FMI 3-34.119/MCIP 3-17.01

IMPROVISED EXPLOSIVE DEVICE DEFEAT

September 2005

Expires September 2007

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This protection applies to publications required solely for official use and to those containing valuable technical or operational information. This determination was made on 10 August 2005. Other requests for this document will be referred to Commandant, United States Army Engineer School, ATTN: ATSE-DD, 320 MANSCEN Loop, Suite 336, Fort Leonard Wood, Missouri 65473-8929.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

HEADQUARTERS, DEPARTMENT OF THE ARMY
UNITED STATES MARINE CORPS

Foreword

Attacks from improvised explosive devices (IEDs) are one of the major causes of Soldiers and Marines being killed in action (KIA) and wounded in action (WIA). The construct of IED defeat operations supports the National Security Strategy to defeat terrorism and prevent attacks against the United States (U.S.) and coalition forces. It also supports Joint Vision 2020 and the Army Campaign Plan. A key component is the implementation of an integrated IED strategy to counter IED threats and support the Global War on Terrorism. Attaining this goal requires the steady infusion of integrated doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) solutions to counter IED threats to meet the Army's requirements. The IED threat and the protection of our Soldiers and Marines are an extremely important mission. Until recently, there was no single proponent designated to coordinate DOTMLPF solutions for these types of explosive hazards impacting our freedom of maneuver.

In August 2004, the Department of the Army (DA) assigned the United States Army Training and Doctrine Command (TRADOC) as the Army specified proponent for IED defeat. TRADOC then assigned the Maneuver Support Center (MANSCEN) to conduct a mission analysis and determine resource requirements for implementing an integrated DOTMLPF strategy to counter IED threats. MANSCEN was further tasked to establish an IED Defeat Integrated Capabilities Development Team (ICDT) to develop an integrated DOTMLPF strategy to counter IED threats.

This IED Defeat ICDT will interface with the Joint Improvised Explosive Device Defeat (JIEDD) Task Force (TF), and primarily the IED Defeat Joint Integrated Product Team (JIPT), to provide DOTMLPF analysis and assign the appropriate proponency through the process as necessary. The ICDT will also identify and resolve the remaining capability gaps and is tasked with the development, writing, and publication of this field manual interim (FMI) on IED defeat operations.

FMI 3-34.119/Marine Corps Information Publication (MCIP) 3-17.01 is a new FMI publication based on the contemporary operational environment (COE) and emerging tactics, techniques, and procedures (TTP). The emergence of enemy use of IEDs as a preferred method of asymmetric attack, coupled with a strong demand from the field for doctrine to address IED defeat, mandates the development of new doctrine. This manual will serve as a reference for force commanders and staff, training developers, and doctrine developers throughout the Army. Take time to review the materials in this publication and incorporate the doctrine and TTP into your daily operations. The information contained in these pages is useful to all service members regardless of rank.

Randal R Castro

RANDAL R. CASTRO
MAJOR GENERAL, U.S. ARMY
COMMANDING

This publication is available at

Army Knowledge Online

www.us.army.mil

Field Manual Interim
No. 3-34.119
Marine Corps Information Publication
No. 3-17.01

Headquarters,
Department of the Army
United States Marine Corps
Washington, DC, 21 September 2005
Expires 21 September 2007

IMPROVISED EXPLOSIVE DEVICE DEFEAT

Contents

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This protection applies to publications required solely for official use and to those containing valuable technical or operational information. This determination was made on 10 August 2005. Other requests for this document will be referred to Commandant, United States Army Engineer School, ATTN: ATSE-DD, 320 MANSCEN Loop, Suite 336, Fort Leonard Wood, Missouri 65473-8929.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Preface

FMI 3-34.119/MCIP 3-17.01 establishes doctrine (fundamental principals and TTP) for the defeat of adversary IED operations. It is based on existing doctrine and lessons learned from recent combat operations.

This publication applies to the Active Army, the Army National Guard (ARNG)/the Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR). The primary audience for this FMI is commanders, leaders, and staffs at corps-level and below.

To make this manual useful to leaders involved in IED defeat operations regardless of where these operations may occur, the doctrine contained herein is broad in scope and involves principles applicable to various theaters. This FMI is not focused on any region or country. IED operations have some common characteristics, but their methods of implementation may vary widely.

FMI 3-34.119/MCIP 3-17.01 is not a stand-alone document. Readers must be familiar with the fundamentals of assured mobility found in Field Manual (FM) 3-34. This manual uses assured mobility as a framework to assist leaders with planning and executing IED defeat operations. Additionally, this FMI incorporates lessons learned and major studies from sources across the Army and joint community. It focuses on the asymmetric threats and establishes doctrine to defeat those threats.

> ***Note.*** An FMI is a DA publication that provides expedited delivery of urgently needed doctrine that the proponent has approved for use without placing it through the standard development process. Unless an FMI is rescinded, the information it disseminates is incorporated into a new or revised FM. An FMI expires after two years, unless superseded or rescinded.

This manual—

- Provides doctrinal guidance for commanders and staffs for planning, preparing for, and executing and assessing IED defeat operations.
- Serves as an authoritative reference for emerging doctrine, TTP, materiel and force structure, institutional and unit training, and standing operating procedures (SOPs) for IED defeat operations.
- Outlines the critical roles and responsibilities of staff cells for IED defeat operations.

Terms that have joint or Army definitions are identified in both the glossary and the text. Glossary references: The glossary lists most terms used in FMI 3-34.119/MCIP 3-17.01 that have joint or Army definitions. Terms for which FMI 3-34.119/MCIP 3-17.01 is the proponent FMI (the authority) are indicated with an asterisk in the glossary. Text references: Definitions for which FMI 3-34.119/MCIP 3-17.01 is the proponent FMI are printed in boldface in the text. These terms and their definitions will be incorporated into the next revision of FM 1-02. For other definitions in the text, the term is italicized and the number of the proponent FM follows the definition.

The proponent for this publication is United States Army Training and Doctrine Command. The preparing agency is the Doctrine Development Division, United States Army Engineer School. Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commandant, United States Army Engineer School, ATTN: ATSE-DD, Suite 336, 320 MANSCEN Loop, Fort Leonard Wood, Missouri 65473-8929.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Introduction

> *"This is not a new war. Our enemies have been waging it for some time, and it will continue for the foreseeable future. As President Bush has stated, 'This is a different kind of war against a different kind of enemy.' It is a war we must win, a war for our very way of life."*
>
> General Peter J. Schoomaker,
Chief of Staff of the Army
Arrival Message, 1 August 2003

The proliferation of IEDs on the battlefield in both Iraq and Afghanistan has posed the most pervasive threat facing coalition forces in those theaters. The persistent effectiveness of this threat has influenced unit operations, U.S. policy, and public perception. IEDs are a weapon of choice and are likely to remain a major component of the Global War on Terrorism for the foreseeable future.

The definitive history of IEDs has not been extensively documented. However, many specific incidents in the last 100 years have been well documented. Recently there has been a trend of increasing terrorist acts against the United States. These attacks have increased in their frequency, in their level of sophistication, and in their lethality. For example, the Marine barracks in Beirut, Lebanon, was attacked with a truck bomb that killed 241 U.S. Marines in 1983. This was followed by the bombing of Pan American Flight 103 over Lockerbie, Scotland, in 1988. (The plane carried passengers from 21 countries, but 189 of the 259 on board were Americans; the crash also killed 11 people on the ground.) In the first terrorist attack on the World Trade Center in New York City in 1993, a truck bomb failed to cause the desired number of casualties but nevertheless demonstrated the ability to attack the U.S. homeland. In 1996, another truck bomb killed 19 U.S. Soldiers and injured 372 at the Khobar Towers housing complex in Dhahran, Saudi Arabia. The violence continued with the bombings of the United States embassies in Kenya and Tanzania in 1998 and the United States Ship (USS) Cole in the port of Aden, Yemen, in 2000.

With the development of sufficiently powerful, stable, and accessible explosives, a preferred weapon of a terrorist is a bomb or IED. As a weapon, bombs are efficient as they allow a person or group to strike with great destructive effect. The sophistication of the device depends on the maker. They can range from being very simple to very complex with booby traps, antihandling devices, and sophisticated electronic initiation devices to prevent disarming. Generally, bombs can be triggered in a variety of ways. A timer is common and can be set hours in advance. Remote-controlled detonators with a limited range allow the timing of the detonation exactly. Bombs can be manufactured out of many household products (including fertilizer and batteries), but most sophisticated bombs use a small amount of explosive to trigger a larger quantity of poorer grade explosive material. Bombs do not have to be large to be effective. Most bombs are small and are directed at individual targets, such as military personnel or politicians. Often these are planted along a roadside and detonated as a vehicle passes. Larger devices can be placed in vehicles parked along the roadway or driven into the target by suicide bombers willing to give up their lives for the cause.

This manual provides commanders, leaders, and staffs with fundamental principals and TTP for the defeat of adversary IED operations. Based on current doctrine, this manual also incorporates the lessons learned from recent combat operations. The following briefly describes the chapters and appendixes:

- Chapter 1 defines IED defeat operations. It describes how commanders and their staff use the IED defeat framework to assist with planning, preparing, executing, and assessing IED operations.
- Chapter 2 provides a description of the COE in which IEDs are employed. It explains how and why the enemy uses IEDs to disrupt friendly operations from a strategic to a tactical perspective.
- Chapter 3 defines how threat forces operate and how they use IEDs.

- Chapter 4 provides the characteristics of IEDs and offers threat TTP on their use and employment. It describes the components and common initiation methods. It also provides basic indicators and locations of where IEDs can be used.
- Chapter 5 identifies U.S. government agencies that are involved in IED defeat operations. It is not an all-inclusive list. It covers agencies from the strategic level to the operational level and includes intelligence and technology development organizations. This chapter provides basic mission statements of the organizations.
- Chapter 6 provides guidance for a leader upon encountering an IED. All units must be able to maintain operations despite these hazards. It briefly describes military search and route clearance operations.
- Chapter 7 provides an overview of the planning processes of the Army and describes how a commander and his staff integrate IED defeat considerations into unit plans. Additionally, it discusses intelligence preparation of the battlefield (IPB), targeting, and risk management as additional tools to assist the commander and staff in integrating IED defeat considerations throughout. This chapter also offers planning considerations for IED defeat based on the factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). The METT-TC factors are not all-inclusive but serve as a base for further development depending on the situation.
- Chapter 8 provides information to develop a training strategy for preparing units for IED defeat operations.
- Appendix A complies with current Army directives which state that the metric system will be incorporated into all new publications.
- Appendixes B through H provide greater depth to the chapters and offer basic suggestions for conducting IED defeat operations.

