveillance if it is there and to make a determination of his or her surveillance status. The CIA jargon for completing an SDR and verifying without any doubt that surveillance is not there is "getting black."*
>
> -- James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (2006)
>
> _____
>
> *Case officers posted to Moscow station underwent rigorous training in "denied area tradecraft"… The primary discipline was the surveillance detection route (SDR). Case officers moved about on long and circuitous routes planned in advance while searching for KGB "tails." If they detected surveillance, they aborted their missions. If no surveillance was detected, they would "go black" for brief periods and perform operational acts.*
>
> -- Benjamin B. Fischer, "Spy Dust and Ghost Surveillance: How the KGB Spooked the CIA and Hid Aldrich Ames in Plain Sight," *International Journal of Intelligence and Counterintelligence*, Vol 24 No 2 (Summer 2011), p. 275
>
> _____
>
> See a brief discussion of "Surveillance Detection Runs" in an excellent article by Barry G. Royden, CIA, entitled "Tolkachev, A Worthy Successor to Penkovsky: An Exceptional Espionage Operation" originally classified SECRET and published in CIA's *Studies In Intelligence*, Vol. 41, No. 4. 1997. Later declassified and published in *Studies In Intelligence*, Vol 47, No. 3, 2003, Unclassified Edition; available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article02.html>

Surveillance Device. A piece of equipment or mechanism used to gain unauthorized access to and removal of information. (DoDI 5240.05, TSCM, 3 Apr 2014)

Suspect. A person about whom some credible information exists to believe that the person committed a particular criminal offense. (AR 195-2, Criminal Investigation Activities, 15 May 2009) Also see *subject*.

Susceptibility. The inherent capacity of an asset to be affected by one or more threats or Hazards. (DoDI 3020.45, DCIP Management, 21 Apr 2008)

Suspension of Access. The temporary withdrawal of a person's eligibility for access to classified information. Access is suspended when information becomes known that casts doubt on whether continued access is consistent with national security interests. (AR 380-67, Personnel Security Program, 24 Jan 2014)

Suspicious Activity. Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. (ISE-FS-200 v1.5 cited in DoDI 2000.26, SAR, 1 Nov 2011) See *suspicious activity report (SAR).*

Suspicious Activity Report (SAR). Official documentation of behavior that may be indicative of preoperational planning related to terrorism or criminal intentions. (DoDI 2000.12, DoD AT Program, 1 Mar 2013, w/ change 1 dated 9 Sep 2013)

-- Also, official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. (ISE-FS-200 v1.5 cited in DoDI 2000.26, SAR, 1 Nov 2011) See *suspicious activity*.

> **eGuardian** -- the FBI's law enforcement-centric threat reporting system -- rapidly disseminates SARs dealing with information regarding a potential threat or suspicious activity throughout the national law enforcement community to include DoD.

For DoD policy see DoDI 2000.26, *Suspicious Activity Reporting*, 1 Nov 2011.

Access to the eGuardian system is via Law Enforcement Online (LEO). Only DoD law enforcement personnel or analysts within DoD law enforcement organizations will enter SARs into the eGuardian system.

Categories of Suspicious Activity (see encl 4, DoDI 2000.26): Acquisition of Expertise; Breach or Attempted Intrusion; Eliciting Information; Expressed or Implied Threat; Flyover or Landing, Materials Acquisition or Storage; Misrepresentation; Recruiting; Sabotage, Tampering, or Vandalism; Surveillance; Testing of Security; Theft, Loss, or Diversion; Weapons Discovery; and Unexplained Absences of International Military Students.

Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting Version 1.5 (ISE-FS-200 v1.5) available on line at: <http://www.ise.gov/sites/default/files/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued_2009.pdf>

Suspicious Contact. Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country. (DSS Glossary)

Swallow. A female operative who uses sex as a tool. (Spy Dust)

The swallow's mission is to engage in sexual activity with the targeted person and gather the intelligence either through pillow talk or blackmail. In order to be able to blackmail the targeted person into disclosing secrets, the sexual activity usually takes place in a prearranged room or residence equipped with hidden cameras and recording devices.

-- *Encyclopedia of the Central Intelligence Agency* (2003)

A male operative who uses sex as a tool is referred to as a "Raven."

For additional open source information see David Lewis, *Sexpionage: The Exploitation of Sex by Soviet Intelligence* (1976).

Sweep. [Jargon] To electronically and/or physically examine a room or area in order to detect any clandestine devices; a search for "bugs," i.e., concealed electronic listening devices at a specific location. (Words of Intelligence, 2nd Edition, 2011)

Synchronization. 1) The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2) In the intelligence context, application of intelligence sources and methods in concert with the operation plan to ensure intelligence requirements are answered in time to influence the decisions they support. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

Synthesis. In intelligence usage, the examining and combining of processed information with other information and intelligence for final interpretation. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Systems Administrator (SA). Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

System Assurance. The justified measures of confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle. (DoDI 5200.39, CPI Protection within DoD, 16 Jul 2008 with change 1 dated 28 Dec 2010)

T ==========

Tactical Control (TACON). Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. TACON is inherent in operational control. TACON may be delegated to, and exercised at any level at or below the level of combatant command. When forces are transferred between combatant commands, the command relationship the gaining commander will exercise (and the losing commander will relinquish) over these forces must be specified by the Secretary of Defense. TACON provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. (JP 1, 25 Mar 2013 and JP 1-02) Also see *combatant command*; *combatant command (command authority)*; *operational control*.

Tactical Intelligence. Intelligence required for planning and conducting tactical operations. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Tactical Intelligence and Related Activities (TIARA). Those activities outside the National Foreign Intelligence Program that accomplish the following: 1) respond to operational commanders' tasking for time-sensitive information on foreign entities; 2) respond to national intelligence community tasking of systems whose primary mission is support to operating forces; 3) train personnel for intelligence duties; 4) provide an intelligence reserve; or 5) are devoted to research and development of intelligence or related capabilities. Specifically excluded are programs that are so closely integrated with a weapon system that their primary function is to provide immediate-use targeting data. (Previously in JP 1-02)

Tactical Level of War. The level of war at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011) Also see *operational level of war; strategic level of war*.

Tactical Questioning (TQ). The field-expedient initial questioning for information of immediate tactical value of a captured or detained person at or near the point of capture and before the individual is placed in a detention facility. Tactical questioning is generally performed by members of patrols, but can be done by any appropriately trained DoD personnel. Tactical questioning is limited to direct questioning. (DoDD 3115.09, DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning, 11 Oct 2012 w/ chg 1 dated 15 Nov 2013)

> For DoD policy see DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, 11 Oct 2012

-- Also, direct questioning by any Department of Defense personnel of a captured or detained person to obtain time-sensitive tactical intelligence, at or near the point of capture or detention and consistent with applicable law. (JP 1-02 and JP 3-63, Detainee Operations, 30 May 2008)

-- Also, expedient initial questioning for information of immediate tactical value. (Army FM 2-22.3, Human Intelligence Collector Operations, Sep 2006)

Tag. Something that is attached to the item to be located and/or tracked, which increases its ability to be detected or its probability of identification by a surveillance system suitably tuned to the tag. (Defense Science Board 2004 Summer Study, *Transition to and from Hostilities*, Dec 2004)

> Tags can be either active (such as radio-emitting tags) or passive (such as radio frequency identification [RFID] tags). Passive tags can also be chemical (such as infrared fluorescent) or biological in nature.

Task. A clearly defined action or activity specifically assigned to an individual or organization that must be done as it is imposed by an appropriate authority. (JP 1, 25 Mar 2013)

Task Critical Asset. An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD Components or DISLA organizations to execute the task or mission-essential task it supports. Task critical assets are used to identify defense critical assets. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

Target. 1) An entity or object considered for possible engagement or other action; 2) **in intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed…** [emphasis added] (JP 1-02 and JP 3-60)

-- Also, an individual, organization, or intelligence service against which intelligence operations are conducted. Also refers to documents or instruments which an intelligence service is trying to obtain, or the subject of a surveillance. (FBI FCI Terms)

Target Audience (TA). An individual or group selected for influence. (JP 1-02 and JP 3-13, Information Operations, 13 Feb 2006)

Target Folder. A folder, hardcopy or electronic, containing target intelligence and related materials prepared for planning and executing action against a specific target. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007)

Target Intelligence. Intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (JP 3-60, Joint Targeting, 13 Apr 2007)

Targeted Violence: Pre-conceived violence focused on individuals, groups, or locations where perpetrators are engaged in behaviors that precede and are related to their attacks. These perpetrators consider, plan and prepare before engaging in acts of violence and are often detectable, providing an opportunity for disruption of the intended violence. (DSB Report, *Predicting Violent Behavior*, Aug 2012)

"There is no panacea for stopping all targeted violence."

-- DSB Report, *Predicting Violent Behavior*, August 2012

Copy of Defense Science Board Report (DSB), *Predicting Violent Behavior*, Aug 2012 available at: <http://www.acq.osd.mil/dsb/reports/PredictingViolentBehavior.pdf> (accessed 10 Oct 2012)

Targeting. The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0, Joint Operations, 11 Aug 2011)

-- Also, the act of focusing on a country, organization, non-state actor, installation, system, or person to identify an operational or intelligence goal. (National HUMINT Glossary)

-- Also, the process of selecting targets and matching the appropriate response to them, including operational requirements and capabilities. The purpose of targeting is to disrupt, delay, or limit threat interference with friendly COAs [courses of actions]. (FM 2-22.2, Counterintelligence, Oct 2009)

CI support to the targeting process include the development of CI targets list to identify those FISS and ITO persons, organizations, facilities, or installations that must be exploited through raid and capture to gain additional intelligence or neutralization to disable or destroy, negate, mitigate, or degrade the adversary's ability to collect on U.S. forces.

-- FM 2.22-2, *Counterintelligence*, October 2009, p. 5-7

See JP 3-60, *Joint Targeting*, for additional information.

Note: The doctrinal targeting process that has been adopted by the Army is denoted by the acronym "D3A," which stands for "Decide, Deliver, Detect, and Assess" and is covered in-depth in FM 6-20-10, *Tactics, Techniques, and Procedures for the Targeting Process*, 8 May 1996.

TARP. Acronym for *Threat Awareness and Reporting Program*; see Army Regulation 381-12, TARP, 4 Oct 2012.

Task Asset. [In critical infrastructure usage] an asset that is directly used to support execution of one or more operations, tasks, activities, or mission essential tasks (METs). (DoDI 3020.45, DCIP Management, 21 Apr 2008) Also see *asset, defense critical asset, defense critical infrastructure program (DCIP), task critical asset*.

Task Critical Asset (TCA). An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD Components or DISLA organizations to execute the task or mission-essential task it supports. Task critical assets are used to identify defense critical assets. (DoDD 3020.40, Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012) Also see *asset, defense critical asset, defense critical infrastructure program (DCIP), task asset.*

Tier 1 - 3 Task Critical Assets

Tier 1 TCA. An asset the loss, incapacitation, or disruption of which could result in mission (or function) failure at the DoD, Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure sector level.

Tier 2 TCA. An asset the loss, incapacitation, or disruption of which could result in severe mission (or function) degradation at the DoD, Military Department, Combatant Command, subunified command, Defense Agency, or defense infrastructure sector level.

Tier 3 TCA. An asset the loss, incapacitation, or disruption of which could result in mission (or function) failure below the Military Department, Combatant Command, sub-unified command, Defense Agency, or defense infrastructure sector level.

-- DoDM 3020.45-Vol 1, *Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP),* 24 Oct 2008

Task Force Counterintelligence Coordinating Authority (TFCICA). An individual that affects the overall coordination of counterintelligence activities (in a joint force intelligence directorate counterintelligence and human intelligence staff element, joint task force configuration), with other supporting CI organizations, and supporting agencies to ensure full CI coverage of the task force operational area. (JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Tasking. Directing or requesting a source to perform in a specific manner to achieve an objective or conduct an activity. (DoDI S-5200.42, Defense HUMINT and Related Activities (U), 8 Dec 2009)

-- Also, the process associated with acceptance of a validated collection requirement and assigning it to organic collection assets for action. (DHE-M 3301.001, Vol I: Collection Requirement, Reporting, and Evaluation Procedures, 30 Jan 2009, w/ chg 2 dated 1 Feb 2012)

Tear Line. A physical line on an intelligence message or document separating categories of information that have been approved for foreign disclosure and release. (JP 2-0, Joint Intelligence, 22 Oct 2013) Also see *tearline reporting*.

The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with "need-to-know", need-to-release, and write-to-release principles and foreign disclosure guidelines of the information below the tear line.

-- Also, a physical line on an intelligence message or document separating categories of information that have been approved for foreign disclosure and release. Normally, the intelligence below the tear line is that which has been previously cleared for disclosure or release. (DoDI S-5240.17, CI Collection Activities, 14 Mar 2014)

Tearline Reporting. An automated or manual technique for separating an intelligence report into multiple portions separated by machine-or human-readable tearlines. A tearline section is the area in an intelligence report or finished intelligence product where the sanitized version of a more highly classified and/or controlled report is located. The sanitized information within the tearlines contains the substance of the more detailed information without identifying the sensitive sources and methods, allowing wider dissemination of substantive intelligence information to authorized users. (ICD 206, 17 Oct 2007) Also see *tear line*.

Also see ICD 209, *Tearline Production and Dissemination*, 6 Sep 2012

Technical Counterintelligence (TCI). A component of counterintelligence technical services. TCI includes Technical Surveillance Countermeasures (TSCM) and the investigation, study, and control of compromising emanations from information systems, known as TEMPEST. Also see *technical penetration, Technical Surveillance Countermeasures, TEMPEST.*

The essence of technical counterintelligence collection is learning through technical means what foreign intelligence services see, hear, and sense, what they know about one's own technical means, and how they are using this information.

-- Roy Godson, *Dirty Tricks or Trump Cards: US Covert Action and Counterintelligence* (1995), p. 224

Technical Counterintelligence (TCI) Countermeasures. Any action, device, procedure, technique, or other measure that reduces the vulnerability of any equipment or facility that electronically processes information to technical exploitation of classified and/or sensitive information. (AR 381-14, Technical Counterintelligence [U], 30 Sep 2002)

Technical Intelligence (TECHINT). Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. (JP 1-02 and JP 2-0, Joint Intelligence, 22 Oct 2013)

-- Also, the identification, assessment, collection, exploitation, and evacuation of captured enemy materiel (CEM) in support of national and immediate technical intelligence requirements. TECHINT provides rapid performance and vulnerability assessments of enemy equipment, giving a critical edge to US forces in current and future operations. (Army FM 2-22.401, TECHINT, 9 Jun 2006)

Technical Hazard. An insecure condition that could permit the technical exploitation of an area with classified national security information, restricted data, and/or unclassified information requiring protection. (AR 381-14, Technical Counterintelligence, 30 Sep 2002)

Technical Penetration. The use of technological means to conduct an intentional, unauthorized interception of information-bearing energy. (DoDI 5240.05, TSCM Program, 22 Feb 2006)

-- Also, a deliberate, unauthorized, clandestine emplacement of a device or modification of existing government equipment, or the clandestine employment of a technique, which allows the technical monitoring within an area for the purpose of gaining information. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, *technical penetrations* include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected. (Previously in JP 2-01.2, CI & HUMINT Support to Joint Operations, 13 Jun 2006)

> *"…[I]t had been my experience that the most up-to-snuff secret audio and other clandestine monitoring techniques always seemed to be a step ahead of the counter-surveillance teams."*
> -- Richard Helms with William Hood, *A Look Over My Shoulder* (2003), p. 449

Technical Security. A security discipline dedicated to detecting, neutralizing, and/or exploiting a wide variety of hostile and foreign penetration technologies. This discipline mandates training in various countermeasure techniques. (IC Standard 700-1, 4 Apr 2008)

Technical Services. The investigative use of video surveillance and interception of oral, electronic and wire communications. (AFPD 71-1, Criminal Investigations and Counterintelligence, 1 Jul 1999)

Technical Surveillance. The use of optical, audio, or electronic monitoring devices or systems to surreptitiously collect information. (DoDI 5240.05, TSCM, 3 Apr 2014)

-- Also, surveillance accomplished through the use of electronic listening devices, vehicle trackers, and signaling devices. (CI Community Lexicon)

Technical Surveillance Countermeasures (TSCM). Techniques to detect, neutralize, and exploit technical surveillance technologies and hazards that permit the unauthorized access to or removal of information. (DoDI 5240.05, TSCM Program, 3 Apr 2014)

-- Also, techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

-- Also, physical, electronic, and visual techniques used to detect and counter technical security devices, technical security hazards, and related physical security deficiencies. (IC Standard 700-1, 4 Apr 2008)

Long history of adversary technical surveillance collection and exploitation of sensitive U.S. facilities and activities…

"*In 1944, the very first TSCM sweep uncovered 120 microphones in the Moscow Embassy* [U.S. Embassy in Moscow]."
-- Frederick L. Wettering, "Counterintelligence: The Broken Triad." *International Journal of Intelligence and Counterintelligence* 13 (Fall 2000), pp. 265-299.

TSCM identifies technically exploitable conditions and provides strategies to mitigate or remove them.

TSCM represents the convergence of two distinct disciplines -- counterintelligence and security countermeasures. These techniques and countermeasures are designed to detect and nullify a wide variety of technologies used to gain unauthorized access to classified national security information, restricted data, or otherwise sensitive information.

-- ICD 702, *TSCM,* 18 Feb 2008

TSCM involves the search for technical surveillance devices or "bugs." …[T]he overwhelming number of technical attacks against US interests occur overseas. … Scare resources should be directed both to specific threat-driven inspections and to the maintenance of an R&D and training effort,

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, p. 61

The TSCM Program includes four separate functions: detection, nullification, isolation, and education.

-- FM 2-22.2, *Counterintelligence*, October 2009, p. 6-5;
also AR 381-14, *Technical Counterintelligence (TCI)* (U), 30 Sep 2002, p. 7

TSCM: the systematic physical and electronic examination of a designated area by properly trained, qualified and equipped persons in an attempt to discover electronic eavesdropping devices, security hazards or security weaknesses.

-- www.dbugman.com

PROJECT GUNMAN

A most spectacular case of electronic espionage occurred in the 1980s, at the height of the Cold War, when it was discovered that Soviet intelligence had successfully implanted very sophisticated bugs in a large number of electronic typewriters at the U.S. embassy in Moscow. On 25 March 1985, the story of the Soviet bug of U.S. typewriters in the Moscow Embassy broke on the CBS nightly news.

For detailed information see Sharon A. Maneki, *Learning From the Enemy: The GUNMAN Project*, NSA, 2012, 35 pages. Available on line at: http://www.nsa.gov/about/_files/cryptologic_heritage/center_crypt_history/ publications/Learning_From_the_Enemy_The_GUNMAN_Project.pdf

Technical Surveillance Device (TSD). A device covertly installed to monitor (visually, audibly, or electronically) sensitive activities and/or information processing within a target area. (ICS Glossary)

Technical Threat Analysis. A continual process of compiling and examining information on technical surveillance activities against personnel, information, operations, and resources. (DoDI 5240.05, TSCM Program, 3 Apr 2014)

Technology. The application of scientific and technical information and know-how to design, produce, manufacture, use, adapt, reconstruct, or reverse-engineer goods. This includes technical information and data in all forms, including electronic form. The term does not include the goods themselves, nor does it include scientific information in the public domain. (DoDI 2040.02, International Transfers of Technology, Articles, and Services, 10 Jul 2008) Also see *critical technology*.

Technology Readiness Level (TRL). A standard utilized in the scientific community to track the maturity of a technology. The readiness level is depicted on a numerical scale form one to nine, where one represents the initial idea stage and nine represents the final fielding and utilization of the technology. (DoD FCIP Strategy FY 2013-017)

Technology Targeting Risk Assessment (TTRA). A country-by-country assessment conducted by the Defense Intelligence Community that quantifies risks to CPI [critical program information] and related enabling technologies for weapons systems, advanced technologies or programs, and facilities such as laboratories, factories, research and development sites (test ranges, etc.), and military installations. The TTRA evaluates five independent risk factors, each of which contributes to an overall risk factor. The five areas evaluated are: Technology Competence, National Level of Interest, Risk of Technology Diversion, Ability to Assimilate, and Technology Protection Risk. (DoDI 5200.39, CPI within DoD, 16 Jul 2008 with change 1 dated 28 Dec 2010)

> The TTRA and CI Assessment provide laboratory/technical directors and Program Managers with information required to establish a comprehensive security program for the protection of identified critical program information (CPI).

Technology Transfer. The intentional communication (sharing) of knowledge, expertise, facilities, equipment, and other resources for application to military and nonmilitary systems. (DoDI 5535.8, DoD Technology Transfer Program, 14 May 1999)

-- Also, transferring, exporting, or disclosing defense articles, defense services, or defense technical data covered by the United States Munitions List (USML) to any foreign person or entity in the United States (U.S.) or abroad. (DSS Glossary)

Telecommunications and Information Systems Security. Protection afforded to telecommunications and information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security material and technical security information. (National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems, 5 Jul 1990)

> Copy of NSD 42 available at: <http://www.fas.org/irp/offdocs/nsd/nsd42.pdf>

TEMPEST. An unclassified term referring to technical investigations for compromising emanations from electrically operated information processing equipment; these investigations are conducted in support of emanations and emissions security. (JP 1-02) Also see *compromising emanations; TEMPEST Test.*

-- Also, an unclassified term that refers to the investigation and study of compromising emanations. (IC Standard 700-1, 4 Apr 2008)

-- Also, a name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, Transient Electro Magnetic Pulse Emanation Standard (TEMPEST) the investigation, study, and control of compromising emanations from telecommunication and automated information systems equipment. (Defense HUMINT Enterprise Manual 3301.002, Vol II Collection Operations, 23 Nov 2010)

-- Also, the evaluation and control of compromising emanations from telecommunications and automated information systems. TEMPEST countermeasures are designed to prevent FISS and ITO [international terrorist organization] exploitation of compromising emanations by containing them within the space of the equipment or facility processing classified information. (Army FM 2-22.2, CI, Oct 2009)

-- An unclassified term referring to technical investigations for compromising emanations from electrically operated, information processing equipment; they are conducted in support of emanations and emission security. (ICS Glossary, Jun 1989)

TEMPEST – the problem of compromising radiation. Any time a machine is used to process classified information electrically… that machine may emit radio frequency or acoustic energy. These emissions, like tiny radio beacons, may radiate through free space for considerable distances…. Or they may be induced on nearby conductors like signal lines, power lines, telephones lines, or waste pipes and be conducted along those paths for some distance…. When these emissions can be intercepted and recorded, it is frequently possible to analyze them and recover the intelligence that was processed by the source equipment. The phenomenon affects not only cipher machines buy any information-processing equipment—teletypewriters, duplicating equipment, intercoms, facsimile, computers.…

-- Source: NSA, *TEMPEST: A Signal Problem*, undated [declassified/redacted version]
see <www.nsa.gov/public/crypt-spectrum.cfm>
also at: http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf

---

TEMPEST (an acronym for Transient Electromagnetic Pulse Emanation Standard) is both a specification for equipment and a term used to describe the process for preventing compromising emanations. The fact that electronic equipment such as computers, printers, and electronic typewriters give off electromagnetic emanations has long been a concern of the US Government. An attacker using off-the-shelf equipment can monitor and retrieve classified or sensitive information as it is being processed without the user being aware that a loss is occurring. …

Given the absence of a domestic threat, any use of TEMPEST countermeasures within the US should require strong justification.

[TEMPEST] ***attacks require a high level of expertise, proximity to the target, and considerable collection time.*** [emphasis added]

The commission recognizes the need for an active overseas TEMPEST program but believes the domestic threat is minimal.

-- Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director Central Intelligence*, 28 Feb 1994, pp. 60-61

According to a declassified NSA publication: *"There is no special meaning in the word 'TEMPEST.' It was simply picked from a covername list by a NSA engineer in the early 1950s. However, TEMPEST has now become a generic word used throughout the US Government and industry to describe the unintentional emanation of classified information from an equipment."*

-- NSA, *Crypotolog*, Nov 1983 [declassified], p. 1

For a history of TEMPEST see declassified NSA publication, *A History of U.S. Communications Security (U),* [Vol I], revised July 1973, pp. 89-101; covers the timeframe through 1972.

This NSA report identified the main TEMPEST countermeasures as: "low-level keying, shielding, filtering, grounding, isolation, and physical protective measures." It also highlighted that shielded enclosures "provided not only the best means, but the only means we had come across to provide really complete TEMPEST protection in those environments where a large-scale intercept effort could be mounted at close range."

TEMPEST Test. A laboratory or on site (field) test to determine the nature and amplitude of conducted or radiated signals containing compromising information. (NSTISSI 7002, TEMPEST Glossary, 17 Mar 1995) Also see *compromising emanations; TEMPEST.*

Temporary Refuge. Protection afforded for humanitarian reasons to a foreign national in a DoD shore installation, facility, or military vessel within the territorial jurisdiction of a foreign nation or in international waters, under conditions of urgency in order to secure the life or safety of that person against imminent danger, such as pursuit by a mob. (DoDI 2000.11, Procedures for Handling Requests for Asylum and Temporary Refuge, 13 May 2010)

Terrorism. The unlawful use of violence or threat of unlawful violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010) Also see *homegrown terrorist, radicalization, violent extremism, violent radicalization.*

> ***There is no universally accepted definition of terrorism.***
> ***It remains the subject of continuing debate in international bodies.***
> -- Lord Carlile of Berriew Q.C. (March 2007)

-- Also, premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents (22 USC §2656f(d) and the National Strategy for Combating Terrorism, Feb 2003) [Definition used by Department of State, NCTC and CIA].

-- Also, the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (28 CFR §0.85) [Definition used by FBI, which reflects its mission, identifying a terrorist incident as a violation of the criminal laws of the United States and a suspected terrorist would, therefore, be subject to arrest and prosecution.]

-- Also, [the federal crime of terrorism] an offense that is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct. This includes terrorist acts committed within and outside U.S. national boundaries. (18 USC §2332b(g)(5)(A)).

-- Also, violent or illegal action taken on the basis of radical or extremist beliefs. (CRS Report R42553, Countering Violent Extremism in The United States, 19 Feb 2014)

> The Federal Bureau of Investigation (FBI) is the lead agency for investigating the federal crime of terrorism. If another federal agency identifies an individual who is engaged in terrorist activities or in acts in preparation of terrorist activities, the other agency is required to promptly notify the FBI. The extraterritorial jurisdiction for terrorism crimes is specified in 18 U.S.C. 2332b(e) and (f).
>
> Pursuant to 28 C.F.R. 0.85(1), the Attorney General has assigned responsibility to the Director of the FBI to "Exercise Lead Agency responsibility in investigating all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States. Within the United States, this would include the collection, coordination, analysis, management and dissemination of intelligence and criminal information as appropriate."
> -- Congressional Research Service (CRS) Report R41780, 27 Apr 2011
>
> ---
>
> For additional information on terrorism, see US Army TRADOC G2 Handbook No.1, *A Military Guide to Terrorism in the Twenty-First Century*, 15 Aug 2007.
> Copy available at: <http://www.fas.org/irp/threat/terrorism/>

Terrorism Threat Assessment. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat; [or] the product of a threat analysis for a particular unit, installation, or activity. (DoDI 2000.16, DoD Antiterrorism Standards, 2 Oct 2006)

Terrorist. One that engages in acts or an act of terrorism. (answer.com; accessed 27 October 2011)

> *Terrorists undertake criminal acts that involve the use or threat of violence against innocent persons. These acts are premeditated, intended to achieve a political objective through coercion or intimidation of an audience beyond the immediate victims.*
> – National Security Decision Directive 207, *The National Program for Combating Terrorism* (U), originally TOP SECRET, declassified

> Note: *Within DoD; None -- the term "terrorist" removed from JP 1-02.* Previously defined in JP 3-26, Counterterrorism (13 Nov 2009) as "those who commit acts of terrorism."

Terrorist Extremist. An extremist that uses terrorism -- the purposeful targeting of ordinary people -- to produce fear to coerce or intimidate governments or societies in the pursuit of political, religious, or ideological goals. Extremists use terrorism to impede and undermine political progress, economic prosperity, the security and stability of the international state system, and the future of civil society. (National Military Support Plan - War on Terrorism, 1 Feb 2006)

Terrorist Group. Any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of terrorism.