Chapter 1

Fundamentals

With the proliferation of technology and access to explosive materials, many enemy groups have come to rely on IEDs as a primary means of attack. As seen in recent conflicts in Afghanistan and Iraq, IED attacks have destabilizing and destructive effects on friendly operations. This chapter defines IED defeat operations and provides commanders, leaders, and staffs with a framework to effectively counter-IED attacks. Additionally, this chapter provides key definitions associated with IED defeat.

SECTION I – OPERATIONS

1-1. The focus of IED defeat is often on the IED itself. However, the device is merely the end product of a complex set of enemy activities. An IED attack is the result of a planned tactical operation with several key elements that work in a coordinated and synchronized manner to attain a desired result. The results can have operational or strategic impacts, not solely because of the military value of the target, but also the psychological impact on units, the local population, the world community, and political leaders.

1-2. Successful IED defeat operations begin with a thorough understanding of the enemy and the common activities associated with an IED attack. Activities include leadership, planning, financing, materiel procurement, bomb making, target selection, recruiting, and attack execution. A holistic approach to understanding the requirements of an IED attack assists commanders and planners in identifying vulnerabilities. These vulnerabilities can be exploited to break the operational chain of events of the enemy. See Chapter 3 for a detailed discussion on enemy IED attack characteristics.

1-3. IED defeat operations are unit activities that are planned, prepared for, executed, and assessed to identify, deter, and mitigate the effects of an IED attack. As part of the broader mission of the unit, these activities are conducted to predict, detect, prevent, avoid, neutralize, and protect the force from IED attack. IED defeat operations are not a staff- or function-specific responsibility. IED defeat cuts across the battlefield operating systems (BOS) and requires the entire staff to consider all options to eliminate the IED threat. The goal is to identify and defeat enemy leaders, suppliers, trainers, enablers, and executors responsible for the employment of IEDs, while protecting the force from the effects of an IED attack.

SECTION II – FRAMEWORK

1-4. The IED defeat framework derives from the imperatives and fundamentals of assured mobility that are found in FM 3-34. Assured mobility encompasses those actions that enable commanders with the ability to deploy, move, and maneuver where and when they desire (without interruption or delay) and to achieve the mission (see FM 3-34).

1-5. The IED defeat framework is a parallel construct to assured mobility and enables commanders and staffs to plan and take proactive measures to seek out and defeat IED events before they occur. It also provides a methodology for addressing IED events upon contact and subsequent detonation. The IED defeat framework (Figure 1-1, page 1-4) consists of the following:

- **Predict activities.** These activities are used to identify and understand enemy personnel, equipment, infrastructure, TTP, support mechanisms, or other actions to forecast specific enemy IED operations directed against U.S. interests. This is driven largely by success in analysis in the requirements management. Predict activities assists in—
    - Identifying patterns of enemy behavior.
    - Identifying emerging threats.
    - Predicting future enemy actions.
    - Prioritizing intelligence, surveillance, and reconnaissance (ISR) missions.
    - Exploiting IED threat vulnerabilities.
    - Targeting enemy IED attack nodes (such as funding and supplies).
    - Disseminating alert information rapidly to specific users.
    - Analyzing forensics and enabling better on-scene technical analysis.
- **Detect activities.** These activities contribute to the identification and location of enemy personnel, explosive devices, and their component parts, equipment, logistics operations, and infrastructure in order to provide accurate and timely information. These actions assist in the efforts to interdict and destroy these activities. Detect activities aid in—
    - Detecting and identifying explosive material and other IED components.
    - Detecting chemical, biological, radiological, and nuclear (CBRN) material.
    - Recognizing suicide bombers.
    - Conducting forensic operations to track bomb makers and/or handlers.
    - Conducting persistent surveillance.
    - Training to improve detection of IED indicators by digital means.
    - Developing priority information requirements (PIR) tied to IED operations decisive points. Linking and synchronizing detection assets to PIR-related named areas of interest (NAIs).
    - Using detection means across the full range available (from imagery, mechanical-clearance operations, search techniques, dogs, and so forth).
    - Recognizing individual Soldier actions and awareness in all activities.
- **Prevent activities.** These activities disrupt and defeat the IED operational chain of events. The actions focus on the target to interdict or destroy key enemy personnel (bomb makers, leaders, and financiers), the infrastructure/logistics capabilities (suppliers and bomb factories), and surveillance/targeting efforts (reconnaissance and overmatch operations) before emplacement of the device. They also include actions to deter public support for the use of IEDs by the enemy. Prevent activities aid in—
    - Disrupting enemy operations and their support structure.
    - Denying critical IED-related supplies to the enemy.
    - Increasing awareness of enemy TTP and their effectiveness.
    - Denying the enemy the opportunity to emplace IEDs (through presence patrols, observation posts, checkpoints, aggressive surveillance operations, and so forth).
    - Rewarding local nationals' cooperation in determining the locations of caches, bomb making, or emplacing activities.
    - Denying easily concealed locations (such as trash piles and debris along sides of primary routes) and removing abandoned vehicles along routes.

- **Avoid activities.** These activities keep friendly forces from IEDs when prevention activities are not possible or have failed. Avoid activities include—
  - Increasing situational understanding (SU) of the area of operations (AOs) and continually refining the common operational picture (COP) and the timely and accurate dissemination of related information.
  - Ensuring timely and accurate status reporting and tracking.
  - Altering routes and routines.
  - Marking and bypassing suspected IEDs.
- **Neutralize activities.** These activities contribute to the destruction or reduction of enemy personnel, explosive devices, or supplies. They can be proactive or reactive in nature.
  - Proactive activities include conducting operations to eliminate or interrupt the enemy's leaders, suppliers, trainers, enablers, and executors responsible for the employment of IEDs against coalition forces.
  - Reactive activities include conducting controlled detonations or render safe procedures (RSPs) against identified IEDs, caches, captured enemy ammunition (CEA), and so forth. Explosive ordnance disposal (EOD) forces are the only personnel authorized to render safe IEDs.
- **Protect activities.** These activities improve the survivability of IED targets through hardening, awareness training, or other techniques. Protect activities include—
  - Disrupting, channeling, blocking, or redirecting energy and fragmentation.
  - Creating greater standoff distances to reduce the effect that IEDs have on their intended targets.
  - Incorporating unmanned platforms.
  - Using jamming devices.
  - Reducing time and distance in which intended targets are within IED range.
  - Accelerating processes and increasing the effectiveness by which reaction and evacuation operations are conducted.
  - Providing blast and fragmentation mitigation for platforms, structures, and personnel.
  - Avoiding establishing patterns and predictable forms of behavior.
  - Conducting proper precombat inspections (PCIs) and rehearsals for all operations.
  - Treating every operation as a combat mission (from a simple convoy to daily forward operating base [FOB] security).

1-6. The IED defeat framework (Figure 1-1, page 1-4) can be broken down into two major subelements—proactive (predetection) and reactive (postdetection).

- Proactive elements are actions taken by friendly forces to predict, detect, prevent, avoid, neutralize, and protect against IED events.
- Reactive elements are actions taken by friendly forces to detect, avoid, neutralize, and protect against IED events.

Note. The fundamentals of detect, avoid, neutralize, and protect applies to both sides of the framework (proactive and reactive measures).

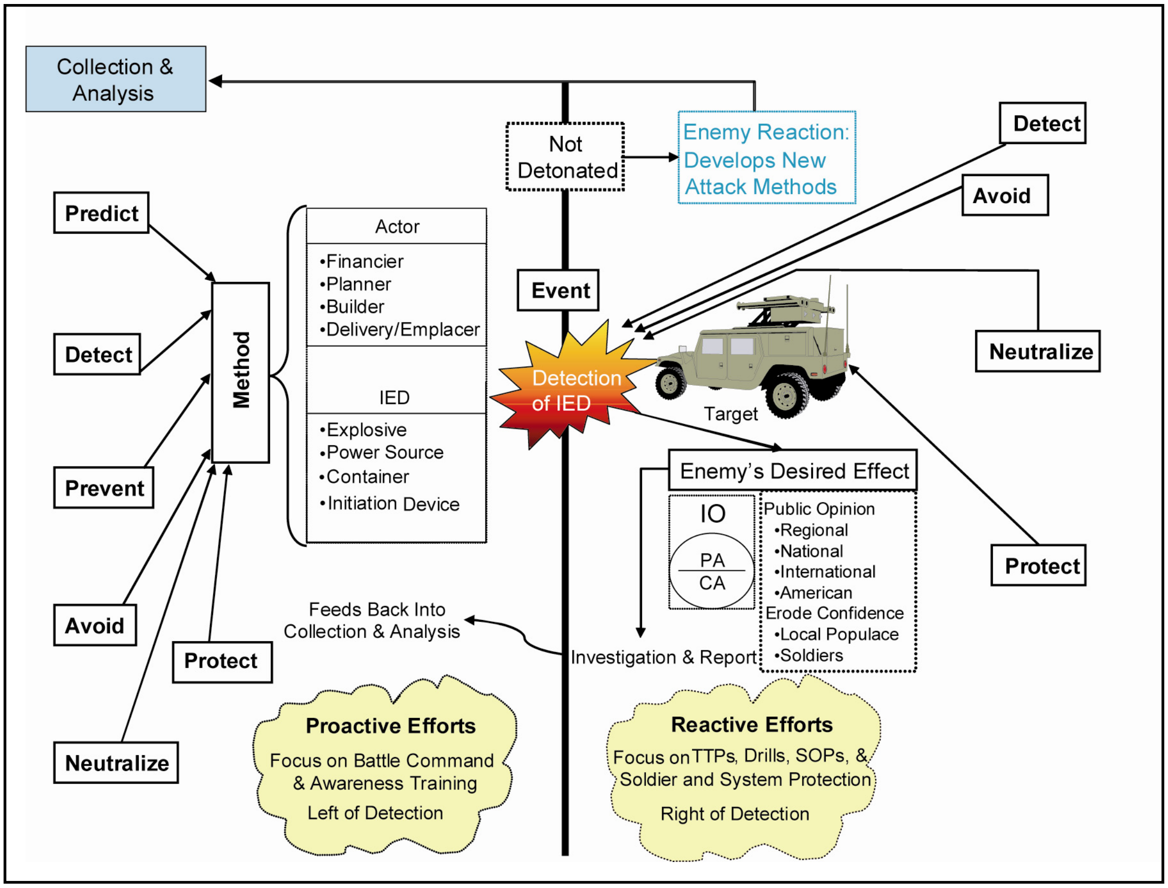

Figure 1-1. IED defeat framework

SECTION III – TERMINOLOGY

1-7. The following terminology is inherent to IED defeat and is used throughout this manual:

- **Booby trap.** A *booby trap* is an explosive or nonexplosive device or other material deliberately placed to cause casualties when an apparently harmless object is disturbed or a normally safe act is performed (Joint Publication [JP] 1-02).
- **Captured enemy ammunition.** A *CEA* is all ammunition products and components produced for or used by a foreign force that is hostile to the United States (that is or was engaged in combat against the United States) in the custody of a U.S. military force or under the control of a Department of Defense (DOD) component. The term includes confined gaseous, liquid, and solid propellants; explosives; pyrotechnics; chemical and riot-control agents; smokes and incendiaries (including bulk explosives); chemical warfare agents; chemical munitions; rockets; guided and ballistic missiles; bombs; warheads; mortar rounds; artillery ammunition; small arms ammunition; grenades; mines; torpedoes; depth charges; cluster munitions and dispensers; demolition charges, and devices and components of the above. CEA can also include North Atlantic Treaty Organization (NATO) or U.S. manufactured munitions that may not have been under U.S. custody or control.
- **Defeat.** *Defeat* is a tactical mission task that occurs when an enemy force has temporarily or permanently lost the physical means or the will to fight. The defeated force's commander is unwilling or unable to pursue his adopted course of action (COA), thereby yielding to the friendly commander's will, and can no longer interfere to a significant degree with the actions of friendly forces. Defeat can result from the use of force or the threat of its use (FM 1-02).

- **Explosive hazard. An *explosive hazard* is any hazard containing an explosive component. All explosive hazards currently encountered on the battlefield can be broken down into five categories: unexploded ordnance (UXO), booby traps, IEDs, CEA, and bulk explosives.**
- **Explosive ordnance.** *Explosive ordnance* is all munitions containing explosives, nuclear fission or fusion materials, and biological and chemical agents. This includes bombs and warheads; guided and ballistic missiles; artillery, mortar, rocket, and small arms ammunition; all mines, torpedoes, and depth charges; demolition charges; pyrotechnics; clusters and dispensers; cartridge and propellant-actuated devices; electro-explosive devices; clandestine and IEDs; and all similar or related items or components explosive in nature (JP 1-02).
- **Improvised explosive device.** An *IED* is 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. Also called IED (JP 1-02).
- **Improvised explosive device hunting. *Improvised explosive device hunting* is a counter-IED operation to proactively locate IEDs and the personnel who make and emplace them before the IED is detonated. See also military search.**
- **Military search. *Military search* is the management and application of systematic procedures and appropriate detection equipment to locate specified targets.**
- **Neutralize.** The definition of *neutralize* is used—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).
- **Render-safe procedures.** *Render-safe procedures* are to render safe those particular courses or modes of action taken by EOD personnel for access to, diagnosis, rendering safe, recovery, and final disposal of explosive ordnance or any hazardous material associated with an EOD incident. The RSPs include the portion of the EOD procedures involving the application of special EOD methods and tools to provide for the interruption of functions or separation of essential components of unexploded explosive ordnance to prevent an unacceptable detonation (JP 1-02).
- **Unexploded explosive ordnance; unexploded explosive.** *Unexploded explosive ordnance/unexploded explosive* is explosive ordnance which has been primed, fused, armed, or otherwise prepared for action, and which has been fired, dropped, launched, projected, or placed in such a manner as to constitute a hazard to operations, installations, personnel, or material and remains unexploded either by malfunction or design or for any other cause. Also called UXO (JP 1-02).

This page is intentionally left blank.

Chapter 2

Contemporary Operational Environment

The persistent effectiveness of the IED threat has impacted unit operations, U.S. policy, and public perception. Therefore, this deadly enemy capability is likely to be a component of war and armed conflict for the foreseeable future. This chapter provides an overview of the COE and the baseline rationale for why and how state and nonstate actors employ IEDs against a superior military force. In the complicated environment of today, it is impossible to predict the exact nature of the operational environment (OE) in which IEDs might be used. Therefore, the U.S. Army must be ready to meet challenges that IEDs present within a multitude of diverse OEs. The FM 7-100 series manuals introduce the baseline for the COE and should be referred to in conjunction with this manual when training against a nonspecific capabilities-based enemy operating in an environment that is adaptive and asymmetrical.

CONCEPT

2-1. *OE* is defined as a composite of the conditions, circumstances, and influences that affect the employment of military force and bear on the decisions of the unit commander (JP 1-02). The OE is complex, dynamic, multidimensional, and comprises a collection of interrelated variables.

2-2. The COE is the synergistic combination of all the critical variables that represent the conditions, circumstances, and influences that can affect military operations today and for the foreseeable future. The COE concept can be used to describe the overall global OE or the manifestations of this OE in one or more specific OEs that exist within it. Finally, the COE concept provides a conceptual framework for assessing and understanding the nature of any specific OE. Therefore, the conceptual framework for understanding a specific OE and why the enemy uses IEDs must include an analysis of the critical variables of the COE.

CRITICAL VARIABLES

2-3. There are a number of variables, including but not limited to military capabilities, that affect the use of IEDs. These are the same critical variables by which the nature of any OE can be defined. As these conditions, circumstances, and influences vary according to the particular situation, so does the exact nature of a specific OE. These variables are interrelated and sometimes overlap. Different variables will be more or less important in different situations, but they are all common to any OE. The most difficult aspect of analyzing the OE is that the content of the variables does not remain fixed, but will evolve overtime. Therefore, we can expect the environments in which we are operating to change overtime. Nevertheless, the collective content of these variables will define any OE in which the Army might encounter IEDs at a given time and place.

2-4. While these variables can be useful in describing the overall (strategic) environment within which IEDs are used, they are most useful in defining the nature of specific OEs. Each OE is different because the content of the variables is different. Only by studying and understanding these variables will the U.S. Army be able to keep adversaries from using them against our forces or to find ways to use them to our own advantage. Beyond the assessment of individual variables, it is crucial to appreciate the relationships that exist among the variables and how this impacts the OE.

2-5. Before examining the types of OE in which IEDs might be employed, from the perspective of each of the eleven COE variables, there are some basic premises that characterize the general nature of the COE. In the foreseeable future, the United States is not likely to have a peer competitor that would be able to engage U.S. forces head-to-head in conventional combat on a large scale. Nations that believe the United States may intervene in their country or region will develop adaptive approaches for dealing with technologically superior forces. Nonstate actors are now playing and will continue to play an important role in any regional conflict—as combatants or noncombatants. Any specific OE in which we might encounter IEDs is a manifestation of the overall nature of the COE. The following are the eleven COE variables:

- Physical environment.
- Nature and stability of the state or nonstate actors.
- Sociological demographics.
- Regional and global relationships.
- Military and paramilitary capabilities.
- Technology.
- Information.
- External organizations.
- National will or nonstate actors will.
- Time.
- Economics.

PHYSICAL ENVIRONMENT

2-6. The enemy clearly understands that less complex and open environments favor U.S. forces with our long-range, precision-guided weapons and our sophisticated ISR capability. Because of this, the enemy usually avoids open terrain and operates in urban areas and other complex terrain to mitigate U.S. technical superiority. Such terrain is also optimal for emplacing IEDs with minimal risk to those who emplace them. However, the physical environment includes more than just terrain and weather patterns. Natural resources, population centers, and critical infrastructures are also important, especially since they may become targets for IEDs.

> ***Note.*** Complex terrain is a topographical area consisting of an urban center larger than a village and/or of two or more types of restrictive terrain or environmental conditions occupying the same space. (Restrictive terrain or environmental conditions include, but are not limited to slope, high altitude, forestation, severe weather, and urbanization.) Complex terrain, due to its unique combination of restrictive terrain and environmental conditions, imposes significant limitations on observation, maneuver, fires, and intelligence collection.

NATURE AND STABILITY OF THE STATE OR NONSTATE ACTORS

2-7. In the state or states within which the IEDs are employed, the nature and stability of a country often is related to where the real strength of the state lies. It may be the political leadership, the military, the police, or some other element within the population. In understanding where the power resides, you can analyze who would use IEDs, against whom, and why—as a means to achieve a specific end. Those who employ IEDs may be nonstate actors (such as criminals, insurgents, or terrorists) that are either subnational or transnational in nature; in that case, you need to understand the nature and stability of the nonstate organization. A weak state may be unable to control the activities of nonstate actors who would use IEDs within its territory.

2-8. The enemy can be any individual, group of individuals (organized or not organized), paramilitary or military force, national entity, or national alliance that is in opposition to the United States, its allies, or its multinational partners. In the case of IEDs, the enemy can be any individual, group, or organization that employs IEDs, regardless of their motivation. These adversaries include the people who build the IEDs, those who plan their use, those who emplace them, those who conduct surveillance before and after emplacement, and those who harbor or provide sanctuary to the perpetrators or provide them financial or material support.

SOCIOLOGICAL DEMOGRAPHICS

2-9. The demographics variable includes the cultural, religious, and ethnic makeup of a given region, nation, or nonstate actor. Extreme devotion to a particular cause and/or hatred against another nation or another cultural, religious, or ethnic group provides the enemy with the willingness to carry out IED attacks. This variable can be analyzed to determine how far the enemy would go to carry out his attacks (for example, suicide bombers), who it is likely to attack, and where it is likely to attack (where those hated groups or individuals reside, work, or travel or locations of symbolic value).

2-10. Cultural, religious, or ethnic links can cause the local population to support the enemy, to include providing the enemy with information about possible targets for IEDs. However, by understanding the sociological demographics of the local population, U.S. or coalition forces can address the needs of the people and avoid offending their sensitivities. Winning over the population can be a crucial element in successfully fighting the IED threat. If treated properly, the populace can be cooperative about providing U.S. or coalition forces with information about enemy activity, the location of weapons caches and bomb-making factories, and the locations of emplaced IEDs.

2-11. The aforementioned physical environment is intertwined with our analysis of sociological demographics. For example, an urban environment is affected by the cultures found within it. Since the enemy prefers to operate in complex terrain and the majority of the world population resides in urban settings, the potential for U.S. forces to continue to operate in this type of environment is a reality. The enemy will use IEDs not only to target U.S. forces, but also to target specific groups or individuals within the population (often in an urban setting).

REGIONAL AND GLOBAL RELATIONSHIPS

2-12. The relationship of a state or nonstate actor to other actors and the level of allegiance to that relationship can determine the effectiveness of IEDs in a specific OE. These relationships can determine the level of support and motivation and increase the capability of the enemy to use IEDs. When analyzing the OE, closely consider the relationships that exist between state and nonstate actors and what this means in terms of funding, training, equipping, and manning of forces employing IEDs.

2-13. Regional and global relationships could be between similar kinds of nonstate actors (for example, terrorists) who could share TTP for building and employing IEDs. Nation-states could share these TTP with nonstate actors and vice versa.