> Current list of Foreign Terrorist Organizations (FTOs) at US Department of State web site: <http://www.state.gov/s/ct/rls/other/des/123085.htm>

Terrorist Identities Datamart Environment (TIDE). The U.S. Government's (USG) central repository of information on international terrorist identities. TIDE supports the USG's various terrorist screening systems or "watchlists" and the US Intelligence Community's overall counterterrorism mission. (NCTC)

> *The TIDE database includes, to the extent permitted by law, all information the USG possesses related to the identities of individuals known or appropriately suspected to be or to have been involved in activities constituting, in preparation for, in aid of, or related to terrorism (with the exception of purely domestic terrorism information). This information is available to counterterrorism professionals throughout the Intelligence Community, including the Department of Defense, via the web-based, read-only "TIDE Online."*
>
> -- NCTC Fact Sheet at <http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf>

Terrorism Screening Center (TSC). A multi-agency center administered by the FBI with support from the Department of Homeland Security, the Department of State, the Department of Justice, the Department of Defense, the Department of the Treasury, and the Office of the Director of National Intelligence. The TSC maintains the U.S. government's consolidated Terrorist Watchlist—a single database of identifying information about those known or reasonably suspected of being involved in terrorist activity. (fbi.gov)

> The TSC was created by HSPD-6 (16 Sep 2003) to consolidate the USG's approach to terrorist screening by creating a single comprehensive database of known or appropriately suspected terrorists (KSTs), and to make the information from this consolidated list available to foreign, federal, state, local, territorial, tribal, regulatory and private sector entities through the TSC's 24/7 Terrorist Screening Operations Center (TSOC).
>
> For additional information see FBI web site at: <http://www.fbi.gov/about-us/nsb/tsc>

Terrorist Screening Database (TSDB). Under Homeland Security Presidential Directive-6, the TSDB is the master terrorist watchlist, for both international and domestic terrorists, maintained by the Terrorist Screening Center (TSC) for the U.S. Government.

Terrorist Threat. An expression of intention, by an individual or group, to commit an act or acts of violence to inflict injury or damage in pursuit of political, religious, or ideological objectives. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012, w/ change 1 dated 9 Sep 2013)

> *Terrorist threats emanate from a diverse array of terrorist actors, ranging from formal groups to homegrown violent extremists (HVEs) and ad hoc, foreign-based actors.*
>
> *US-based extremists will likely continue to pose the most frequent threat to the US Homeland.*
>
> -- DNI, Worldwide Threat Assessment of the US Intelligence Community, SSCI, 29 January 2014, p. 4

Terrorists with Global Reach – Transnational Terrorists. Terrorist organizations with an operational and support network in multiple countries that possess the capability to recruit, plan, resource, and execute terrorist acts worldwide. (National Military Support Plan - War on Terrorism, 1 Feb 2006)

TFCICA. See *Task Force Counterintelligence Coordinating Authority*.

Theater. The geographical area for which a commander of a geographic combatant command has been assigned responsibility. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02)

Theater Clearance. Clearance for official travel within a geographic combatant command area of responsibility granted by the responsible geographic combatant commander or other delegated authority. (DoDD 4500.54E, DoD Foreign Clearance Program, 28 Dec 2009)

Theater of War. Defined by the Secretary of Defense or the geographic combatant commander, the area of air, land, and water that is, or may become, directly involved in the conduct of the war. A theater of war does not normally encompass the geographic combatant commander's entire area of responsibility and may contain more than one theater of operations. (JP 1-02)

Theater Strategy. An overarching construct outlining a combatant commander's vision for integrating and synchronizing military activities and operations with the other instruments of national power in order to achieve national strategic objectives. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Thermal Imagery. Imagery produced by sensing and recording the thermal energy emitted or reflected from the objects which are imaged. (JP 1-02)

Third Agency Rule. An agreement among the US Government agencies participating in the exchange of intelligence data forbidding one agency to disseminate to another agency information which originated with a third agency. (National HUMINT Glossary)

-- Also, the tenet that information, usually classified or sensitive, originating in one U.S. agency not be disseminated by another agency to which the information has not been made available without the consent of the originating agency. (AR 381-20, Army CI Program, 25 May 2010)

Threat. The intention and capability of an adversary to undertake actions that would be detrimental to the interest of the U.S. (IC Standard 700-1, 4 Apr 2008)

-- Also, the sum of the potential strengths, capabilities, and strategic objectives of any adversary that can limit or negate U.S. mission accomplishment or reduce force, system, or equipment effectiveness. (DoDD 5200.1-M, Acquisition Systems Protection Program, March 1994)

-- Also, an adversary having the intent, capability, and opportunity to cause loss or damage. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, the perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, (1) A source of unacceptable risk; or (2) The capability of an adversary coupled with the adversary's intention to undertake actions that would be detrimental to the success of certain activities or operations. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, the capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operations. (IOSS OPSEC Glossary of Terms, 27 Aug 2003)

-- Also, any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland. (ADRP 3-0, Unified Land Operations, May 2012)

-- Also see *threat to national security; transnational threat; foreign intelligence collection threat; insider threat.*

Threat Advisory. An advisory is a one-time product or produced on a recurring schedule – daily, weekly, or monthly. The advisory informs authorized recipients of an immediate or the potential for a foreign intelligence or terrorist threat. The advisory typically contains information of a perishable nature. (DoDI 5240.18, CI Analysis & Production, 17 Nov 2009 with change 1 dated 15 Oct 2013)

> A threat advisory is distinguishable from an assessment and an analysis report in that it is prepared when there is an imminent or near-term intelligence or terrorist threat. A threat advisory often contains perishable information with only limited study or research conducted prior to publication.

Threat Analysis. a process that examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities. (DoDM 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

-- Also, *terrorism threat analysis*, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target the DoD Components or DoD elements and personnel. A threat analysis shall review the factors of a terrorist group's operational capability, intentions, activity, and the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013; also JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

Threat Assessment. A resultant product of the defined process used to conduct a threat analysis and develop an evaluation of a potential threat. Also, it is the product of a threat analysis for a particular unit, installation, or activity. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, *DCIP Threat Assessment*: [in Defense Critical Infrastructure Protection usage] a compilation of strategic intelligence information incorporating multi-faceted threats facing DCAs [Defense Critical Assets] and Tier 1 TCAs [Task Critical Assets]. DCIP threat assessments address threats posed to DCAs [and Tier 1 TCAs] from domestic and transnational terrorist elements, foreign intelligence and security services, and weapons of mass destruction. (DoDI 5240.19, CI Support to the Defense Critical Infrastructure Program, 31 Jan 2014)

-- Also, an evaluation of the current or projected capability of a foreign intelligence service or international terrorist group to limit, neutralize, or negate the effectiveness of a friendly mission, organization, or material item through multidisciplined intelligence collection, espionage, or sabotage. (AR 381-20, Army CI Program, 25 May 2010)

-- Also, in antiterrorism, examining the capabilities, intentions, and activities, past and present, of terrorist organizations as well as the security environment within which friendly forces operate to determine the level of threat. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

-- Also, [in antiterrorism usage] the process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat; the product of a threat analysis for a particular unit, installation, or activity. (DoDI 2000.12, DoD Antiterrorism Program, 1 Mar 2012 with change 1 dated 9 Sep 2013)

Threat Finance. The covert movement of the profits of illicit acts or of funds that will support illicit acts. (*A Guide to Counter Threat Finance Intelligence* by Marilyn B. Peterson, 2009) Also see *counter threat finance (CTF).*

> ***The covert movement of money is the underlying facilitator of all threat activity.***
>
> Within DoD, see DoDD 5205.14, *DoD Counter Threat Finance Policy*, 19 Aug 2010 (w/ chg1 dated 16 Nov 2012)

Threat Indicator. Any observable action that displays violent behavior, abnormal disgruntlement, radicalization, or an extreme world view on religion or another type of ideology. (US Army, Asymmetric Warfare Group, Insider Threats in Partnering Environments: *A Guide for Military Leaders*, Jun 2011)

Copy of reference available at: <https://rdl.train.army.mil/catalog/go/100.ATSC/883A3A74-A803-4CD5-B693-0D59B108E7EC-1326399638300>

Reference also at: <http://www.wired.com/images_blogs/dangerroom/2012/10/awsc-pdf-CDR-72811.pdf>

Threat Warning. The urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources. (JP 1-02 and JP 2-01, Joint and National Intelligence Support to Military Operations, 5 Jan 2012)

Threats to the National Security. International terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or a successor order. (FBI, Domestic Investigations and Operations Guide, 15 Oct 2011)

Time Bomb. Resident computer program that triggers an unauthorized act at a predefined time. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Time-Sensitive Collection Requirement (TSCR). A HUMINT collection requirement (HCR) needing immediate or time-specific action. Those organizations tasked with the time sensitive collection requirement should provide initial intelligence reports or a report stating an inability to collect on the requirement with 48 hours of issuance. (DHE-M 3301.002, Vol II Collection Operations, 23 Nov 2010)

Tosses (hand, vehicular) [e.g., hand toss, car toss]. Tradecraft techniques for placing drops by tossing them while on the move. (CI Centre Glossary)

Traces. The product resulting from a name check. (AFOSI Instruction 71-101, 6 Jun 2000)

Tracking. Precise and continuous position-finding of targets by radar, optical, or other means. (JP 1-02 and JP 3-07.4, Joint Counterdrug Operations, 13 Jun 2007)

Tradecraft. Specialized methods and equipment used in the organization and activity of intelligence organizations, especially techniques and methods for handling communications with agents. Operational practices and skills used in the performance of intelligence related duties. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; DoDI S-5240.17, CI Collection Activities, 14 Mar 2014; and CI Community Lexicon)

Tradecraft

The methods of the clandestine operator…
Principles and techniques of clandestine operations

Successful espionage is impossible without good tradecraft

In general, tradecraft is the sum total of the skills the Case Officer or agent must master in order to securely operate in the field and preserve security of operational activity.

_____

"Tradecraft is an art—a combination of common sense and imagination…. [T]he art of tradecraft, the methods employed to mange an intelligence operation. It is an art because of the nuances involved and it is not easy to learn. Some, lacking the personality traits, can never master it."

-- Richard L. Holm, The Craft We Chose (2011), pp 25 and 275

_____

The techniques adopted by spies to conceal their activities are lumped together under the catch-all term "tradecraft." It refers to a vast range of protective measures devised to preserve the operational security of spying.

-- Frederick P. Hitz (Former CIA IG 1990-1998), *The Great Game* (2005)

Pillars of Tradecraft: *assessment; cover and disguise; concealments; clandestine surveillance; and covert communications*.

-- *Spycraft* (p. 363)

[T]he greatest danger… lay not in betrayal by a Soviet mole, as Angleton would have it, but by simple mistakes in tradecraft and a failure to maintain proper compartmentation of information.

-- Benjamin Weiser, *A Secret Life* (2004)

"The spy who does not take tradecraft seriously is unlikely to remain a spy for very long."

-- H.H.A. Cooper and Lawrence J. Redlinger, *Making Spies: A Talent Spotter's Handbook*

-- Also, the art, discipline and methodology of conducting secure clandestine operations and intelligence collection. (National HUMINT Glossary)

-- Also, the tactics, techniques, and procedures used in executing HUMINT, counterintelligence, or related activities to obscure, protect, or otherwise frustrate detection. (HDI Lexicon, April 2008)

-- Also, specialized techniques used in intelligence operations. (FBI FCI Terms)

-- Also, the techniques, technology, and methodologies used in covert intelligence operations. Tradecraft applies to both the procedures, such as surveillance detection routes, as well as the use of devices in covert audio and agent communications. (Spycraft)

-- Also, the art, methodology, and know-how of conducting clandestine operations and intelligence collection techniques. Includes such things as dead drops, covert communications, how to recruit agents, secret writing and photography, surveillance, and surveillance detection. (A Spy's Journey)

-- Also, the essential skills required to conduct successful clandestine operations. (Encyclopedia of Cold War Espionage, Spies, and Secret Operations, 3rd edition, 2012)

-- Also, the techniques of the espionage trade, or the methods by which an agency involved in espionage conducts its business. Elements of tradecraft, in general terms, include the ways in which an intelligence officer arranges to make contact with an agent, the means by which the agent passes on information to the officer, the method for paying the agent, and the many precautions and tactics of deception applied along the way. (<http://www.espionageinfo.com/Te-Uk/Tradecraft.html>)

Tradecraft - Analytical. The term "tradecraft" usually applied to espionage techniques, but there is also *analytical tradecraft*: techniques, methods, and standards of the practice of analysis, e.g., framing questions, marshaling evidence, making concise arguments, identifying intelligence gaps, etc. Analytical tradecraft affords some criteria by which to judge analytical products and analysts.

Transmission Security. The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (JP 1-02 and JP 6-0, Joint Communications, 10 Jun 2010) Also see *communications security*.

Transnational Threat. Any transnational activity (including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery for such weapons, and organized crime) that threatens the national security of the United States. (50 USC §401a)

-- Also, any activity, individual, or group not tied to a particular country or region that operates across international boundaries and threatens United States national security or interests. (JP 1-02 and JP 3-26, Counterterrorism, 13 Nov 2009)

> DoD further defines a *transnational threat* as any activity, individual, or group not tied to a particular country or region that operates across international boundaries and threatens US national security or interests. These threats also include extremists who enter into convenient relationships that exploit each others' capabilities and cloud the distinction between crime and terrorism (e.g., violent extremist organizations and opportunists, drug trafficking organizations, transnational criminal organizations [TCOs], and those trafficking in persons).
>
> Lawless and subversive organizations can take advantage of failed states, contested spaces, and ungoverned areas by forging alliances with corrupt government officials and some foreign intelligence services, further destabilizing political, financial, and security institutions in fragile states, undermining competition in world strategic markets, using cyberspace technologies and other methods to perpetrate sophisticated frauds, creating the potential for the transfer of WMD to terrorists, and expanding narco-trafficking and human and weapons smuggling networks.
>
> -- JP 3-27, Homeland Defense, 29 Jul 2013 (p. I-4)

Transnational Organized Crime (TOC). Self-perpetuating associations who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/ or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms. (White House, Strategy to Combat Transnational Organized Crime, Jul 2011)

> ***Transnational Criminal Organizations pose a National Security Threat***
>
> TOC represent a globally-networked national security threat and pose a real and present risk to the safety and security of Americans and our partners across the globe.
>
> *Countering TOC* is defined as the means to detect, counter, contain, disrupt, deter, or dismantle the transnational activities of state and non-state adversaries threatening U.S. and partner nation national security.
>
> Copy of the *Strategy to Combat Transnational Organized Crime* (July 2011) *at:* <https://www.hsdl.org/?view&did=682263>.
>
> Also see *The "New" Face of Transnational Crime Organizations (TCOs): A Geopolitical Perspective and Implications to U.S. National Security,* March 2013 (a compendium of white papers on TCOs).
>
> _____
>
> *"Transnational organized crime (TOC) networks erode good governance, cripple the rule of law through corruption, hinder economic competitiveness, steal vast amounts of money, and traffic millions of people around the globe. (Cybercrime, an expanding for-profit TOC enterprise….) TOC threatens US national interests in a number of ways: …drug activity, facilitating terrorist activity, money laundering, corruption, human trafficking, and environmental crime."*
>
> -- James R. Clapper, DNI, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Committee on Armed Services, 18 April 2013

Trap. A hidden indicator to detect or confirm surreptitious tampering or search of items (e.g., documents, letters, packages, luggage, drawers, safes, rooms, film, equipment) by security or other personnel. (AFOSI Manual 71-119, CI Investigations, 27 Oct 2009)

Trap and Trace. A device which capture the incoming electronic or other impulses which identify the origination number of an instrument or device from which a wire or electronic communication was transmitted; see 18 USC §3127(4). (AR 381-10, US Army Intelligence Activities, 3 May 2007) Also see *pen register; trap and trace device*.