MILITARY AND PARAMILITARY CAPABILITIES

2-14. Military capabilities are most often thought of in terms of a standing professional force. However, the enemy does not require a standing army to use IEDs in order to achieve a specific means. When considering the impact of military capabilities on the use of IEDs, more important is the level of equipment, training, resources, and leadership available for procurement, development, and execution of IEDs.

2-15. Paramilitary organizations are those that are distinct from the regular armed forces but resemble them in organization, equipment, training, or purpose. Basically, any organization that accomplishes its purpose, even partially, through the force of arms can be considered a paramilitary organization. Some types of paramilitary organizations (such as police and other internal security forces) may be part of the government infrastructure. Other types (such as insurgents, terrorists, and large-scale drug and other criminal organizations) operate outside the government or any institutionalized controlling authority. When it is expedient for their purposes, these paramilitary forces can employ IEDs.

TECHNOLOGY

2-16. Easy access to new technology allows the enemy to achieve equality or even overmatch U.S. forces in selected niche areas. IEDs range from relatively crude devices to fairly sophisticated and precision weapons. In their own way, IEDs can be precision weapons. Analysis of the technology variable is critical for maintaining SU and for determining what types of IEDs, methods of emplacement, and triggers the enemy will use.

2-17. Advanced technology is available on the world market for a wide variety of nation-state and nonstate actors who can afford it. However, any of these actors (if their intent is hostile to U.S. interests) will attempt to find ways to use whatever technology is available to them in adaptive and innovative ways against us. For example, the enemy can use readily available communications technology (such as cellular or satellite telephones or handheld radios) to communicate with operatives or to remotely detonate IEDs.

INFORMATION

2-18. The enemy understands the value of information and information warfare (IW). The enemy has seen the important role that IW has played in achieving the overall objectives of various actors in current and past conflicts. Media and other information means facilitate the visibility of IED operations to the world (providing publicity), while the use of IEDs can provide standoff and anonymity to the user. The enemy can use the perception management aspect of IW to try to provide justification for its actions and as a means for recruitment. Knowing that casualties from IEDs will be publicized in the media in the United States and other coalition countries, the enemy can use this reporting to affect the U.S. national will and the coalition will. The enemy will exploit U.S. mistakes and leverage the media and other information systems to impact U.S. political decision making. IW is a nonlethal tool that is used in conjunction with lethal operations to achieve an end.

2-19. The enemy will emphasize the fact that U.S. and coalition forces and/or local authorities are unable to protect themselves or the local population from the effects of IEDs. This is a physical and psychological threat to elements of the local population; it can keep them from supporting U.S. objectives and coerce them into providing aid to enemy forces or at least passively protecting them.

EXTERNAL ORGANIZATIONS

2-20. External organizations (such as international governmental organizations, nongovernmental organizations [NGOs], media, transnational corporations, and private security organizations) impact the enemy's decisions on whom to target, how to target, and how to manipulate the situation for its benefit. External organizations within the OE provide the enemy with a multitude of targets, opportunities for concealment among noncombatants, and potential information gatherers—all of which the enemy can use to its advantage when employing IEDs. Analyzing this variable can help determine where the enemy will use IEDs, who it will target, and how.

NATIONAL WILL OR NONSTATE ACTORS WILL

2-21. The unification of common values within a segment of the population and a unified effort to pursue, protect, and/or spread those values can further the ability of the enemy to achieve its ends. It can also define the level of support the enemy can expect to sustain from the local population and/or other populations sharing those common values. The enemy will attempt to attack the U.S. national will or the coalition partners will through the use of IEDs (along with IW) because they provide a tactical weapon with which to achieve strategic goals. The enemy uses IEDs because it believes they are effective and that the use of IEDs is acceptable at least to the members of the group or cause on whose behalf it is using them.

2-22. Victory does not necessarily go to the best-trained or best-equipped entity but to the entity that is willing to sacrifice the most in order to win. The enemy entity may view the will of its organizational leadership and the devotion and collective will of its members and supporters as an advantage over the United States or a U.S.-led coalition. The will of a suicide bomber may reflect the overall will of the organization that sent him to deliver the IED.

TIME

2-23. In an era of push-button technology and past U.S. successes in relatively short-time periods, the enemy will attempt to prolong U.S. operations for as long as possible until the U.S. national will and/or the coalition will falters. A protracted campaign of IED use can be a means for the enemy to achieve this. The enemy views time as an advantage for itself and not for the United States.

2-24. Ways that IEDs support the enemy's use of time are often at critical junctures, such as when U.S. forces attempt entry into an OE. The enemy will take advantage of the relatively immature and nonsecure sea ports of debarkation (SPODs) and aerial ports of debarkation (APODs) and use IEDs as a weapon of choice.

2-25. Another way in which enemy employment of IEDs may be affected by time would be if the enemy determined that U.S. or coalition forces deployed in the region become less alert to the IED threat over time. If a unit or an area has not been targeted by IEDs for a period of time, complacency and lack of attention may make U.S. or coalition forces more vulnerable targets.

2-26. Over time, the enemy will change the types of IEDs and triggering devices it uses and its TTP for employing them. U.S. or coalition forces may be trained to look for certain things, but when the enemy observes that forces are looking for those things it will adapt by doing something different.

ECONOMICS

2-27. The economic factors differ from one specific OE to another. Differences in the ability to produce, distribute, and receive goods are important to the frequency of IED use and the types of IEDs used. As previously mentioned, IEDs range from relatively crude devices to fairly sophisticated and precision weapons. With IEDs, an enemy can use a large number of cheap, expendable things to affect the ability of the United States to use a limited number of expensive precision munitions or other high-technology systems. The economic situation within an OE should be carefully analyzed to determine what is currently available to the enemy, its ability to acquire materials, the level of sophistication, and its ability to sustain IED operations.

2-28. IEDs can be used to attack economic targets. Sometimes their purpose is not to inflict casualties, but rather to disrupt the flow of goods or resources. IED attacks against critical infrastructures can cripple an economy.

ADAPTIVE PRINCIPLES OF THE ENEMY

2-29. An enemy who is not a peer competitor will avoid engaging U.S. and/or coalition forces in a head-to-head conventional fight. The enemy will not fight U.S. or coalition forces in the same manner as it would its peers or lesser forces in its region. Instead, it will have to resort to adaptive approaches in order to accomplish its goals against a U.S. or coalition force that overmatches it in conventional military power. Asymmetry in warfare is not a new phenomenon, but given the relative capabilities of the United States as opposed to its potential opponents, it is increasingly likely that our enemies will seek adaptive, asymmetric approaches. They will seek to avoid or counter U.S. strengths without having to oppose them directly, while exploiting perceived U.S. weaknesses. In such cases, IEDs may become the weapons of choice.

2-30. Various nation-state and nonstate actors generally view the United States as having an overall advantage in technology and warfighting capability. Despite our strengths, these actors also see some weaknesses that they may be able to exploit. Actions against such a superior force will focus on perceived centers of gravity (such as national will and the willingness to endure casualties, hardship, stress, and continued deployments overtime). Based on these perceived vulnerabilities, enemy forces are likely to employ the following principles for dealing with technologically or numerically superior forces:

- Cause politically unacceptable casualties.
- Control access into the region.
- Employ operational shielding.
- Neutralize technological overmatch.

- Control the tempo.
- Change the nature of the conflict.
- Allow no sanctuary.

CAUSE POLITICALLY UNACCEPTABLE CASUALTIES

2-31. The enemy will attempt to inflict highly-visible and embarrassing losses on U.S. forces in order to weaken U.S. domestic resolve and national will to sustain the deployment or conflict. In recent history, modern wealthy nations have shown an apparent lack of commitment overtime and sensitivity to domestic and world opinion in relation to conflict and seemingly needless casualties. The enemy will try to influence public opinion in the U.S. homeland to the effect that the goal of intervention is not worth the cost.

2-32. IEDs are well-suited to the goal of causing politically unacceptable casualties. They can cause a relatively large number of casualties for a relatively small expense. The casualties do not necessarily have to be within U.S. or coalition forces. The United States or its coalition partners may be even less willing to accept military or civilian casualties.

CONTROL ACCESS INTO THE REGION

2-33. U.S. and coalition forces capable of achieving overmatch against the enemy must first enter the region using power-projection capabilities. To completely deter U.S. or coalition involvement or severely limit its scope and intensity, the enemy would first target the national will of the United States and/or its coalition partners. Given the challenges IED operations have caused for U.S. and coalition forces in the past, an enemy could mount an extensive IED campaign in its region in order to dissuade such forces from intervening there.

2-34. Access-control operations do not necessarily have to deny access entirely. A more realistic goal is to limit the U.S. or coalition accumulation of applicable combat power to a level and to locations that do not threaten the goals of the enemy organization. One means of accomplishing this is the employment of IEDs to attack U.S. or coalition forces at APODs and SPODS, along routes to the region, at transfer points en route, at aerial ports of embarkation (APOEs) and sea ports of embarkation (SPOEs), and even at their home stations. These are fragile and convenient targets. In order to selectively deny a U.S. or coalition force the use of or access to forward bases of operation within or near the region, enemy organizations might use IEDs to attack the population and economic centers for the intimidation effect.

EMPLOY OPERATIONAL SHIELDING

2-35. The enemy will use any means necessary to protect key elements of its forces or infrastructure from destruction by a more powerful U.S. or coalition force. This protection may come from use of urban and other complex terrain and exploiting U.S. or coalition concerns about the attendant risk of civilian casualties or unacceptable collateral damage when engaging the enemy. Dispersion and the use of IW can also help protect the enemy. The enemy will try to conceal and protect the locations where its personnel plan IED operations, collect the necessary materials, make bombs, or train operatives for IED emplacement.

2-36. Operational shielding generally cannot protect the entire enemy organization for an extended time period. Rather, the enemy organization will seek to protect selected elements of its forces for enough time to gain the freedom of action necessary to execute IED operations.

NEUTRALIZE TECHNOLOGICAL OVERMATCH

2-37. Although the United States currently enjoys overwhelming military superiority, this no longer serves as an adequate deterrent against many emerging threats, especially those from nonstate actors. When conflict occurs, any enemy will seek ways to neutralize our technological advantage. Against a technologically superior force, enemy organizations will disperse their forces in areas where complex terrain limits the U.S. ability to apply our full range of technological capabilities. However, the enemy can rapidly mass forces from these dispersed locations to conduct IED operations at the time and place of its own choosing. Enemy organizations train its forces to operate in adverse weather, limited visibility, rugged terrain, and urban environments. Such conditions can shield the enemy from the effects of U.S. or coalition force high-technology weapons and deny U.S. or coalition forces the full benefits of their advanced reconnaissance, intelligence, surveillance, and target acquisition (RISTA) systems.