> A *trap and trace device* identifies all incoming phone numbers to a particular telephone.
> A *pen register* captures all outgoing phone numbers a particular telephone has called.

Trap and Trace Device. Captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011) Also see *pen register; trap and trace*.

Trash Cover. The intentional search of a specific person's trash (that is located at the place of collection), whether from a home or business, designed to find information relevant to an ongoing investigation when no reasonable expectation of privacy exists. A trash cover is a targeted effort to gather information regarding a particular person or entity by reviewing that person or entity's refuse. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

Treason. -- Violation of the allegiance owed to one's sovereign or state; betrayal of one's country. (JP 1-02)

-- Also, [previously defined in DoDI 5240.06, *CI Awareness, Briefing, and Reporting Programs*, 7 Aug 2004) Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason [in war time, treason is a violation of Title 18 USC, § 2381].

"Treason is the ultimate mid-life crisis."

-- Dr. Marcus, CIA Psychiatrist in *Sira* by David Ignatius

Treason is the only crime specifically defined in the U.S. Constitution. Article III Section 3 delineates treason as follows: "Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No Person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court."

The crime is prohibited by legislation passed by Congress; 18 U.S.C. § 2381 states "whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined under this title but not less than $10,000; and shall be incapable of holding any office under the United States." In the history of the United States there have been fewer than 40 federal prosecutions for treason and even fewer convictions.

_____

"*Treason is the ultimate word of betrayal. Treason means stabbing your country on the back. But in legal terms, treason, the only crime that is defined in the U.S. Constitution has a narrow meaning… The founding fathers, well aware of the political use of treason charges by the kings of England, wanted to restrict the crime to one that could not be used as an excuse for the elimination of political rivals."*

-- Thomas B. Allen and Norman Polmar, *Merchants of Treason: America's Secrets for Sale* (1988), p. 176

_____

"Treason is loved of many, but the traitor is hated of all."

-- Robert Greene

Triple Agent. An agent who serves three [intelligence] services in an agent capacity but who, like a double agent, wittingly or unwittingly withholds significant information from two services at the instigation of the third service. (FBI FCI Terms)

Trojan. A type of malware disguised or attached to legitimate or innocuous-seeming software, but that instead carries a malicious payload, most often opening a backdoor to unauthorized users. (Cybersecurity and cyberwar) Also see *Trojan Horse*.

Trojan Horse. A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) Also see *Trojan.*

-- Also, a computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security (for example, making a "blind copy" of a sensitive file for the creator of the Trojan horse). (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

-- Also, a malicious program that pretends to be a benign application; it purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but they can be just as destructive. (McAfee.com; accessed 15 Nov 2010)

True Name. A genuine and accurate representation of an individual or organization name, that may involve alterations of other identity information (e.g., address, telephone number, credit score, employer) when used under an approved cover in order to conceal true identity, purpose, or organizational affiliation. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013)

Trusted Foundry Program. DoD program that provides a cost-effective means to assure the integrity and confidentiality of integrated circuits during design and manufacturing while providing the US Government with access to leading edge microelectronics technologies for both Trusted and non-sensitive applications. (DMEA web site)

> Defense Microelectronics Activity (DMEA) is the program manager for the DoD Trusted Foundry program; see website at: <http://www.dmea.osd.mil/trustedic.html>
>
> Also see NSA's Trusted Access Program Office (TAPO) web site at: <http://www.nsa.gov/business/programs/tapo.shtml>

TSCM. See *Technical Surveillance Countermeasures*.

TSCM Practitioner. An individual trained and certified to conduct all TSCM activities within DoD. (DoDI 5240.05, TSCM, 3 Apr 2014) Also see *TSCM Technician*.

TSCM Technician. An individual trained to perform limited TSCM activities under the oversight of a TSCM practitioner. (DoDI 5240.05, TSCM, 3 Apr 2014) Also see *TSCM Practitioner*.

TSCM Equipment. Equipment or mechanisms used to identify the presence of surveillance devices. TSCM includes general purpose, specialized, or fabricated equipment to determine the existence and capability of surveillance devices. (DoDI 5240.05, TSCM, 3 Apr 2014)

Turnover. The official changing of an agent from one case officer to the other—i.e., turning him over to another. (A Spy's Journey)

Two-Person Control (TPC). the continuous surveillance and control of material at all times by a minimum of two authorized individuals, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed and each familiar with established security requirements. (DoDI 5200.33, Defense Courier Operations, 30 Jun 2011) Also see *two-person integrity; two-person rule.*

-- Also, continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Two-Person Integrity. A provision that prohibits one person from working alone. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995)

Two-Person Rule. A system designed to prohibit access by an individual to nuclear weapons and certain designated components by requiring the presence at all times of at least two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task to be performed. (JP 1-02)

U

Umbrella Special Access Program (SAP). An approved Department of Defense (DoD) Special Access Program (SAP) that contains compartments for specific projects within the overall program. While there is no formal requirement to obtain separate approval for each individual project under the umbrella SAP, each project must be consistent with the Special Access Program Oversight Committee (SAPOC)-approved scope of the umbrella SAP. The nickname, program description, and accomplishments of each significant project will be reported in the annual Special Access Program report. *Note: An individual participant's access can be afforded across-the-board at the umbrella level or specific individual project access can be granted on a limited or non-umbrella level.* (DSS Glossary)

Unacceptable Risk. Threat to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, privileged, proprietary, financial, or medical records; or to the privacy of data subjects, which will not be tolerated by the Government. (DoDI 5200.02, DoD Personnel Security Program, 21 Mar 2014)

Unacknowledged SAP. A SAP [Special Access Program] having protective controls ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information. (DoDD 5205.07, SAP Policy, 1 Jul 2010) Also see *acknowledged SAP*.

Unauthorized Access. Any access that violates the stated security policy. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient. (EO 13526, Classified National Security Information, 29 Dec 2009 and DoDD 5210.50, Unauthorized Disclosure of Classified Information to the Public, 22 Jul 2005)

> *Unauthorized disclosures of classified information, including media leaks, may compromise sources and methods and pose a threat to national security.*
> -- ICD 701 Security Policy for Unauthorized Disclosures of Classified Information, 14 Mar 2007

-- Also, a communication or physical transfer, usually of sensitive but unclassified information or classified information, to an unauthorized recipient. (ODNI, U.S. National Intelligence – An Overview 2011)

-- Also, an event involving the exposure of information to entities not authorized access to the information. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, intentionally conveying classified documents, information, or material to any unauthorized person (one without the required clearance, access, and need to know). (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010)

> *Unauthorized disclosures of classified information put at risk the success of the most sensitive classified operations, plans, partnerships, and technologies of DoD and our mission partners.*
>
> *Personnel who disclose classified information without authorization, in addition to having potentially committed a crime, breach the trust that we, as leaders, have placed in them.*
> -- SECDEF memorandum, subj: Deterring and Preventing Unauthorized Disclosures of Classified Information, 18 Oct 2012*
>
> * Copy available at: <http://www.fas.org/sgp/othergov/dod/osd101812.pdf>

Unauthorized disclosure of classified information is an increasingly common occurrence.

The harm caused by… frequent unauthorized disclosures is manifold. Particular items of information appearing in the press provide valuable intelligence for our adversaries concerning the capabilities and plans of the United States for national defense and foreign relations…. Disclosures about US intelligence programs are particularly damaging, because they may cause sources to dry up. Lives of human agents are endangered and expensive technical systems become subject to countermeasures.

--*The Willard Report*, 31 March 1982

Leaking sensitive information is like giving the enemy our play book.

Each year, countless unauthorized leaks cause severe damage to our intelligence activities and expose our capabilities. The fact of the matter is, some of the worst damage done to our intelligence community has come not from penetration by spies, but from unauthorized leaks by those with access to classified information…. The threat leaks pose to our national security is alarming, and it is imperative we do more to protect our national secrets.

-- Congressman Rep. Pete Hoekstra at the Heritage Foundation, 25 July 2005.
See full remarks at <http://www.fas.org/sgp/news/2005/07/hoekstra072505.html>

Intelligence requires secrets. And secrecy is under assault…. When secrecy is breached, foreign targets of US intelligence—such as adversary countries and terrorists—learn about, and then often develop countermeasures to, US intelligence techniques and operations. As a result, the effectiveness of intelligence declines, to the detriment of the national security policymakers and warfighters, and the citizenry that it is meant to serve.

-- James B. Bruce, Former CIA Officer

See Bruce's excellent article, entitled "The Consequences of Permissive Neglect: Laws and Leaks of Classified Intelligence" in *Studies of Intelligence* (Vol 47 No 1), available online at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/article04.html>

Leaks are a problem that has plagued intelligence agencies throughout modern history – they can undermine intelligence operations, jeopardize intelligence sources and methods, and have a terrible impact on the lives of covert agents who are publicly exposed.

-- Senator Ron Wyden, cited in Senate Report 112-12, 4 April 2011, p. 12

The unauthorized release of classified documents in 2010 by major newspapers and the Wikileaks website underscore the risks of widespread dissemination of sensitive information.

-- CRS Report RL33539, *Intelligence Issues for Congress*, 20 Jun 2011

In the secret operations canon it is axiomatic that the probability of leaks escalates exponentially each time a classified document is exposed to another person—be it an Agency employee, a member of Congress, a senior official, a typist, or a file clerk. Effective compartmentation is fundamental to all secret activity…. The potential leaks—deliberate or accidental—is vast.

-- Richard Helms with William Hood, *A Look Over My Shoulder* (2003), pp.184-185

Every once in a while, there are people in the United States government who decide that they want to break federal criminal law and release classified information, and they ought to be imprisoned. And if we find out who they are, they will be imprisoned. Why people do it, I do not know.

-- Defense Secretary Donald Rumsfeld

When information about our intelligence, our people, or our operations appears in the media, it does incredible damage to our nation's security and our ability to do our job of protecting the nation. More importantly, it could jeopardize lives. For this reason, such leaks cannot be tolerated."

-- CIA Director Leon Panetta, Nov 2010

_____

Leaks of classified information regarding intelligence sources and methods can disrupt intelligence operations, threaten the lives of intelligence officers and assets, and make foreign partners less likely to work with us. The culture of leaks has to change.

-- Senator Dianne Feinstein, Chairman of the Senate Intelligence Committee, 25 July 2012

Uncertain Environment. Operational environment in which host government forces, whether opposed to or receptive to operations that a unit intends to conduct, do not have totally effective control of the territory and population in the intended operational area. (JP 1-02 and JP 3-0, Joint Operations, 11 Aug 2011)

Uncertainty. Doubt resulting from awareness of imperfect knowledge. This may arise from information absence, perceived error, deception, unpersuasive nature of evidence, complexity, etc. (*A Handbook of the Psychology of Intelligence Analysis*, Richard L. Rees, Ph.D., Editor; n.d. - circa 2007)

In analysis, uncertainty can derive from seeing plausible alternatives to the truth (the latter of which may be unknown or unknowable). Moreover, emotional and motivational factors attend cognitive uncertainty. Analysts can feel anxiety or discomfort if they lack confidence or self-esteem generally, feel an aversion to ambiguity, or have a need to please, or have a hypersensitivity to criticism. This affective element can exist even in the presence of sufficient evidence to make a reasonable judgment. Some analyst may well estimate the truth, but—in contrast to the inscription on the wall of the CIA lobby (*John* 8:32)—the truth.

-- *A Handbook of the Psychology of Intelligence Analysis*, Richard L. Rees, Ph.D., Editor; n.d., p. 375

Unconventional Warfare (UW). A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes, but is not limited to, guerrilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery. (DoDD 3000.07, Irregular Warfare, 1 Dec 2008)

-- Also, activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area. (JP 3-05, Special Operations, 18 Apr 2011)

Undeclared. An officer, asset, agent, or action whose agency affiliation is not formally identified to a foreign intelligence or security service, government or organization, or other US Government entity. (National HUMINT Glossary)

-- Also, an individual or action whose intelligence affiliation is not disclosed. (HDI Lexicon, April 2008)

Undercover Activity. Any investigative activity involving the use of an assumed identity by an undercover employee for an official purpose, investigative activity, or function. (FBI, Domestic Investigations and Operations Guide, 15 Oct 2011)

Undercover Employee. An employee of the FBI, another federal, state, or local law enforcement agency, another entity of the United States Intelligence Community (USIC), or another foreign intelligence agency working under the direction and control of the FBI whose relationship with the FBI is concealed from third parties by the maintenance of a cover or alias identity for an official purpose, investigative activity, or function. (FBI, Domestic Investigations and Operations Guide, 15 Oct 2011)

Undercover Operation. A phrase usually associated with the law enforcement community and which describes an operation that is so planned and executed as to conceal the identity of, or permit plausible denial by, the sponsor. (DSS Glossary)

Understand. The ability to individually and collectively comprehend the implications of the character, nature, or subtleties of information about the environment and situation to aid decision-making. (Joint Capability Areas Taxonomy & Lexicon, 15 Jan 2008)

Unified Action. The synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013)

Unified Command Plan (UCP). The document, approved by the President, that sets forth basic guidance to all unified combatant commanders; establishes their missions, responsibilities, and force structure; delineates the general geographical area of responsibility for geographic combatant commanders; and specifies functional responsibilities for functional combatant commanders. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02) Also see *Combatant Command*.