High-Technology Targeting of United States Systems

2-38. Enemy forces might concentrate the use of IEDs on the destruction of high-visibility (flagship) U.S. systems. Losses among these premier systems may not only degrade operational capability, but also undermine U.S. or coalition morale. Thus, attacks against such targets are not always linked to military-style objectives.

Technology for Situational Understanding

2-39. The enemy will use its own RISTA means to support IED employment. The proliferation of advanced technologies permits some enemy organizations to achieve a SU of U.S. or coalition deployments and force dispositions formerly reserved for the militaries of technologically advanced nations. Much information on the sources of such technology is readily and cheaply available on the Internet and in open-source documents. These media can provide enemy forces with extensive information on U.S. or coalition members and their armed forces. Intelligence can also be obtained through greater use of human intelligence (HUMINT) assets that, among other sources, gain intelligence through sympathetic elements in the local population and from civilians or local workers contracted by U.S. or coalition forces for base operation purposes. Similarly, communication technologies are becoming more reliable and inexpensive. Therefore, they could act as a primary communication system or a redundant measure. There will be little U.S. or coalition forces can do to prevent the use of these assets, especially since it is becoming harder to discriminate between civilian and military-type usage.

Availability of Technology

2-40. Enemy forces use all the technology available to them, sometimes in adaptive or innovative ways. Low-technology solutions could be used against high-technology systems of an enemy. The construction of IEDs often involves employment of components for other than their originally intended purpose. Enemy forces take advantage of opportunities to upgrade available materials primarily through captured equipment, the black market, or outside support. See Chapter 4 for additional information.

Nonlinear Operations

2-41. IEDs are often employed in nonlinear operations. The enemy considers the difference between linear and nonlinear operations less in terms of geography and more in the terms of effects desired. Linear operations normally produce small effects from small actions and large effects from large actions (or perhaps large effects from an aggregation of small actions) in a linear relationship. Linear operations are proportional and additive, and typically produce a predictable, measurable effect. In contrast, this relationship may not always be present in nonlinear operations, which can produce large effects from small actions. In some cases, small actions produce small effects or no effects at all (for example, if an IED explodes without affecting the intended target). Thus, nonlinear operations can produce disproportionate, often unpredictable, effects.

Systems Warfare

2-42. The enemy can use IEDs in conducting systems warfare against U.S. or coalition systems. Because the focus of systems warfare is not just on the immediate target, but on the effects that can be created by striking that target, this approach could also fall under the label of “effects-based operations.” In this approach, the enemy views its adversary as a collection of complex, dynamic, and interrelated systems and advocates the use of all elements of available power to create actions leading to desired effects on those systems. The intent is to identify critical system components and attack them in a way that will degrade or destroy the use or importance of the overall system.

2-43. Several things have to happen to wage systems warfare. Acknowledging the difficulty of successfully predicting outcomes in nonlinear, complex environments and the multitude of constantly occurring complex interactions, the enemy will develop possibilities or hypotheses about the systems of its opponent comprising the U.S. and its coalition coherence, will, and decision making.

2-44. Systems warfare requires detailed information on targets and their possible effects. The enemy will attempt to find and attack critical links, nodes, seams, and vulnerabilities in U.S. systems that offer the best opportunity to "level the playing field." This entails RISTA capabilities linked directly to IED operations that are tailored to affect specific capabilities whose loss or degradation will significantly reduce overall force effectiveness of U.S. or coalition forces.

2-45. Therefore, the enemy often targets the "soft" components of U.S. or coalition combat systems. Attacking U.S. or coalition logistics, command and control (C2), and RISTA can undermine the overall effectiveness of our combat system without having to directly engage our superior combat and combat support (CS) forces. IEDs can be the weapons of choice for doing so.

Note. A combat system is the "system of systems" that results from the synergistic combination of five basic subsystems that are interrelated to achieve a military function: combat forces, CS forces, logistics forces, C2, and RISTA.

2-46. IEDs are useful for systems warfare, as a means of attacking U.S. and coalition lines of communications (LOCs), convoys, and other logistics assets. They also provide a means to attack U.S. or coalition C2, combat forces, and CS forces without having to mount force-on-force attacks. In the nonlinear, distributed battlespace of a complex OE, some of the smallest activities and interactions can cause the greatest effects. No activity is subject to successful prediction.

CONTROL THE TEMPO

2-47. The enemy forces will try to execute IED operations at the time and place of their own choosing. IED activities may not be linked to other enemy actions or objectives. Rather, their purpose is to inflict mass casualties or destroy flagship systems (both of which reduce U.S. or coalition forces) and continue the fight.

2-48. Enemy forces can vary the tempo of IED operations. A period of relatively low activity in IED employment might lull U.S. or coalition forces into a false sense of security, making them more vulnerable to the next round of IEDs.

CHANGE THE NATURE OF THE CONFLICT

2-49. Enemy forces will try to change the nature of the conflict in order to exploit the differences between friendly and enemy capabilities and sensitivities and to present U.S. or coalition forces with conditions for which it is not prepared. Enemy organizations will adjust their IED TTP to the strengths and weaknesses of U.S. or coalition forces. The enemy is prepared to disperse his forces in areas of sanctuary and employ them in ways that present a battlefield that is difficult for U.S. or coalition forces to analyze and predict. Enemy forces may use a sympathetic population to provide refuge or a base of operations. They move out of sanctuaries and employ IEDs when they can create a window of opportunity or when physical or natural conditions present an opportunity. Also, they may use IEDs against U.S., coalition, or host nation (HN) civilians or Soldiers and Marines not directly connected to the intervention, as a device to change the fundamental nature of the conflict.

ALLOW NO SANCTUARY

2-50. Enemy forces seek to use IEDs to deny U.S. or coalition forces safe haven during every phase of a deployment and as long as they are in the region or threatening to intervene there. The resultant drain on U.S. or coalition manpower and resources to provide adequate force protection (FP) measures can reduce strategic, operational, and tactical means to conduct war. Such actions will not only deny U.S. or coalition forces sanctuary, but also erodes their national will.

2-51. IEDs can be used to cause politically unacceptable casualties anywhere and at any time. However, they can be used at a particular time and/or place in order to deny U.S. or coalition forces access to an area, deny them safe haven, disrupt logistics, or impede movement. They can also be used to assassinate key military, government, or civilian figures or to target a particular group or organization. Physical casualties caused by IEDs also create a psychological effect that can intimidate or coerce others.

2-52. IED operations are basically nonlinear. The enemy, whether a nation-state or nonstate actor, will try to present U.S. or coalition forces with a nonlinear, simultaneous battlespace in which there is no safe "rear area." The enemy can use IEDs to attack our headquarters (HQ), logistics centers, and supply and evacuation routes. It can also use IEDs to attack our living quarters, dining facilities, and places frequented by our off-duty Soldiers, Marines, and civilians.

VARIED ACTIONS

2-53. Most of the above principles to some degree involve decentralized, dispersed, and distributed activities. To best attack superior forces, enemy leaders use initiative to conduct IED operations at a time and place of their choosing. This may mean acting at a time and place and under circumstances to offset U.S. advantages and maximize sanctuary from effects of U.S. or coalition systems. The enemy also varies the types of IEDs it employs and the methods of employment. This can make pattern analysis and templating challenging for U.S. or coalition forces.

This page is intentionally left blank.

Chapter 3

Improvised Explosive Device Threat

Although virtually any person or type of conventional or paramilitary group may employ an IED, it is a proven and effective weapon for insurgents, terrorists, and other nonstate actors. Such groups may or may not be linked to a political state and are not limited by geographic boundaries. Their motivations are often ideological and do not share the same characteristics or centers of gravity as those found in a typical state versus state conflict. They are typically organized in a nonhierarchical, nonlinear network of cells. The structure resembles that of a communication network, such as the Internet, and its nonlinearity makes it extremely survivable. There are often many communication paths and decentralized C2. Some of these networks are independent and range from the theater down to the village level. Others are linked together to provide coordinated attacks against U.S. and coalition forces and are a part of large international terrorist organizations. The rapid technological advances in communication devices (such as wireless) and the Internet provide low-cost and easily obtainable modes of communication.

3-1. Regardless of the type of group that systematically employs IEDs, key functions must be performed. These functions can be described as a nonlinear system, and critical personnel, actions, and resources determine the enemy IED system. The enemy IED activity model in Figure 3-1, page 3-3, describes the key nodes in a system designed to conduct IED attacks. Many of these nodes are part of the operation of a larger nonstate group. Successful IED defeat requires the commander to influence a subset of these functions to defeat the IED threat. The interconnections depicted in Figure 3-1 represent the impact one node may have on another. For example, local support will make it easier for the enemy to recruit and find supplies. These interconnections will be used to determine the level of effect that attacking a node has on the overall capability of the enemy. Descriptions of enemy nodes include—

- **International leadership.** International leadership is a person or group that provides the overall direction and purpose for the group if it is transnational in nature. This leadership may coordinate the relationship between the nodes and conduct strategic planning.
- **Regional and local leadership.** These nodes describe the leadership required to carry out the operations delegated by the overall group leadership. A network can also be made up of many splinter organizations carrying out specific orders from a larger, more centralized coordination group.
- **Recruitment.** Recruitment is the activities related to the act of building a force of operatives, trainers, financers, and technicians to carry out the campaign of the group.
- **Training.** Training is the act of providing a means to educate recruited personnel in a skill needed to perform a role in the overall effort. Some personnel may be trained as engineers, while others may be trained to emplace IEDs.
- **Target selection and planning.** Planners must first select a target before mission planning can begin. Through observation, the enemy collects valuable information on troop movement, times of vulnerability, target vulnerability, and areas of approach and escape. IED operations will become more complex as friendly security and IED defeat capabilities grow.
- **Surveillance.** Surveillance is to observe potential targets in order to collect information used in the planning of IED operations. These observations aid the enemy planner with critical information, such as ideal IED emplacement locations, high-traffic areas, concealment data, observation points, and avenues of escape and reinforcement.