Six Combatant Commands (COCOMs) have geographic area responsibilities:
-- U.S. Northern Command (NORTHCOM)
-- U.S. Central Command (CENTCOM)
-- U.S. European Command (EUCOM)
-- U.S. Pacific Command (PACOM)
-- U.S. Southern Command (SOUTHCOM)
-- U.S. Africa Command (AFRICOM)

Three COCOMs that have worldwide functional responsibilities not bounded by geography:
-- U.S. Special Operations Command (SOCOM)
-- U.S. Strategic Command (STRATCOM)
-- U.S. Transportation Command (TRANSCOM)

Note: U.S. Joint Forces Command (JFCOM) was disestablished in August 2011.

For additional information, see CRS Report, *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*, 3 Jan 2013, copy available at: <http://www.fas.org/sgp/crs/natsec/R42077.pdf>

Uniform Code of Military Justice (UCMJ). The criminal code governing the Armed Services of the United States. (CI Community Lexicon)

UCMJ (10 USC Chapter 47), is the foundation of military law in the United States. See UCMJ appendix in Manual for Courts-Martial (MCM): <http://www.au.af.mil/au/awc/awcgate/law/mcm.pdf>

Unilateral Operation. A clandestine activity conducted without the knowledge or assistance of a foreign intelligence or security service, host country, foreign organization, or non-state actor. (National HUMINT Glossary)

United States (US). Includes the land area, internal waters, territorial sea, and airspace of the United States, including the following: a) US territories, possessions, and commonwealths; and b) Other areas over which the US Government has complete jurisdiction and control or has exclusive authority or defense responsibility. (JP 1-02)

-- Also, when used in a geographic sense, means all areas under the territorial sovereignty of the United States. (FBI Domestic Investigations and Operations Guide, 15 Oct 2011)

Unity of Effort. Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization - the product of successful unified action. (JP 1, Doctrine for the Armed Forces of the United States, 25 Mar 2013 and JP 1-02)

Unknown Subject (UNSUB). The subject of an investigation, whose identity has not been determined, commonly referred to as an "UNSUB." Also see *DoD Unknown Subject*.

Unknown Subject Lead. [Within DoD,] information indicating an unidentified current or former DoD-affiliated individual may have passed information or provided support to an FIE. (DoD Manual 5240.26, CI Insider Threat Program, *draft* 20 Nov 2013)

Unload Signal. A visual signal to indicate the departure of an individual or removal of an object from a given locale. (HDI Lexicon, April 2008)

Unsolicited Correspondence. Request for information from a person which may range from direct inquiries by phone, e-mail, fax, or letter in which the recipient is asked to provide seemingly innocuous data. (AR 381-12, Threat Awareness and Reporting Program, 4 Oct 2010)

> Typical requests include solicitation of research papers, requests for additional information after a public presentation, suggestions for mutual research, requests for survey participation, and so forth; correspondence where the actual purpose may be to identify by name and position any individual who might be targeted later by a foreign intelligence service, and to elicit targeted information not readily obtainable by other means.

Unwitting. A person who is not aware of USG sponsorship of or affiliation with the cover. (DoDI S-5105.63, Implementation of DoD Cover and Cover Support Activities, 20 Jun 2013) Also see *witting.*

-- Also, not aware of US Government sponsorship or affiliation. (National HUMINT Glossary)

-- Also, unaware of the true nature of the activities being conducted or of the intelligence connections of persons involved. (HDI Lexicon, April 2008)

U.S. Coast Guard (USCG). A military, multi-function, maritime service that is the principal Federal agency responsible for safety, security, and stewardship with the maritime domain. It has diverse missions: national defense, homeland security, maritime safety, and environmental & natural resources stewardship. In March 2003, pursuant to the Homeland Security Act, the USCG was transferred from the Department of Transportation to the Department of Homeland Security (DHS).

> The CI component of the USCG is the Coast Guard Counterintelligence Service (CGCIS).

U.S. Homeland. The physical territory of the United States: the 50 states, District of Columbia, US territories and territorial waters; significant infrastructure linked to the United States; and major commercial air, land and sea corridors into the country. Also see *homeland*.

U.S. National. US citizen and US permanent and temporary legal resident aliens. (JP 1-02)

U.S. Person (USPERS; also USP). For intelligence purposes, a US person is defined as one of the following: 1) a US citizen; 2) an alien known by the intelligence agency concerned to be a permanent resident alien; 3) an unincorporated association substantially composed of US citizens or permanent resident aliens; or 4) a corporation incorporated in the United States, except for those directed and controlled by a foreign government or governments. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

> Note: A person or organization outside the United States shall be presumed not to be a USP unless specific information to the contrary is obtained.

U.S. Secret Service (USSS). A federal law enforcement agency mandated by Congress to carry out dual missions: protection of national and visiting foreign leaders, and criminal investigations. (www.secretservice.gov)

> The Secret Service was established in 1865, solely to suppress the counterfeiting of U.S. currency. Headquarters in Washington, D.C. and more than 150 offices throughout the United States and abroad. Congress transferred USSS to the Department of Homeland Security (DHS) in 2002.
>
> Criminal investigation activities encompass financial crimes, identity theft, counterfeiting, computer fraud, and computer-based attacks on the nation's financial, banking, and telecommunications infrastructure.
>
> Protection mission is the most prominent of the two, covering the President, Vice President, their families, former Presidents, and major candidates for those offices, along with the White House and the Vice President's residence (through the Service's Uniformed Division). Protective duties of the Service also extend to foreign missions in the District of Columbia and to designated individuals, such as the Homeland Security Secretary and visiting foreign dignitaries.
>
> Separate from these specific mandated assignments, USSS is responsible for certain security activities such as National Special Security Events (NSSEs), which include the major party quadrennial national conventions as well as international conferences and events held in the United States.
>
> -- See CRS Report RL34603, *The U.S. Secret Service: An Examination and Analysis of Its Evolving Missions*, 31 July 2008

U.S.A. Patriot Act. USA Patriot Act of 2011 (Public Law 107-56); see *Patriot Act*.

V ==========

Validation. [In intelligence usage], a process associated with the collection and production of intelligence that confirms that an intelligence collection or production requirement is sufficiently important to justify the dedication of intelligence resources, does not duplicate an existing requirement, and has not been previously satisfied. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011)

Vault. A room(s) used for the storing, handling, discussing, and/or processing of Special Access Program (SAP) information and constructed to afford maximum protection against unauthorized entry. (DSS Glossary)

Vehicle-Borne Improvised Explosive Device (VBIED). A device placed or fabricated in an improvised manner on a vehicle incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. Otherwise known as a car bomb. (JP 1-02 and JP 3-10, Joint Security Operations in Theater, 3 Feb 2010)

VENONA. Highly classified U.S. SIGINT (cryptanalysis) effort during World War II to decipher encoded Soviet intelligence messages transmitted to Moscow on espionage activity in the United States. VENOA traffic indicated that the Soviets had over 300 assets of various kinds inside numerous U.S. Government agencies.

-- Also, code name for the U.S. codebreaking project that deciphered portions of the texts of Soviet intelligence messages between Moscow and other cities in the 1940s. Most messages concerned spy activities in the United States. (Spy Book)

I stood in the vestibule of the enemy's house, having entered by stealth.
I held in my hand a set of keys… and we were determined to use them.
-- FBI Agent Robert J. Lamphere

_____

VENONA decryptions of Soviet intelligence messages in the 1940s, majority during WWII, identified numerous agents with access to the White House, Congress, and political parties, as well as agents in the media and in high-tech defense industries, however 178 Russian code names have yet to be linked to the true names of the American spies.

Research in Soviet Archives has added to the corroboration of some VENONA material, including the identities of many codenamed individuals

For additional information:
<www.nsa.gov/public_info/declass/venona/index.shtml>
<http://web.archive.org/web/20060614231955/http://www.nsa.gov/publications/publi00039.cfm>

Also see "In the Enemy's House: Venona and the Maturation of American Counterintelligence" at:
<http://web.archive.org/web/20061115021025/http://www.fbi.gov/libref/historic/history/foxpaper.htm>

Also see *The FBI-KGB War: A Special Agent's Story* by Robert J. Lamphere and Tom Shachtman.

Vetting. A generic term to describe the full spectrum of asset evaluation for authenticity, reliability and hostile control. It includes ops testing, caser officer and psychological assessment, polygraph, security, counterintelligence interview, production review and personal record questionnaires. (National HUMINT Glossary) Also see *asset validation, source validation* and *counterintelligence flags*.

-- Also, as related to *source validation*, an ongoing process the purpose of which is to continually determine, by means of specific operational acts and analytical assessments, the motivation, veracity, and control of a reporting source. (DoDI S-3325.07, Guidance for the Conduct of DoD Human Source Validation (U), 22 Jun 2009)

-- Also, the complete process of investigating and testing a potential source or information to determine its ability and suitability for clandestine activities. (AFOSI Instruction 71-101, 6 Jun 2000)

-- Also, a process of examination and evaluation, generally referring to performing a background check on someone before offering him or her employment, conferring an award, etc. In addition, in intelligence gathering, assets are vetted to determine their usefulness. (en.wikipedia.org/wiki/Vetting)

"Vetting" literally means getting a sick animal examined by a veterinarian; it has evolved into a term meaning to test or scrutinize.

-- Spy Book

Vetting is used in agent/source authentication. The vetting process is one of testing and examining the agent to determine the degree of the agent's/source's reliability and truthfulness in reporting information. It is designed to weed out fabricators and double agents.

Violent Behavior. The intentional use of physical force or power, threatened or actual, against a person or group that either results in or has a high likelihood of injury, death, or psychological harm to self or others. (DoDI 1438.06, DoD Workplace Violence Prevention and Response Policy 16 Jan 2014)

Violent Extremism. Individuals who openly express their religious, political, or ideological views through violence or a call for violence. (US Army Tactical Reference Guide, Radicalization into Violent Extremism: *A Guide for Military Leaders*, Aug 2011) Also see *radicalization*, *terrorism*, *violent radicalization.*

--Also, any ideology that encourages, endorses, condones, justifies, or supports the commission of a violent act or crime… to achieve political, social, or economic changes…. (FBI Counterterrorism Analytical Lexicon)

-- Also, the process of adopting or promoting an extremist belief system for the purpose of facilitating ideologically based violence to advance political, religious, or social change. (House Bill 1955, 110th Congress, 24 Oct 2007)

Copy of Army reference cited above available at: <https://rdl.train.army.mil/catalog/go/100.ATSC/883A3A74-A803-4CD5-B693-0D59B108E7EC-1326399638300> Reference also at: <http://www.wired.com/images_blogs/dangerroom/2012/10/awsc-pdf-CDR-72811.pdf>

The Complexity of Violent Extremism

The threat posed by violent extremism is neither constrained by international borders nor limited to any single ideology. Groups and individuals inspired by a range of religious, political, or other ideological beliefs have promoted and used violence against the homeland.

Increasingly sophisticated use of the Internet, mainstream and social media, and information technology by violent extremists adds an additional layer of complexity.

-- Department of Homeland Security
See <http://www.dhs.gov/topic/countering-violent-extremism. (accessed 16 Jul 2013)

"Violent extremism presents one of the greatest threats to the citizenry of the United States and its allies."

-- *Edges of Radicalization*, Combating Terrorism Center, Feb 2012, p. 6

Violent Jihadist. The term characterizes jihadists who have made the jump to illegally supporting, plotting, or directly engaging in violent terrorist activity. (CRS Report R41416, 23 Jan 2013)

> American Jihadist Terrorism: Combating a Complex Threat, CRS Report R41416, 23 Jan 2013 available online at: <http://www.fas.org/sgp/crs/terror/R41416.pdf>

Violent Radicalization. The process of adopting or promoting an extremist belief system for the purpose of facilitating ideologically based violence to advance political, religious, or social change. (House Bill 1955, 24 Oct 2007) Also see *radicalization, terrorism, violent extremism*.

Virus. Malicious software; a form of Trojan horse that reproduces itself in other executable code. (DoD 5220.22.22-M-Sup 1, NISPOM Supplement, Feb 1995) Also see *computer virus*.

-- Also, a computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010)

-- Also, a software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. (US Army TRADOC DCSINT Handbook 1.02, 15 Aug 2007)

> *A virus is a computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies, or creates the files. Some viruses display symptoms, and others damage files and computer systems, but neither is essential in the definition of a virus; a non-damaging virus is still a virus.*
>
> – McAfee.com; accessed 15 Nov 2010

Volunteer. A person who initiates contact with a government, and who volunteers operational or intelligence information and/or request political asylum; includes call-ins, walk-ins, virtual walk-ins, and write-ins. (National HUMINT Glossary)

Vulnerability. 1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished; 2). The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment; and 3) In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 1-02 and JP 3-60, Joint Targeting, 13 Apr 2007)

-- Also, a situation or circumstance, which left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, a weakness or susceptibility of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (DHS, National Infrastructure Protection Plan - 2009)

Vulnerability Analysis. A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity. (DoD 5205.02-M, DoD OPSEC Program Manual, 3 Nov 2008)

Vulnerability Assessment (VA). A Department of Defense, command, or unit-level evaluation (assessment) to determine the vulnerability of a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. (JP 1-02 and JP 3-07.2, Antiterrorism, 24 Nov 2010)

-- Also, [regarding infrastructure] a systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities. (DoDD 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 Jan 2010 w/ chg 2 dated 21 Sep 2012)

-- Also, the comprehensive evaluation of an installation, facility, or activity to determine preparedness to deter, withstand, and /or recover from the full range of adversarial capabilities based on the threat assessment, compliance with protection standards, and risk management. (DoD 5200.08-R, Physical Security Program, 9 Apr 2007)

-- Also, the process of identifying weaknesses in the protection of friendly operations and activities which, if successfully exploited by foreign intelligence, could compromise current or future plans, capabilities, or activities, including RDA [research, development and acquisition]. (AR 381-20, Army CI Program, 25 May 2010)

Vulnerability Study. An analysis of the capabilities and limitations of a force in a specific situation to determine vulnerabilities capable of exploitation by an opposing force. (JP 1-02)

W ==========

Waived Special Access Program. A SAP [Special Access Program] for which the Secretary of Defense has waived applicable reporting in accordance with [Section 119 of Title 10 US Code] following a determination of adverse effect to national security. An unacknowledged SAP that has more restrictive reporting and access controls. (DoDD 5205.07, SAP Policy, 1 Jul 2010)

-- Also, an unacknowledged Special Access Program (SAP) to which access is extremely limited in accordance with the statutory authority of Section 119e of 10 United States Code (U.S.C), Reference b. The unacknowledged SAP protections also apply to Waived SAPs. Only the Chairman, Senior Minority member, and, by agreement, their Staff Directors of the four Congressional Defense Committees normally have access to program material.

Waiver. An exemption from a specific requirement. (DSS Glossary)

Walk-in. An unsolicited contact who provides information. (JP 1-02; JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011; DoDI S-5240.17, CI Collection Activities, 14 Mar 2014; and DHE-M 3301.002, Vol II Collections Operations, 23 Nov 2010) Also see *volunteer*.

-- Also, an individual who voluntarily offers his services or information to a foreign government. (FBI FCI Terms)

-- Also, an individual who offer his/her services to an intelligence service without being solicited. (CIA, D&D Lexicon, 1 May 2002)

-- Also, someone who has something to offer or sell to the intelligence service he is approaching: a volunteer spy. (A Spy's Journey)

Individuals who walk-in and provide information or offer to assist are motivated by a wide range of factors, including a sincere desire to help, pure greed, desire for revenge against some real or perceived grievance, etc. Each walk-in interview is unique.

In the real world of secret operations volunteers have produced some of the greatest coups. "It's the walk-in trade that keeps the shop open" is one of the first bits of operational wisdom impressed on newcomers to the business.

-- William Hood, *Mole: The True Story of the First Russian Intelligence Officer Recruited by the CIA* (1982)

As always with a "walk-in," as we irreverently referred to volunteer agents, the first consideration is the possibility of provocation.

-- Richard Helms with William Hood, *A Look Over My Shoulder: A Life in the Central Intelligence Agency* (2003), p. 219

[Walk-in] applies universally to agents who volunteer their services to a hostile intelligence agency by making an approach to an adversary at its premises. The KGB recognized that some of its best sources including John Walker, Aldrich Ames, and Robert Hanssen, acted in this way, but did not use the same term, preferring "self-recruited agents.

-- *Historical Dictionary of Cold War Counterintelligence* (2007)

For the story of a walk-in, see Barry G. Royden, "Tolkachev, A Worthy Successor to Penkovsky," *Studies in Intelligence*, v 47, n 3: pp. 5-33. Full article available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article02.html>

…it should be emphasized once more that work with "walk-ins" is an important part of agent operations for strategic intelligence and when properly planned and conducted can be very fruitful.

-- Ivan A. Serov, GRU General (1962)

See Ivan A. Serov, "Work with Walk-Ins,"* *Studies in Intelligence*, Vol 8, No, 1. This article, originally published in 1962, is adapted from one of several on Soviet intelligence doctrine written by high-ranking officers of the GRU (Soviet Military Intelligence). The article shows that Soviet/Russian problems in assessing and handling the walk-in are not unlike our own. The full article available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol8no1/html/v08i1a02p_0001.htm >

* Note: Russian term *dobrozhelatel* ("well-wisher") is virtually the same as our "walk-in."

Warning. 1) A communication and acknowledgment of dangers implicit in a wide spectrum of activities by potential opponents ranging from routine defense measures to substantial increases in readiness and force preparedness and to acts of terrorism or political, economic, or military provocation; and 2) operating procedures, practices, or conditions that may result in injury or death if not carefully observed or followed. (JP 1-02) Also see *warning intelligence*.

-- Also, a communication and acknowledgment of dangers implicit in a wide spectrum of activities by potential opponents ranging from routine defense measures to substantive increases in readiness and force preparedness and to acts of terrorism or political, economic, or military provocation. (DoDD 3115.16, The Defense Warning Network,5 Dec 2013)

-- Also, to issue an advance notification of possible harm or victimization following the receipt of information or intelligence concerning the possibility of a crime or terrorist attack. (ODNI, U.S. National Intelligence – An Overview 2011)

Warning Intelligence. Those intelligence activities intended to detect and report time sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests. (JP 2-0, Joint Intelligence, 22 Oct 2013)

Watch List. A list of words -- such as names, entities, or phrases -- which can be employed by a computer to select out required information from a mass of data. (Senate Report 94-755, Book I – Glossary, 26 Apr 1976)

Weapon System. A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012)

Weapons of Mass Destruction (WMD). Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. (JP 1-02 and JP 3-40, Combating WMD, 10 Jun 2009)

Specifically defined in US Code as: (1) any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or missile having an explosive or incendiary charge of more than one-quarter ounce, or mine or similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. (18 USC 18 §2332a)

White List. The identities and locations of individuals who have been identified as being of intelligence or counterintelligence interest and are expected to be able to provide information or assistance in existing or new intelligence areas of interest. (CI Community Lexicon) Also see *Black List*; *Gray List.*

> *White lists contain the identities and locations of individuals in enemy controlled areas. These individuals are of intelligence or CI interest. They are expected to be able to provide information or assistance in the accumulation of intelligence data or in the exploitation of existing or new intelligence areas of interest. They are usually in accord with or favorably inclined toward U.S. policies. Their contributions are based on a voluntary and cooperative attitude. Decisions to place individuals on the white list may be affected by the combat situation, critical need for specialists in scientific fields, and such intelligence needs as indicated from time to time.*
> *Examples of individuals included in this category are:*
> 1) *Deposed political leaders of a hostile state.*
> 2) *Intelligence agents employed by U.S. or allied intelligence agencies.*
> 3) *Key civilians in areas of scientific research, including faculty members of universities and staffs of industrial or national research facilities whose credibility have been established.*
>
> -- USMC, MCWP 2-6 (previously 2-14), Counterintelligence, 5 Sep 2000

Wilderness of Mirrors. The organizational culture of the secret services. In it deceptions are false, lies are truth, the reflections are illuminating and confusing. The phrase centers on the problem of the reliability of the secret information about espionage and the identity of spies. The mirrors comprise information from defectors, disinformation from the opposing sides in the Cold War, deviously covered false trails, and facts thought to be valid but incomplete (and later established as totally untrue). (Encyclopedia of Cold War Espionage, Spies, and Secret Operations, 3rd edition, 2012)

-- Also, expression to sgnify the confusion of the world of intelligence and espionage. James Jesus Angleton, long-time head of counterespionage for the CIA, is generally credited with coining the term, having written that the Wilderness of Mirrors "is that… myriad of strategms, deceptions, artifices and all other devices of disinformation which the Soviet bloc and its coordinated intelligence services use to confuse and split the West," thus producing "an ever-fluid landscape where fact and illusion merge…." (Spy Book)

> ***"Wilderness of Mirrors"*** a description of counterintelligence attributed to James J. Angleton. It comes from T.S. Eliot's poem "Gerontion" (1920); also the title of a 1980 book authored by David C. Martin about CIA counterintelligence (New York: HarperCollins, First Edition, 1980).
>
> Angleton was CIA's Chief of the Counterintelligence from 1954 until his retirement in 1974. In December 1974, Angleton was basically forced into retirement by the Director of CIA (William Colby), who became convinced that Angleton's "labyrinthine" approach to counterintelligence severely hampered the Agency's primary mission -- clandestine HUMINT collection.

Window Dressing. [Tradecraft jargon] Ancillary materials that are included in a cover story or deception operation to help convince the opposition or casual observers that what they are observing is genuine. (CI Centre Glossary)

Witting. A term of intelligence art that indicates that one is not only aware of a fact or piece of information but also aware of its connection to intelligence activities. (JP 1-02 and JP 2-01.2, CI & HUMINT in Joint Operations, 16 Mar 2011 w/ chg 1 dated 26 Aug 2011) Also see *unwitting*.

-- Also, a person is aware of USG sponsorship or affiliation. (National HUMINT Glossary)

-- Also, aware of the true nature of the activities being conducted or of the intelligence connections of persons involved. (HDI Lexicon, April 2008)

-- Also, knowledgeable as to certain aspects of a clandestine organization and its activities. (AFOSI Manual 71-142, OFCO, 9 Jun 2000)

Workplace Violence. Any act of violent behavior, threats of physical violence, harassment, intimidation, bullying, verbal or non-verbal threat, or other threatening, disruptive behavior that occurs at or outside the work site. (DoDI 1438.06, DoD Workplace Violence Prevention and Response Policy 16 Jan 2014)

Worm. A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. (CNSSI No. 4009, National Information Assurance Glossary, 26 April 2010) See *worms*.

-- Also, a type of malware that spreads automatically over a network, installing and replicating itself. The network traffic from rapid replication and spread can cripple networks even when the malware does not have a malicious payload. (Cybersecurity and Cyberwar)

> A worm is an unwanted software program secretly planted on a computer that enables (among other things) someone other than the owner to control it.
>
> In 2009, cyber security analysts worldwide reported that a "worm" called Stuxnet had penetrated and, in all likelihood, damaged an Iranian nuclear facility. The attack was apparently prosecuted through the facility's industrial control system.
>
> -- RAND Report, *A Cyberworm that Knows No Boundaries*, 2011* (see Appendix B - Worms)
>
> * Copy at: <http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.pdf>

Worms. Parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies on the same computer, or can send the copies to other computers via a network. Worms often spread via Internet Relay Chat (IRC). (McAfee.com; accessed 15 Nov 2010) See *worm*.

Write for Maximum Utility (WMU). An approach that guides the way that intelligence organizations conceive, format, produce, and disseminate intelligence products in order to increase their usability for the intended customers. (ICD 208, 17 Dec 2008) Also see *write-to-release*.

> *Utility is maximized when customers receive or are able to expeditiously discover and pull or request intelligence, information, and analysis in a form they are able to easily use and able to share with their colleagues, subordinates, and superiors. WMU ensures intelligence, information, and analysis are produced in a manner to facilitate reuse—either in its entirety or in coherent portions—thereby enabling wider dissemination and enhancing its usability.*
>
> *WMU shares certain goals as well as techniques with previous and ongoing IC WTR [write-to-release] efforts. WMU goes further than WTR in linking knowledge of the customer's operating environment to the intelligence production effort. The resulting effort is not "one size fits all" or production of all intelligence products at the lowest classification, but products tailored to best meet a customer's requirements. This may mean producing the definitive assessment on a given topic area based on all available intelligence, regardless of classification.*
>
> -- ICD 208, *Write for Maximum Utility*, 17 Dec 2008

Write-to-Release (WTR). A general approach whereby intelligence reports are written in such a way that sources and methods are protected so that the report can be distributed to customers or intelligence partners at lower security levels. In essence, write-to-release is proactive sanitization that makes intelligence more readily usable by a more diverse set of customers. The term encompasses a number of specific implementation approaches, including sanitized leads and tearline reporting. (ICD 208, 17 Dec 2008) Also see *tearline reporting* and *write for maximum utility*.

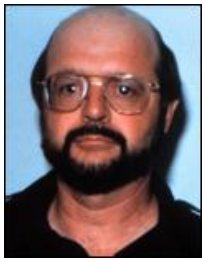
Written Statement. Permanently record of pretrial testimony of accused persons, suspects, victims, complaints, and witnesses. (FM 19-20, Law Enforcement Investigations, Nov 1985)

> *Written statements may be used in courts as evidence attesting to what was told investigators. They also are used to refresh the memory of the persons making the statements.*
>
> -- FM19-20, Law Enforcement Investigations, Nov 1985, p. 53

Y ==========

Year of the Spy. The year 1985 was labeled "The Year of the Spy" by the media because of the number of espionage-related incidents that came to light that year. Unbeknownst to the media and the CIA at the time, several other significant spying ventures started during this same year and would not come to light until years later. (Spy Dust)

-- Also, the phrase, coined late in 1985, to summarize the activities among notable spies and defectors in the Cold War. (Encyclopedia of Cold War Espionage, Spies, and Secret Operations, 3rd edition, 2012)


John A. Walker, Jr.


Sharon M. Scranage


Jonathan J. Pollard


Larry Wu-tai Chin


Ronald W. Pelton

"The Year of the Spy" -- 1985

Spring 1985, the John Walker Spy Ring—John A. Walker, Jerry Whitworth, Arthur Walker, and Michael Walker—arrested for passing classified material to the Soviet Union.

July 1985, CIA employee Sharon Marie Scranage and boyfriend Michael Soussoudis arrested for passing material to Ghanian intelligence.

November 21, Navy intelligence analyst Jonathan Jay Pollard arrested for spying for Israel.

November 23, former CIA analyst Larry Wu-Tai Chin arrested on charges of spying for the People's Republic of China since 1952.

November 25, former National Security Agency employee Ronald William Pelton arrested for selling military secrets to the Soviets.

-- FBI at <http://www.fbi.gov/about-us/investigate/counterintelligence/cases>

For general background on these cases see Thomas B. Allen and Norman Polmar, *Merchants of Treason: America's Secrets for Sale,* New York: Delacorte Press, 1988.

For additional background see –

Walker Spy Ring: Hunter, Robert W., with Lynn Dean Hunter, eds. *Spy Hunter: Inside the FBI Investigation of the Walker Espionage Case*. Annapolis, MD: Naval Institute Press, 1999.

Other works on the Walker Espionage Ring:

-- Barron, John. *Breaking the Ring: The Bizarre Case of the Walker Family Spy Ring*. Boston: Houghton Mifflin, 1987.

-- Blitzer, Wolf. *Territory of Lies: The Exclusive Story of the Walker Family Spy Ring*. New York: Houghton Mifflin, 1987.

-- Blum, Howard. *I Pledge Allegiance: The True Story of the Walkers: An American Spy Family*. Simon & Schuster Books, 1987.

-- Earley, Pete. *Family of Spies: Inside the John Walker Spy Ring*. Bantam Books, 1988.

-- Kneece, Jack. *Family Treason: The Walker Spy Case*. New York: Stein & Day, 1986.

-- Walker, John Anthony. *My Life as a Spy*. Amherst, New York: Prometheus, 2008.

Pollard: Olive, Ronald J. *Capturing Jonathan Pollard: How One of the Most Notorious Spies in America History Was Brought to Justice.* Annapolis, MD: Naval Institute Press, 2006.