- **Attack rehearsal.** A rehearsal both prepares the IED team for its actions and tests and evaluates the plan of attack.
- **Regional and local support.** Active local support consists of citizens and other locals assisting with enemy IED efforts (such as looking out for troops while IEDs are being placed or donating supplies). Passive local support for insurgent IED efforts consists of the refusal of citizens and other locals to give U.S. or coalition forces information or assistance. Passive local support of IED efforts result in part from fear of reprisal, but may also be attributed to sympathy with enemy objectives.
- **Movement.** Movement is the physical movement of devices, supplies, and personnel into and out of an AO during predetonation and postdetonation phases.
- **Funding.** Funding is the means and methods used to subsidize the cost of IED operations.
- **Supplies.** Supplies are the materials and the availability of materials used to accomplish IED operations.
- **Improvised explosive device makers.** IED makers are the persons involved in the design and fabrication of an IED.
- **Orders group.** The orders group (which may have no formal name) is a small cell made up of one or more members of the regional and/or local leadership and possibly the IED makers. It is designed to coordinate the IED effort while compartmenting information in case of infiltration or discovery.
- **Improvised explosive device team.** The IED team is the personnel who emplace, monitor, and detonate the IED.
- **International support.** International support is support in the form of funding, training, organization, recruiting, publicity, and planning assistance that is provided to the group from nonlocal sources, to include foreign nations and states, NGOs, terrorist organizations, media outlets, and other organizations or individuals.
- **Emplacement.** Emplacement is the positioning of an IED for the purpose of conducting an attack.
- **Improvised explosive device monitoring and detonating.** To monitor and detonate IEDs is the act of observing the area of emplacement in order to command detonate an IED.
- **Battle damage assessment.** Battle damage assessment (BDA) is the act of observing the detonation or aftermath of an explosion to evaluate the destruction of the IED. Often this is a decision point for the enemy to initiate a follow-on attack or egress out of the kill zone.
- **Infrastructure.** IED makers require an infrastructure of safe houses, work areas, and storage facilities.
- **Information campaign.** The enemy can be very effective using IW as a method of promoting group success, which fuels recruiting efforts and encourages support by portraying a positive image of the operations of the group.

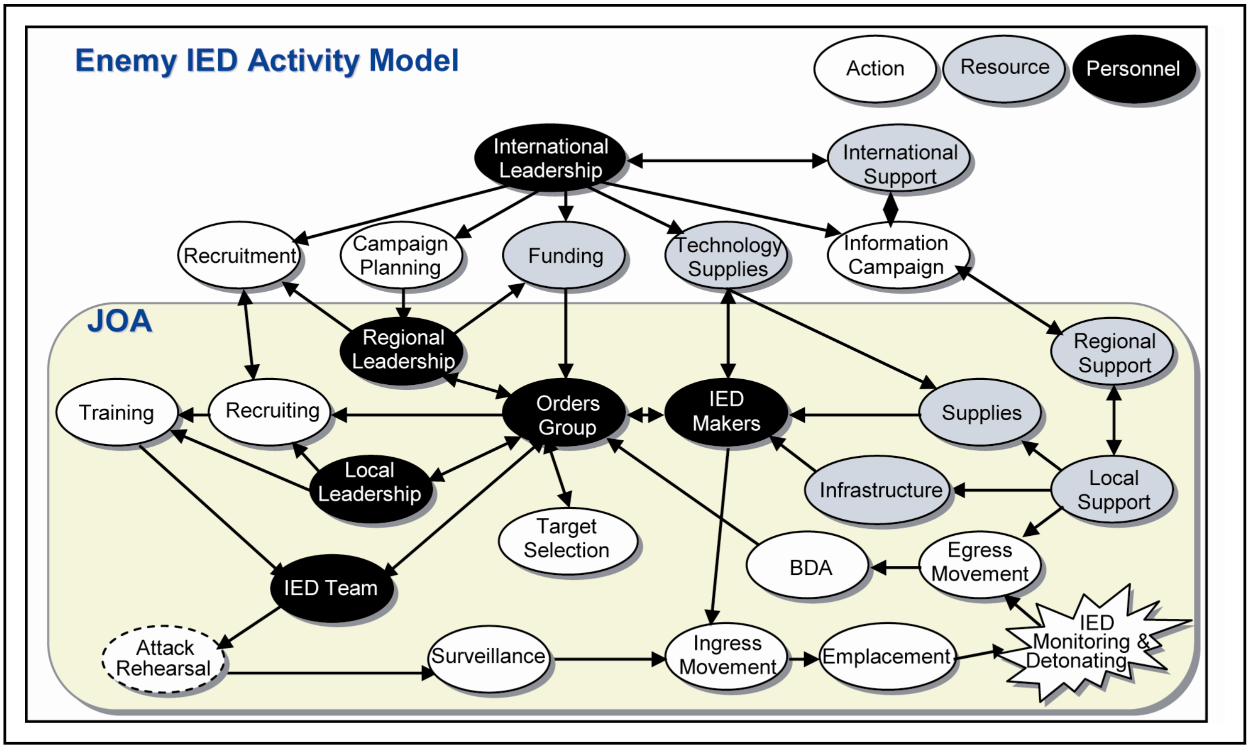

Figure 3-1. Enemy IED system

3-2. Figure 3-1 shows that there are multiple vulnerabilities that the joint task force (JTF) commander can exploit to bring about IED defeat. It is not necessary to attempt to prevent the detonation of every IED. By attacking or isolating one or more key actions (resources or groups of personnel), the JTF commander can prevent the effects of IEDs in a proactive manner.

3-3. The challenge is to identify which nodes the JTF commander can affect and which of those has the largest payoff for IED defeat. Enemy activity nodes fall into different levels of influence from the national to the tactical level. Successful attacks against the enemy will require a joint interagency effort including the DOD, the intelligence community, law enforcement, and interaction with international partners.

This page is intentionally left blank.

Chapter 4

Improvised Explosive Device Characteristics

WARNING

Specific identification features for IEDs are ever-changing based on the capabilities and available resources of the enemy.

DANGER

Do not attempt to move, approach, or take any action on a possible IED. If possible, avoid using any communication or electronic equipment within the established exclusion area. Any of the above dangers may cause an IED to detonate.

IEDs are a dangerous and effective weapon system that military forces face. IEDs can be almost anything with any type of material and initiator. They are an improvised device that are designed to cause death or injury by using explosives alone or in combination with other materials, to include projectiles, toxic chemicals, biological toxins, or radiological material. IEDs can be produced in varying sizes and can have different types of containers and functioning and delivery methods. IEDs can use commercial or military explosives, homemade explosives, or military ordnance and ordnance components. IEDs are primarily conventional high-explosive charges, also known as homemade bombs. A chemical and biological (CB) agent, or even radiological material, may be included to add to the destructive power and the psychological effect of the device. They are unique in nature because the IED builder has had to improvise with the materials at hand. Designed to defeat a specific target or type of target, they generally become more difficult to detect and protect against as they become more sophisticated. IEDs are becoming increasingly sophisticated and can be fabricated from common materials. IEDs may range in size from a cigarette pack to a large vehicle. The degree of sophistication depends on the ingenuity of the designer and the tools and materials available. IEDs of today are extremely diverse and may contain any type of firing device or initiator, plus various commercial, military, or contrived chemical or explosive fillers. Cached, stockpiled munitions, or CEA within the current theater of operations may provide the explosive materials to “would be” enemy bombers.

COMPONENTS

4-1. IEDs can vary widely in shape and form (Figure 4-1, page 4-2) IEDs share a common set of components and consist of the main charge, initiating system, and casing.

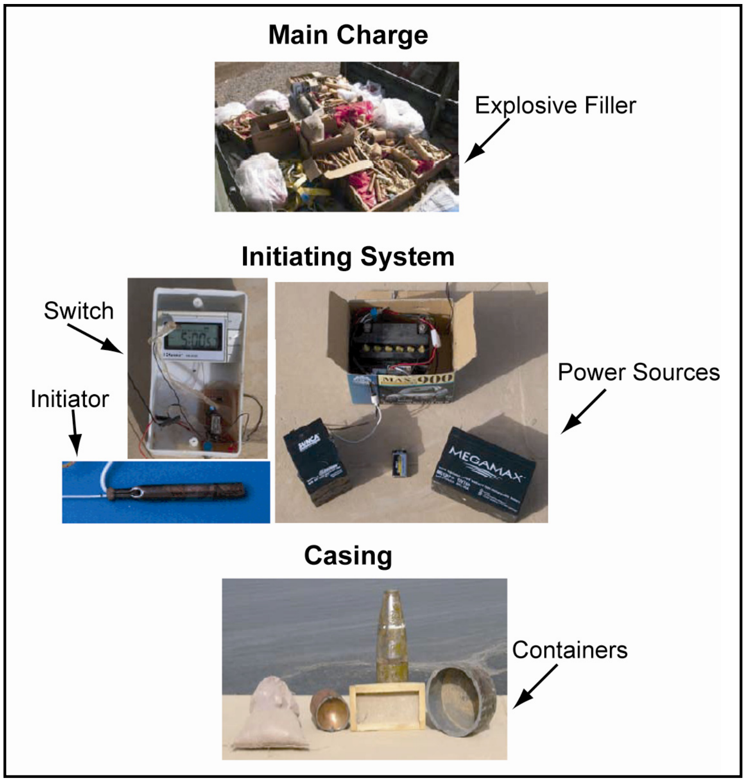

Figure 4-1. Components of an IED

MAIN CHARGE

4-2. The most common explosives used are military munitions, usually 122-millimeter or greater mortar, tank, and/or artillery rounds. These items are the easiest to use and provide a ready-made fragmentation effect and they allow for relatively easy "daisy chaining," which is linking multiple main charges together over long or short distances for simultaneous detonation. Other IEDs have used military and commercial explosives, such as PE4, trinitrotoluene (TNT), ammonium nitrate (fertilizer), and fuel oil (ANFO). Common hardware, such as ball bearings, bolts, nuts, or nails, can be used to enhance the fragmentation. Propane tanks, fuel cans, and battery acid can and have been added to IEDs to propagate the blast and thermal effects of the IED.

INITIATING SYSTEM

4-3. The initiation system or fuze functions the device. It could be a simple hard wire for command detonation to a cellular telephone or remote controls to toy cars and airplanes for radio-controlled IEDs. The initiator almost always consists of a blasting cap.

4-4. Batteries are used as a power source for detonators. Batteries of all types are the primary source of power for IEDs. Batteries could be as small as 9-volts, AA, and those used in long-range cordless telephones (LRCTs) to car and truck batteries. IEDs may even be wired into the local power supply of a home or office.

CASING

4-5. Casings can range in size from a cigarette pack to a large truck or airplane. The container is used to help hide the IED and to possibly provide fragmentation. A myriad of containers have been used as casings, including soda cans, animal carcasses, plastic bags, and vests or satchels for suicide bombers.

INITIATION METHODS

4-6. Initiation methods (Figure 4-2) include—

- **Time.** Time IEDs are designed to function after a preset delay, allowing the enemy to make his escape or to target military forces which have created a pattern. Timers used include igniferous, chemical, mechanical, and electronic.
- **Command.** Command-initiated IEDs are a common method of employment and allow the enemy to choose the optimum moment of initiation. They are normally used against targets that are in transit or where a routine pattern has been established. The most common types of command-initiated methods are with command wires or radio-controlled devices, such as LRCTs, cordless telephones, and remote car openers and alarms.
- **Victim.** A victim-actuated IED is a means of attacking an individual or group of individuals. There are various types of initiation devices, which include pull or trip, pressure, pressure release, movement-sensitive, light-sensitive, proximity, and electronic switches.