Chin: Hoffman, Tod. *The Spy Within: Lary Chin and China's Penetration of the CIA.* Hanover, NH: Steerforth Press, 2008.

Z ==========

Zero Day. [In computer usage] an attack that exploits a previously unknown vulnerability; taken from the notion that the attacks takes places on the zeroth day of awareness. Knowledge about zero-day exploits are valuable to both defenders and attackers. (Cybersecurity and Cyberwar)

Zombie. [In computer usage] a computer that is infected with a virus or Trojan horse that puts it under the remote control of an online hijacker. The hijacker uses a zombie to generate spam or launch denial of service attacks. (McAfee Labs – Threat Glossary)

-- Also, a computer that has been compromised by an outside party, for the purpose of exploiting its computational and network resources; frequently, lined into a botnet. (Cybersecurity and Cyberwar)

Zoning. A method of surveillance in which the surveillance area is divided into zones, and surveillants are assigned to cover a specific area. (Words of Intelligence, 2nd Edition, 2011)

Counterintelligence
A variety of views...

Counterintelligence (CI) is probably the most misunderstood secret intelligence function. The work itself has suffered as many definitions as there are intelligence services.

-- Richard Helms, Former DCI and Director CIA

Richard Helms with William Hood, *A Look Over My shoulder: A Life in the Central Intelligence Agency* (New York: Random House 2003), pp. 34-35

"…[C]ountering the intelligence efforts of an adversary is the central function of counterintelligence."
-- Roy Godson, Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence (Washington: Brassey's 1995), pp. xii, 15 & 304

"[Counterintelligence is]…intelligence of a special kind, plus something else…. Counterintelligence collects, stores, analyzes and disseminates information about certain foreign threats to U.S. security and then acts to destroy or neutralize them…. Its end purpose is not the mere collection and analysis of information, but action, and successful action, against those who threaten the security of the United States."
-- Francis McNamara, U.S. Counterintelligence Today, (Washington: The Nathan Hale Institute1985), p. 18

"[Counterintelligence] …must strive to know everything possible about an adversary's intelligence capabilities, including his sources, and methods of collection, his covert actions at influencing and managing our actions and perceptions, and even his culture and thought processes."
-- S. Eugene Poteat, "Counterintelligence Spy vs. Spy, Traitor vs. Traitor," *American Intelligence Journal* (Winter 2000-2001), p. 62

"[Counterintelligence is] …information about an adversary's intelligence operations, capabilities, agents, collection technology, and so on. It is *not* security. It is intelligence on which security policies should be based. Nor is it intelligence about an adversary's policy making or military operations or other nonintelligence capabilities and activities."
-- William E. Odom, Fixing Intelligence For a More Secure America (New Haven: Yale University Press 2003), p. xxix

"…[E]fforts taken to protect one's own intelligence operations from penetration and disruption by hostile nations or their intelligence services. It is both analytical and operational. …not a separate step in the intelligence process but an important function throughout the process."
-- Mark M. Lowenthal, Intelligence: From Secrets to Policy (Washington: CQ Press 2000), p. 98

"…[N]ational effort to prevent foreign intelligence services… from infiltrating our institutions and establishing the potential to engage in espionage, subversion, terrorism, and sabotage."
-- Newton Miller, "Counterintelligence at the Crossroads," Intelligence Requirements for the 1980's: Elements of Intelligence, ed. Roy Godson (Washington: National Strategy Information Center, Inc., 1983), p. 50

"[Counterintelligence] …involves the use of both offensive and defensive measures to: protect sensitive US information and operations from compromise and penetration by foreign intelligence services and other hostile entities; ensure the security and integrity of ongoing US diplomatic, military and intelligence operations; and penetrate, compromise and neutralize hostile operations mounted by foreign intelligence services, terrorist organizations and drug cartels."
-- "Richard L. Haver, "The Ames Case: Catalyst for a National Counterintelligence Strategy," *Defense Intelligence Journal*, Vol. 4 No. 1 (Spring 1995), p. 12

"[Counterintelligence] …includes all information gathered and activities conducted by the government aimed at detecting, analyzing, and countering threat. …the term refers to active operations conducted to counter--through detection, assessment, neutralization, and manipulation--the intelligence operations of foreign countries and groups. …it includes recruitment of foreign intelligence officers, disruption of activities, prosecution of criminal espionage, and manipulation and deception. …it involves the use of surveillance, double agents, and other clandestine techniques."
-- Kenneth E, deGraffenreid, "Countering Hostile Intelligence Activities as a Strategic Threat," National Strategy Information Center, Inc., Sep 1989, p. 3

"Counterintelligence is a term often associated with catching spies. …[It is also] information gathered and activities conducted with the purpose of disrupting and neutralizing the activities of hostile intelligence services."
-- Jeffery Richelson, The US Intelligence Community, 2d ed. (Ballinger Publishing Co., Cambridge MA, 1989), pp. 317 - 330

"Counterintelligence is a critical part of nearly all intelligence activities. When performed properly, the CI function is integral to the intelligence activity itself and part of the overall security of the organization."
-- Aspin-Brown Commission Report, Preparing for the 21st Century: An Appraisal of U.S. Intelligence, 1 March 1996

"[Counterintelligence is] …the most arcane and organizationally fragmented, the least doctrinally clarified, and legally, and thus politically, the most sensitive intelligence activity."
-- William E. Odom, Fixing Intelligence For a More Secure America (New Haven: Yale University Press 2003), p. 167

"CI, the quality-control of intelligence, is the key to the struggle between states and armies for a favorable disparity of knowledge. …CI concerns all other aspects of intelligence; that it must use all of the elements of intelligence as part of itself, while at the same time CI as a whole must be part of the analysis, collection, and covert action practiced by intelligence services. In its inward-looking perspective, CI is a double-check on one's own intelligence operations. In its outward-looking perspective, it is the sharpest weapon in the intelligence arsenal."
-- Angelo Codevilla, Informing Statecraft: Intelligence for a New Century (1992), pp. 325-326

"Counterintelligence… is a strategic instrument available to states to protect themselves and advance their interests in the struggle for power, wealth, and influence. …the end product, the mission of counterintelligence, is action—action to protect against foreigners and action to manipulate foreigners in the service of national goals."
-- Roy Godson, Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence (Washington: Brassey's 1995), pp. 238-239

Across the profession, there are vast differences in understanding of what counterintelligence means, and how it is done, and even the basic terminology it employs.

-- Hon. Michelle VanCleave (former NCIX 2003-2006)

The NCIX and the National Counterintelligence Mission: what has worked, what has not, and why,
Case Study Prepared for the Project on National Security Reform, May 2008

Miscellaneous Thoughts…

"CI… the most secret of secret intelligence activities…."

-- Senate Report 94-755, Church Committee Report, 26 April 1976

"There are far too many in the Intelligence Community who either do not understand counterintelligence or, who understanding its concepts, have climbed to the top of their career ladders by opposing it."

-- Senator Malcolm Wallop, Senate Intelligence Committee (1985)

"…[T]he counterintelligence community is performing its wartime mission every day as agents counter foreign intelligence threats – that's why we call it the silent war."

-- Colonel Stuart A. Herrington, USA (Ret)
Former Commander, US Army Foreign Counterintelligence Activity

"In the spy game, when you're penetrated – when someone is working for the other side inside your security world – they own you."

-- Richard Haver, Former Executive Director for IC Affairs and Former Special Asst to USD(I)

"…I became convinced that no intelligence service can be more effective than its counterintelligence component for very long."

-- Richard Helms, Former DCI and Director CIA
Richard Helms with William Hood, *A Look Over My shoulder: A Life in the Central Intelligence Agency* (2003), pp. 34-35

"In short, there appears to be no abatement in espionage either now or on the horizon."

-- Eli Jacobs, Chairman, Jacobs Panel
SSCI, S. Hrg. 101-1293, "S. 2726 to Improve U.S. Counterintelligence Measures," 101st Congress 2nd session, 1991, p. 9
(Testimony before the Senate Select Committee on Intelligence, 23 May 1980)

"No one can realistically expect that espionage will ever be totally eradicated. But we can take steps to minimize its occurrence and lessen its impact."

-- Senator David L. Boren, Chairman Senate Select Committee on Intelligence, 23 May 1990
SSCI, S. Hrg. 101-1293, "S. 2726 to Improve U.S. Counterintelligence Measures," 101st Congress 2nd session, 1991, p. 9

CI... A Never-Ending Necessity

*The Ten Commandments of Counterintelligence**

- I -- Be Offensive
- II -- Honor Your Professionals
- III -- Own the Street
- IV -- Know Your History
- V -- Do Not Ignore Analysis
- VI -- Do Not Be Parochial
- VII -- Train Your People
- VIII -- Do Not Be Shoved Aside
- IX -- Do Not Stay Too Long
- X -- Never Give Up

-- James M. Olson, Former Chief of CIA Counterintelligence
(served 31 years in the CIA)

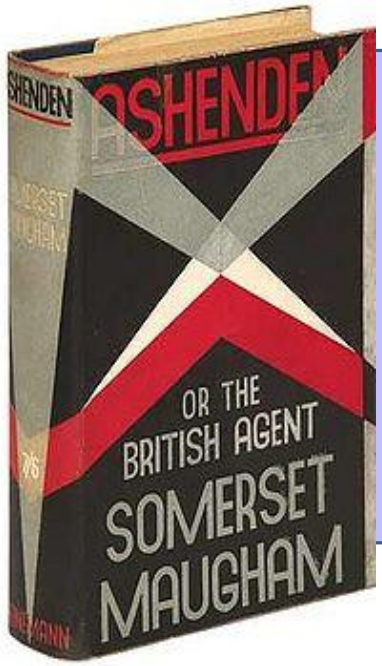
---

* James M. Olson, "The Ten Commandments of Counterintelligence," Center for the Study of Intelligence, CIA, *Studies in Intelligence*, Volume. 45 ,No. 5, Fall-Winter 2001, pp. 81-87; available online at <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/article08.html>
Also available online at: <http://www.dtic.mil/dtic/tr/fulltext/u2/a529667.pdf>

To advance its interests, the United States will need to do what prudent statesmen have done in different ways for centuries: ensure that counterintelligence is adequate to the task.

-- Roy Godson, Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence (Washington: Brassey's 1995), pp. 238-239

Need for Counterintelligence…



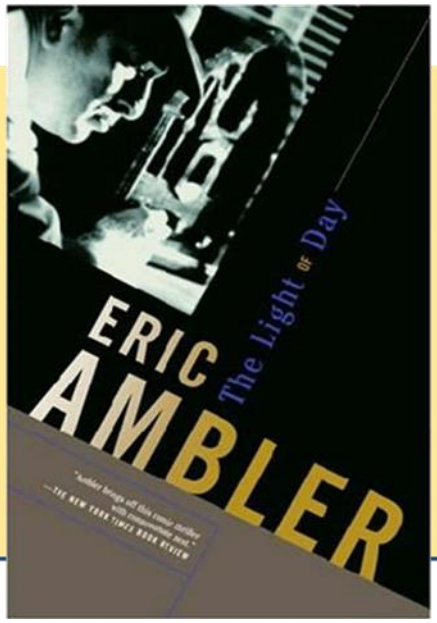
But there will always be espionage and there will always be counter-espionage. Though conditions may have altered, though difficulties may be greater…, there will always be secrets which one side jealously guards and which the other will use every means to discover; there will always be men who from malice or for money will betray their kith and kin and there will always be men who, from love of adventure or a sense of duty, will risk a shameful death to secure information valuable to their country.

W. Somerset Maugham, *Ashenden: or the British Agent* (1928)

Inescapable Truth… there will always be Spies

We must develop effective espionage and counterespionage services and must learn to subvert, sabotage and destroy our enemies by more clever, more sophisticated and more effective methods than those used against us.

-- Doolittle Report (1954)*



I think if I were asked to single out one specific group of men, one category as being the most suspicious, unbelieving, unreasonable, petty, inhuman, sadistic, double-crossing set of bastards in any language, I would say without hesitation the people who run counterespionage departments.

-- Eric Ambler, *Light of Day* (1962)

---

* *Report on the Covert Activities of the Central Intelligence Agency* (aka Doolittle Report), 30 Sep 1954, redacted copy (originally classified TOP SECRET). Lt Gen James H. Doolittle was the Chairman of this Presidential directed Special Study Group. One result of the report was the creation of a counterintelligence staff within CIA which was run by James J. Angleton from 1954 to 1974. Redacted copy available online at: <http://www.foia.cia.gov/helms/pdf/doolittle_report.pdf>

COUNTERINTELLIGENCE—*THE WILDERNESS OF MIRRORS*

Counterintelligence officers—people who specialize in catching spies—work in a part of the profession so labyrinthine that it is often referred to as a "wilderness of mirrors"…

-- H. Keith Melton and Robert Wallace, *The Official CIA Manual of Trickery and Deception* (2009)

One final perspective…

Counterintelligence… a wilderness of mirrors

"A wilderness of mirrors" -- a description of counterintelligence attributed to James J. Angleton. It comes from T.S. Eliot's poem "Gerontion" (1920); also the title of a 1980 book authored by David C. Martin about CIA counterintelligence.

Angleton was CIA's Chief of the Counterintelligence from 1954 until his retirement in 1974. In December 1974, Angleton was basically forced into retirement by the Director of CIA (William Colby), who became convinced that Angleton's "labyrinthine" approach to counterintelligence severely hampered the Agency's primary mission -- clandestine HUMINT collection.

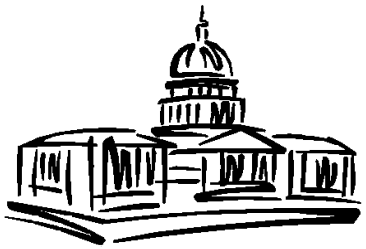
THE CHALLENGE: *THINKING THE UNTHINKABLE*

Most fundamental to counterintelligence–as true today as ever–is the need to "think the unthinkable." Yet this is one of the most difficult attitudes to instill and maintain because it runs contrary to human nature, especially in open societies like the United States. …

Today, thinking the unthinkable is not easier, but it is just as critical to our national security.

As we proceed to face the counterintelligence threat of the 21st century, we are faced with a host of challenges: some new, others ancient and deeply rooted in human weakness, and some not yet even invented.

-- Honorable Richard Shelby, Chairman of the U.S. Senate Select Committee on Intelligence (2001)*



To all Counterintelligence professionals --

Combating adversarial intelligence threats is a demanding and challenging profession… CI is a strategic instrument of national security underappreciated by most. A sincere thank you for all you do!!!!!!

-- COL Mark L. Reagan (USA Ret)
Editor, *Terms & Definitions of Interest for Counterintelligence Professionals*

CI a strategic enabler and a national asset… Critical to U.S. National Security

---

* Quote from "Intelligence and Espionage in the 21st Century," Heritage Lectures - No. 705, The Heritage Foundation, 18 May 2001

Key Sources

A Spy's Journey: A CIA Memoir by Floyd L. Paseman. Minneapolis, MN: Zenith Press, 2004 (Glossary pp. 290-296) – cited as A Spy's Journey.

Consumer's Guide to Intelligence (PAS 95-00010), CIA, Public Affairs Staff, July 1995; updated, 2d ed. 1996; replaced with ***National Intelligence: A Consumer's Guide - 2009***, Office of Director National Intelligence (ODNI). Copy available online at: <www.dni.gov/reports/IC_Consumers_Guide_2009.pdf>

Counterintelligence Community Lexicon (CI Community Lexicon), National Counterintelligence Center, NACIC 2000-10004, June 2000 – cited as CI Community Lexicon.

Cyber Threats to National Security, Symposium Five: Keeping the Nation's Industrial Base Safe From Cyber Threats, co-sponsored by USNI, CACI and Center for Security Policy, 2011 -- cited as Cyber Threats to National Security, Symposium Five, 2011. Copy available online at: <http://asymetricthreat.net>

Cybersecurity and Cyberwar: What Everyone Needs to Know by P.W. Singer and Allan Friedman. New York, NY: Oxford University Press, 2014 – cited as Cybersecurity and Cyberwar.

DoD Dictionary of Military and Associated Terms, Joint Publication 1-02. Copy available online at: <http://www.dtic.mil/doctrine/dod_dictionary/> (also available at <https://jdeis.js.mil>) – cited as JP 1-02.

Domestic Investigations and Operations Guide [Redacted Version], Federal Bureau of Investigation, 15 Oct 2011. Copy available on line at: <http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version>

Encyclopedia of the Central Intelligence Agency by W. Thomas Smith, Jr. New York, NY: Checkmark Books, 2003 – cited as Encyclopedia of the CIA.

FBI Foreign Counterintelligence Terms in *Spy vs. Spy* by Ronald Kessler (1988) – cited as FBI FCI Terms.

Fair Play: The Moral Dilemmas of Spying by James M. Olson. Washington, DC: Potomac Books, Inc., 2006.

Glossary of Intelligence Terms and Definitions, The Intelligence Community Staff (ICS), Office of the Director of Central Intelligence, 1978; updated June 1989 – cited as ICS Glossary.

Glossary of Key Information Security Terms, NISTIR 7298 Revision 2, May 2013. Copy available at: <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>

Glossary of Security Terms, Definitions, and Acronyms, Intelligence Community Standard - Number 700-1 (previously numbered ICS 2008- 700-1), 4 April 2008 – cited as IC Standard 700-1 (33 pages). Available on line at: <http://www.ncix.gov/publications/policy/docs/ICS_700-01_Glossary_of_Security_Terms_Definitions_and_Acronyms.pdf>

Glossary of Security Terms, Definitions, and Acronyms, Defense Security Service, November 2012 – cited as DSS Glossary (337 pages). Copy available <http://www.cdse.edu/documents/cdse/Glossary_Handbook.pdf>

Glossary of Spy Terms, CI Centre – cited as CI Centre Glossary. Originally available online at <http://cicentre.com/LINKS_Reference_Material.htm> -- site now requires membership to access, see <http://www.cicentre.com/>

Historical Dictionary of Cold War Counterintelligence by Nigel West, Maryland: Scarecrow Press, Inc., 2007.

Human Derived Information Lexicon Terms and Definitions for HUMINT, Counterintelligence, and related Activities, April 2008 – cited as HDI Lexicon.

Intelligence Essentials for Everyone, by Lisa Krizen, Occasional Paper Number Six, Washington DC: DIA Joint Military Intelligence College, June 1999. Copy available online at: <http://www.dia.mil/college/pubs/8342.htm>

McAfee Labs - Threat Glossary**,** undated. Copy available online at: <http://www.mcafee.com/us/mcafee-labs/resources/threat-glossary.aspx >

National Information Assurance (IA) Glossary, Committee on National Security Systems Instruction (CNSSI) No. 4009, 26 Apr 2010. Copy available on line at: <http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf> Also at <http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf>

National Intelligence: A Consumer's Guide – 2009. Copy available online at: <http://www.dni.gov/reports/IC_Consumer's_Guide_2009.pdf>

National HUMINT Glossary, unclassified, 15 pages, undated. Copy available on JWICS at: <http://jwc-nhb-nhc03.idiss.cia.ic.gov/intelink/NationalHUMINTGlossary.pdf>

OPSEC Glossary of Terms. Interagency OPSEC Support Staff. Copy available online at: <http://www.ioss.gov/docs/definitions.html>

Spy Book – The Encyclopedia of Espionage by Norman Polmar and Thomas B. Allen, New York: Random House, revised edition, 2002 – cited as Spy Book.

Spy Dust: Two Masters of Disguise Reveal the Tools and Operations that Helped Win the Cold War by Antonio and Jonna Mendez, with Bruce Henderson, New York: Atria Books, 2002; Glossary pp. 283-298 (copy of glossary available on line at: <http://www.themasterofdisguise.com/glossary.html>) – cited as Spy Dust.

Spycraft: The Secret History of the CIA's Spytechs from Communism to Al-Qaeda by Robert Wallace and H. Keith Melton, New York: Penguin Group, 2008 – cited as Spycraft.

U.S. National Intelligence – An Overview 2011, Office of the Director of National Intelligence. Copy available online at: <http://www.odni.gov/IC_Consumers_Guide_2011.pdf>

Words of Intelligence: An Intelligence Professional's Lexicon for Domestic and Foreign Threats, 2nd Edition, by Jan Goldman. Lanham, MD: Scarecrow Press, Inc., 2011 – cited as Words of Intelligence.

Notes:

DoD issuances (e.g., directives, instructions, DTMs) approved for public release available on the Internet from the DoD Issuances Website at: <http://www.dtic.mil/whs/directives/>. Also see <http://www.dtic.mil/doctrine/doctrine/doctrine.htm>.

Department of the Army publications at <https://www.apd.army.mil/> Also Army Field Manuals (FMs) are available online at: <http://armypubs.army.mil/doctrine/active_fm.html> (requires an AKO account). Selected Army publications are also at: <http://www.fas.org/irp/doddir/army/index.html>

Air Force doctrine at <http://www.cadre.maxwell.af.mil>

Navy doctrine at <https://ndls.nwdc.navy.mil>

Intelligence Community Intelligence Directives (ICDs), unclassified ICDs available online at: <http://www.dni.gov/electronic_reading_room.htm>
Also see <http://www.dni.gov/index.php/intelligence-community/ic-policies-reports/intelligence-community-directives>

United States law at <http://uscode.house.gov/lawrevisioncounsel.shtml>. United States Code (USC) also available online from the Government Printing Office online data base at: <http://www.gpoacess.gov/uscode/index.html>

Key DoD Counterintelligence Policy References

DoD Regulations

- *DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, 7 Dec 1982; supplemented by DTM 08-11, Intelligence Oversight Policy Guidance, 26 Mar 2008 (w/ change 3 dated 27 Jul 2012)**

DoD Directives

- DoDD 5240.01, DoD Intelligence Activities, 27 Aug 2007 (with change 1 dated 29 Jan 2013)
- *DoDD O-5240.02, Counterintelligence, 20 Dec 2007 (with change 1 dated 30 Dec 2010)**
- DoDD 5240.06, Counterintelligence Awareness and Reporting (CIAR), 17 May 2011 (with change 1 dated 30 May 2013)
- *DoDD 5210.48, Polygraph and Credibility Assessment Program, 25 Jan 2007 (with change 2 dated 15 Nov 2013)**
- DoDD S-3325.09, (U) Oversight Management, and Execution of Defense Clandestine Source Operations, 9 Jan 2013 (with change 1 dated 13 Jun 2013)

DoD Instructions

- *DoDI 5240.04, Counterintelligence Investigations, 2 Feb 2009 (with change 1 dated 15 Oct 2013)**
- DoDI 5240.05, Technical Surveillance Countermeasures (TSCM) Program, 3 Apr 2014
- DoDI C-5240.08, Counterintelligence Security Classification Guide (U), 28 Nov 2011
- *DoDI S-5240.09, Offensive Counterintelligence Operations (OFCO) (U), 29 Oct 2008**
- DoDI 5240.10, Counterintelligence in the Combatant Commands and Other DoD Components, 5 Oct 2011 (with change 1 dated 15 Oct 2013)
- DoDI S-5240.15, Force Protection Response Group (FPRG) (U), 20 Oct 2010 (with change 1)
- DoDI 5240.16, DoD Counterintelligence Functional Services (CIFS), 27 Aug 2012 (with change 1)
- DoDI S-5240.17, (U) Counterintelligence Collection Acclivities (CCA), 14 Mar 2014
- DoDI 5240.18, Counterintelligence Analysis and Production, 17 Nov 2009 (with change 1)
- DoDI 5240.19, Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP), 31 Jan 2014
- DoDI O-5240.21, Counterintelligence Inquires, 14 May 2009 (with change 2 dated 15 Oct 2013)
- DoDI 5240.22, Counterintelligence Support to Force Protection, 24 Sep 2009 (with change 1)
- DoDI S-5240.23, Counterintelligence Activities in Cyberspace (U), 13 Dec 2010 (with change 1)
- DoDI O-5240.24, Counterintelligence Activities Supporting Research, Development, and Acquisition (RDA), 8 Jun 2011 (with change 1 dated 15 Oct 2013)
- DoDI 5240.25, Counterintelligence Badge and Credentials, 30 March 2012 (with change 1)
- DoDI 5240.26, Countering Espionage, International Terrorism, and the Counterintelligence Insider Threat, 4 May 2012 (with change 1 dated 15 Oct 2013)
- DoDI 5240.27, Joint Counterintelligence Training Academy (JCITA), 13 Nov 2013
- DoDI 3305.11, DoD Counterintelligence Training, 19 Mar 2007 (with change 2 dated 15 Oct 2013)
- DoDI 3305.12, Intelligence and Counterintelligence Training of Non-U.S. Persons, 25 Oct 2007 (with change 2 dated 15 Oct 2013)
- DoDI 5210.91, Polygraph and Credibility Assessment (PCA) Procedures, 12 Aug 2010 (with chg 1)
- *DoDI 5200.39, Critical Program Information (CPI) Protection within DoD, 16 Jul 2008 (with chg1)**

DoD Manuals

- DoD Manual S-5240.09-M, OFCO Procedures and Security Classification Guide (U), 13 Jan 2011

Under Development

- *DoD Manual S-5240.26-M, (U) DoD Counterintelligence Insider Threat Program (CIITP)**

**** under revision / under development***

Intelligence Community & Misc. Government Websites

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI): www.dni.gov
NATIONAL COUNTERINTELLIGENCE EXECUTIVE (NCIX): www.ncix.gov
NATIONAL COUNTERTERRORISM CENTER (NCTC): www.nctc.gov
DEPARTMENT OF DEFENSE (DoD): www.defense.gov (also see: www.defenselink.mil)
- Defense Intelligence Agency (DIA): www.dia.mil
- Defense Security Service (DSS): www.dss.mil
- Army: www.army.mil
  -- Intelligence & Security Command (INSCOM): www.inscom.army.mil
  -- 902d Military Intelligence Group: www.inscom.army.mil/MSC/902MIG.aspx
  -- Intelligence Knowledge Network (IKN): https://www.ikn.army.mil/
- Air Force: www.af.mil
  -- Air Force Office of Special Investigations (AFOSI): www.osi.andrews.af.mil
  -- Air Force ISR Agency: www.afisr.af.mil
- Navy: www.navy.mil
  -- Naval Criminal Investigative Service (NCIS): www.ncis.navy.mil
  -- Office of Naval Intelligence (ONI): www.nmic.navy.mil
- Marine Corp: www.marines.mil
  -- USMC Intelligence: www.hqinet001.hqmc.usmc.mil/DirInt/default.html

NATIONAL SECURITY AGENCY (NSA): www.nsa.gov
NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY (NGA): www.nga.mil
NATIONAL RECONNAISSANCE OFFICE (NRO): www.nro.gov
CENTRAL INTELLIGENCE AGENCY (CIA): www.cia.gov
DEPARTMENT OF JUSTICE (DoJ): www.usdoj.gov
- Federal Bureau of Investigation (FBI): www.fbi.gov
- Drug Enforcement Agency (DEA): www.dea.gov
- DoJ Office of Legal Counsel (OLC): www.usdoj.gov/olc
- DoJ National Security Division (NSD): www.usdoj.gov/nsd

DEPARTMENT OF HOMELAND SECURITY (DHS): www.dhs.gov
- U.S. Coast Guard (USCG): www.uscg.mil
- Customs and Border Protection (CBP): http://cbp.gov/
- Immigrations and Customs Enforcement (ICE): www.ice.gov
- Transportation Security Administration (TSA): www.tsa.gov
- U.S. Secret Service (USSS): www.secretservice.gov
- DHS Office of Intelligence & Analysis: www.dhs.gov/xabout/structure/gc_1220886590914.shtm

DEPARTMENT OF STATE: www.state.gov
- Bureau of Diplomatic Security: www.state.gov/m/ds

DEPARTMENT OF TREASURY: www.ustreas.gov
- Office of Terrorism and Financial Intelligence: www.ustreas.gov/offices/enforcement/
- Financial Crimes Enforcement Network (FinCEN): www.fincen.gov

DEPARTMENT OF ENERGY: www.energy.gov
INTERAGENCY OPSEC SUPPORT STAFF (IOSS): www.ioss.gov
WHITE HOUSE: www.whitehouse.gov
U.S. SENATE: www.senate.gov
- Senate Select Committee on Intelligence (SSCI): www.intelligence.senate.gov

U.S. HOUSE OF REPRESENTATIVES: www.house.gov
- House Permanent Select Committee on Intelligence (HPSCI): www.intelligence.house.gov

LIBRARY OF CONGRESS: www.loc.gov
- Federal legislative information available at: www.thomas.loc.gov