WARNING

Specific identification features for IEDs are ever-changing based on the capabilities and available resources of the enemy.

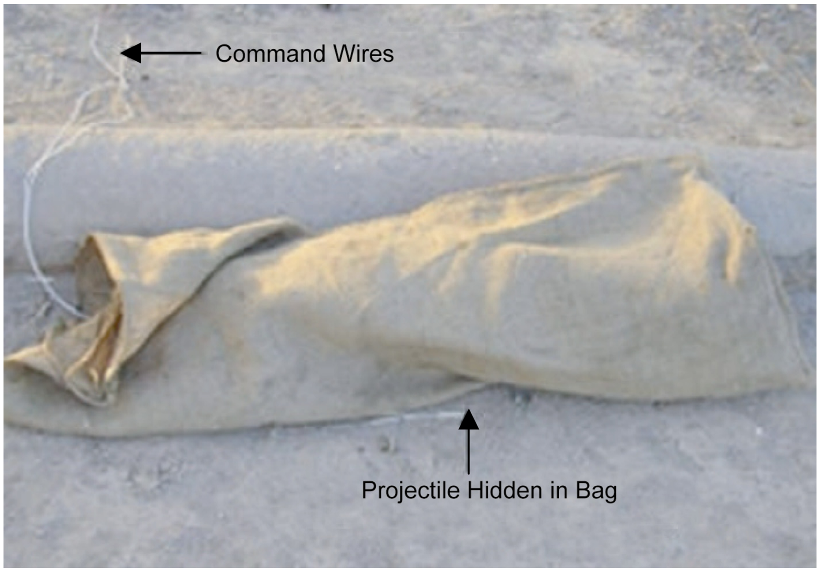

Figure 4-2. Command-initiated concealed IED

USES AND TARGETS

4-7. IEDs can be used in the following manners:

- Disguised static IEDs can be concealed with just about anything (trash, boxes, tires, and so forth) and can be placed in, on, or under a target or in or under unsecured vehicles.
- Disguised moveable IEDs (vehicle-borne improvised explosive devices [VBIEDs], suicide bomber vests, victim-actuated IEDs, or remote-controlled cars).
- Thrown or projected IEDs (improvised grenades or mortars), used mostly from overhead passes.
- IEDs placed in, on, or under a target or in or under unsecured vehicles.

- Hoax IEDs which the enemy uses for a myriad of purposes, such as to learn our TTP, entrapment, nonexplosive obstacle, and development of complacency for future IED attacks. Hoax IEDs include something resembling an actual IED, but have no charge or a fully functioning initiator device.

4-8. IEDs can be designed to attack specific targets, such as high-visibility targets, high-value targets (dignitaries), and military targets, such as—

- Quick-reaction forces (QRFs) and first responders.
- Cordons.
- Checkpoints and control points.
- Logistics movements or combat patrols.
- Anywhere that a targetable pattern has developed.

Note. Secondary and tertiary IEDs should be expected in the area.

INDICATORS

4-9. The primary indication of an IED will be a change in the environment (something new on the route that was not there yesterday). The enemy may leave behind visual indicators of an emplaced IED by accident or on purpose (to inform the local population). Vigilant observation for these subtle indicators can increase the likelihood of IED detection by friendly forces before detonation. Examples of possible roadside IED indicators include, but are not limited to—

- Unusual behavior patterns or changes in community patterns, such as noticeably fewer people or vehicles in a normally busy area, open windows, or the absence of women or children.
- Vehicles following a convoy for a long distance and then pulling to the roadside.
- Personnel on overpasses.
- Signals from vehicles or bystanders (flashing headlights).
- People videotaping ordinary activities or military actions. Enemies using IEDs often tape their activities for use as recruitment or training tools.
- Suspicious objects.
- Metallic objects, such as soda cans and cylinders.
- Colors that seem out of place, such as freshly disturbed dirt, concrete that does not match the surrounding areas, colored detonating cord, or other exposed parts of an IED.
- Markers by the side of the road, such as tires, rock piles, ribbon, or tape that may identify an IED location to the local population or serve as an aiming reference (such as light poles, fronts or ends of guardrails, and road intersections or turns).
- New or out of place objects in an environment, such as dirt piles, construction, dead animals, or trash.
- Graffiti symbols or writing on buildings.
- Signs that are newly erected or seem out of place.

4-10. Friendly forces should be especially vigilant around—

- Obstacles in the roadway to channel convoys.
- Exposed antennas, detonating cord, wires, or ordnance.
- Wires laid out in plain site; these may be part of an IED or designed to draw friendly force attention before detonation of the real IED.

LOCATIONS

4-11. IEDs may be emplaced anywhere that enough space exists or can be created to hide or disguise the IED. Whenever possible, devices are located where employment can exploit known U.S. patterns (such as the use of a main supply route [MSR]) or vulnerabilities (such as soft-skinned vehicles or chokepoints). Common areas of IED emplacement (Figure 4-3) include, but are not limited to—

- Previous IED sites (past successes).
- Frequently traveled, predictable routes, such as roads leading to FOBs and along common patrol routes.
- Boundary turn around points (pattern).
- Roadway shoulders (usually within 10 feet).
- Medians, by the roadside, or buried under the surface of any type of road, often in potholes and covered with dirt or reheated asphalt.
- Trees, light posts, signs, overpasses, and bridge spans that are elevated.
- Unattended vehicles, trucks, cars, carts, or motorcycles (attached or installed in them).
- Guardrails (hidden inside) or under any type of material or packaging.
- Potential incident control points (ICPs).
- Abandoned structures (sometimes partially demolished).
- Cinder blocks (hidden behind) or piles of sand to direct blast into the kill zone.
- Animal carcasses and deceased human bodies.
- Fake bodies or scarecrows in coalition uniforms.
- Buildings.

Note. See Appendix B, paragraph B-5, for particularly suitable IED locations.

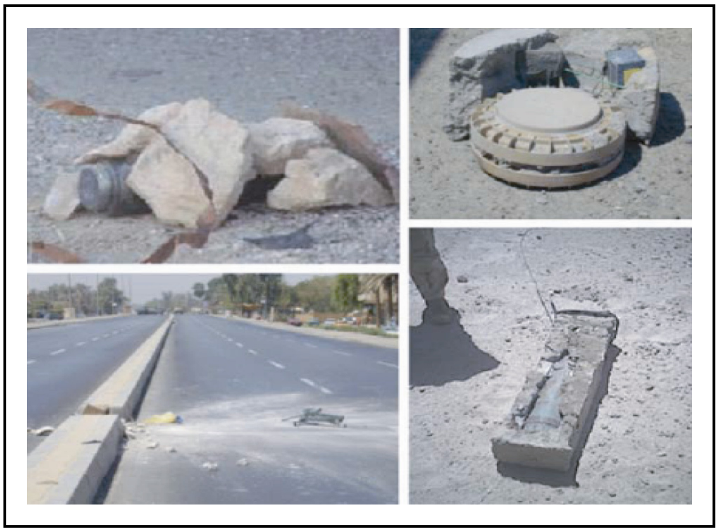

Figure 4-3. Common areas of IED emplacement

This page is intentionally left blank.

Chapter 5

Organizations Involved in Improvised Explosive Device Defeat

See Appendix C for contact information on these organizations. This is not an all inclusive list of organizations involved in IED defeat. All organizations listed in Appendix C have Internet links to other organizations.

ASYMMETRIC WARFARE GROUP

5-1. The Asymmetric Warfare Group (AWG) conducts operations in support of joint and Army force commanders to mitigate and defeat specified asymmetric threats. The AWG—

- Provides, deploys, integrates, coordinates, and executes C2 of trained and ready forces.
- Seeks, collects, develops, validates, and disseminates emerging TTP.
- Assists in exploitation and analysis of asymmetric threats.
- Provides advisory training for in-theater or predeployment forces.
- Provides identification, development, and integration of countermeasure technologies.

CAPTURED MATERIEL EXPLOITATION CENTER

5-2. The Captured Materiel Exploitation Center (CMEC) is formed from the assets of organic and attached technical intelligence (TECHINT) elements augmented by other subject matter experts (SMEs). It manages the command battlefield TECHINT system through the military intelligence (MI) brigade and the Assistant Chief of Staff, Intelligence (G-2). When possible, other armed services should combine assets for the acquisition and exploitation of captured enemy munitions, to include CEA. When this occurs, the CMEC becomes the Joint Captured Material Exploitation Center (JCMEC).

CHEMICAL, BIOLOIGICAL, RADIOLOGICAL, NUCLEAR, AND HIGH-YIELD EXPLOSIVE COMMAND

5-3. The Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Command is assigned to the United States Army Forces Command (FORSCOM) and brings C2 of the Army's most specialized weapons of mass destruction (WMD) operational assets together. This provides a single point of contact within the Army for the DOD to call when a coordinated response to the threat or use of WMD is needed anywhere in the world. CBRNE Command maintains C2 of Army EOD forces.

5-4. The mission of the CBRNE command is to C2 organic and allocated Army technical assets to support full-spectrum CBRNE technical operations that detect, identify, assess, render-safe, dismantle, transfer, and dispose of CBRNE incident devices and materiel including UXO and IEDs. The command is also responsible for managing DOD technical support to consequence management operations and providing CBRNE technical advice and subject matter expertise.

5-5. This deployable operational-level command manages existing and future programmed CBRNE response assets that can simultaneously respond to multiple CBRNE incidents in support of combatant commanders and the joint team at home and around the world. Its subordinate units include two explosive ordnance groups, five ordnance battalions, two technical escort chemical battalions, and operational control of the Army Reserve Unit—Consequence Management. Future growth of the command includes the activation of two subordinate ordnance battalions, a chemical brigade HQ, and an analytical and remediation directorate.

COMBINED EXPLOSIVES EXPLOITATION CELL

5-6. The Combined Explosives Exploitation Cell (CEXC) is a joint agency team tasked with the collection and exploitation of IEDs. CEXC provides immediate in-theater technical and operational analysis of IEDs and develops measures to counter bombing campaigns; collects and exploits TECHINT and forensic evidence from explosives related incidents (with major emphasis on IED components); and collect construction and techniques in order to determine enemy tactics, identify trends, target IED bomb makers; and enable both offensive and defensive counter-IED operations by coalition forces. Critical tasks include—

- Conducting first-line technical exploitation and evaluation of IEDs and components and preparing detailed laboratory reports for all exploited material.
- Providing advice on EOD, FP, and combat tactics in regard to the threat posed by IEDs.
- Attending all significant IED/explosives related incidents.
- Exploiting cache discoveries containing large quantities of military ordnance, bomb-making materials, and/or homemade explosive manufacturing and storage sites.
- Exploiting any incident site where the collection of forensic evidence is important.
- Providing detailed field forensics analysis for targeting.
- Preparing, publishing, and disseminating throughout theater, a comprehensive report for every incident attended and a weekly report summarizing IED incident statistics, significant events, and recovered devices for the last seven days.
- Preparing, publishing, and disseminating throughout theater, spot reports and technical bulletins for rapidly emerging threats, significant incidents, and newly seen devices.
- Providing technical assistance to support the interrogation of IED-related detainees.
- Providing technical advice on FP issues and counter-IED TTP.
- Providing assistance for operations against suspected bomb makers and transporters, IED factories, storage locations, and training sites.
- Providing briefings, component familiarization, personnel, and SME support.

COUNTER EXPLOSIVE HAZARDS CENTER

5-7. The Counter Explosive Hazards Center (CEHC) develops, synchronizes, trains, and integrates counter explosive hazard (mines, UXO, IEDs, booby traps) solutions across the DOTMLPF spectrum. CEHC supports the fundamentals of assured mobility, protect the force in the contemporary and future OEs, and maintain expertise in counter explosive hazard warfare.

ENGINEER UNITS

5-8. The specific combat engineer missions concerning explosive hazard are breaching, clearing, and proofing minefields. In extreme high-operational tempo or high-intensity combat missions, U.S. Army engineers or other non-EOD units may conduct limited reduction or clearing of non-mine explosive hazard and IED hazards, under the technical guidance of Army EOD forces. During the post-conflict phase, engineers may also assist EOD forces in battlefield UXO cleanup operations, as required. JP 3-34, JP 4-04, FM 3-34, and FM 5-116, provide more details on specific engineer units and tasks.

CLEARANCE COMPANY

5-9. A clearance company (Army only) conducts detection and limited IED neutralization (as outlined in Chapter 6) along routes and within areas of support to enable force application, focused logistics, and protection. It provides training readiness and oversight of assigned route and area clearance platoons. The company provides battle command for 3- to 5-route, area, or Sapper platoons. It is capable of clearing a total of 255 kilometers of two-way routes per day (three routes of 85 kilometers each) and can clear a total of two acres per day (two areas at one acre each).

Route Clearance Platoon

5-10. The mission of a route clearance platoon is to conduct route reconnaissance, minesweeping, enemy or unobserved minefield clearance operations, and deliberate route clearance. It clears obstacles with engineer (countermine) equipment or uses demolitions and performs engineer reconnaissance. The platoon provides digital hazard area data to other units at the objective and is fully mobile in-theater using organic assets only. It is capable of—

- Clearing and marking 85 kilometers (daylight only) of route (4 meters wide) per day (enemy capability and terrain dependent).
- Identifying and neutralizing mines, IEDs (as outlined in Chapter 6), and UXO on routes.
- Receiving and analyzing Ground Standoff Mine Detection System (GSTAMIDS) and Airborne Standoff Minefield Detection System (ASTAMIDS) data from other units.

Area Clearance Platoon

5-11. The mission of an area clearance platoon is to conduct area clearance, minesweeping, and enemy or unobserved minefield clearance operations. The platoon clears obstacles with engineer (countermine) equipment or uses demolitions and performs engineer reconnaissance. It is fully mobile in-theater using organic assets only. It is capable of—

- Clearing and proofing 0.004 square kilometers per day of mines (buried and surface), IEDs (as outlined in Chapter 6), and UXO (daylight only).
- Extracting casualties from an explosive hazard area.
- Providing digital hazard area information to other units (objective).

ENGINEER MINE DOG DETACHMENT

5-12. The Engineer Mine Dog Detachment consists of trained mine detection dog teams with specialized search dog capability. Engineer mine detection dogs are trained for the military OE to perform area and route clearance and search, minefield extraction, combat patrols, building search (disruptive and nondisruptive), vehicle search, and cave clearance. The dogs can reduce the time spent on a search. Dogs can search in open areas, fields, woods, hedgerows, and embankments. They are an excellent tool to route proof along roads, tracks, and railways. They can detect metallic and nonmetallic mines, both buried and surface laid. Dogs increase the speed and efficiency of an IED defeat operation.

EXPLOSIVE HAZARDS COORDINATION CELL

5-13. The mission of the explosive hazards coordination cell (EHCC) is to enable the land component commander to predict, track, distribute information on, and mitigate explosive hazards within the theater that affect force application, focused logistics, protection, and battlespace awareness. The EHCC establishes and maintains an explosive hazard database, conducts pattern analysis, and investigates mine and IED strikes and UXO hazard areas. The cell provides technical advice on the mitigation of explosive hazards, including the development of TTP, and provides training updates to field units. They coordinate explosive hazard teams (EHTs). The EHCC capabilities include—

- Establishing, maintaining, and sharing the explosive hazard tracking database within the joint operations area (JOA).
- Ensuring accuracy of explosive hazard information distribution via the battle command system.
- Coordinating site evaluations and/or strike incident investigations at four sites simultaneously or conducting unit training at four sites simultaneously.
- Assisting ISR planners with explosive hazard pattern analysis and intelligence collection management.

- Coordinating technical and tactical training for the brigade combat teams (BCTs) by the EHTs.
- Providing updated TTP and guidance for route and area clearance operations.

5-14. The EOD group or battalion and the EHCC coordinate and synchronize explosive hazard information and capability throughout the COP and JOA.

Explosive Hazards Team

5-15. The mission of an EHT is to provide evaluation of explosive hazard incident sites in support of BCTs and joint, interagency, and multinational (JIM) brigade-sized units and smaller. The EHT capabilities include—

- Conducting site evaluation of explosive hazard incident sites (to include CEA, multiple UXO, and post-blast analysis).
- Conducting TTP training (explosive hazards awareness training [EHAT], PSS-14, and area clearance) for BCT and JIM personnel on explosive hazard mitigation in a JOA.
- Conducting annual recertification, quarterly reinforcement, and predeployment training of explosive ordnance clearance agent (EOCA) personnel. (This is an Army capability only.)
- Providing advice on explosive hazards as requested.
- Providing information into the explosive hazard database via the battle command system.
- Conducting disposal of limited explosive hazards; however, EHTs are not equipped to conduct RSPs on explosive hazards.
- Consolidating and conducting analysis of requests for modifications to the JOA UXO supplemental list.
- Providing recommendations to the CBRNE cell for modification of the JOA UXO supplemental list.

5-16. The EOD company and EHT coordinate and synchronize explosive hazard information and capability throughout the COP and area of responsibility (AOR).

Explosive Ordnance Clearance Agent

5-17. EOCA personnel (Army only) are combat engineers trained to perform limited battlefield disposal of UXO as outlined in the EOCA identification guide and the JOA UXO supplemental list. If the UXO is out of the scope of operations for the EOCA, EOD personnel must be called. EOCA personnel can assist EOD personnel in disposing of other explosive hazards as requested. Properly trained and certified EOCA capabilities include—

- **Unexploded ordnance reconnaissance.** EOCA personnel are trained to perform detailed reconnaissance of a suspected UXO.
- **Unexploded ordnance identification.** EOCA personnel can perform limited identification of the items listed in the EOCA identification guide and the JOA UXO supplemental list. Items that the EOCA cannot positively identify must be reported to EOD personnel.
- **Unexploded ordnance area marking.** EOCA personnel mark the UXO area according to the standard UXO marking system.
- **Protective works.** EOCA personnel can provide the blast and fragmentation danger area of identified UXO. EOCAs may provide the estimated blast and fragmentation danger area for items similar to but not included in the EOCA identification guide and the JOA UXO supplemental list. EOCAs will advise the on-scene commander with the recommended personnel and equipment protective measures. When the commander determines that certain personnel or equipment cannot be removed from the hazard area, protective works must be established to protect those personnel and assets from the effects of the UXO. EOCAs will recommend and supervise the appropriate protective works to be completed.
- **Unexploded ordnance disposal.** EOCA personnel are authorized to destroy (by detonation) individual UXO identified in the EOCA identification guide and the JOA UXO supplemental list.

5-18. The following are the EOCA's limitations:

- Cannot move, combine, and/or destroy multiple UXO (such as a cache).
- Cannot do reconnaissance or do handling of IED or VBIED incidents.
- Can only perform CEA operations under the direct supervision of EOD personnel (includes EHTs).
- Are not to be used for explosive hazard response calls. However, if EOD is not readily available as determined by the maneuver commander, EOCA personnel can be used to conduct an initial reconnaissance of the UXO. If the UXO falls within their capability, then EOCA personnel may dispose of the UXO.

Note. The CBRNE cell at the Army theater land force or joint support manages modifications to the JOA UXO supplemental list. Requests to modify the supplemental list will be coordinated through the local EOD unit or EHT for approval by the CBRNE cell.

MINE AND EXPLOSIVE ORDNANCE INFORMATION AND COORDINATION CENTER

5-19. The Mine and Explosive Ordnance Information and Coordination Center (MEOICC) assists in the development of the COP and provides informational and SU on explosive hazards to all coalition forces, the National Mine Action Authority (NMAA), and NGOs to minimize casualties and equipment damage to coalition forces and the civilian populace and to support stability and reconstruction operations and humanitarian demining operations. The MEOICC conducts information management and exchanges information concerning explosive hazards with sector and division cells and the Coalition Provisional Authority (CPA); provides an interface with the CPA through the NMAA; provides explosive hazards awareness and mine detector training teams; and has oversight responsibility for geospatial and topographic products and weapons intelligence. MEOICC key tasks include**—**

- Training the forces in explosive hazards antitank (AT) mine detection.
- Maintaining the explosive hazards database (EHDB).
- Ensuring that equipment is funded and employed correctly.
- Tracking NGO operations within their AO.
- Transitioning operations to a designated military or civilian authority.

Note. The MEOICC will be replaced by the EHCC.

MOBILITY AUGMENTATION COMPANY

5-20. A mobility augmentation company (MAC) conducts assault gap crossings, mounted and dismounted breaches, and emplaces obstacles in support of maneuver BCTs and support brigades to enable force application, focused logistics, and protection.

SAPPER COMPANY

5-21. The mission of a Sapper company is to execute mobility, countermobility, and survivability tasks and to provide support of maneuver and support brigades to enable force application, focused logistics, and protection. A Sapper company reinforces engineers in maneuver BCTs.

TERRAIN TEAM

5-22. Terrain teams are deployed at the brigade, division, and corps levels to provide terrain analysis and geospatial support to the field. Counter-IED related support includes route analysis, identification of choke points, avenues of approach, line-of-sight analysis, and other tactical decision aids (TDAs). Terrain teams can also perform geospatial pattern analysis of tracking and locating IEDs. They provide the geospatial input to the IPB process.

EXPLOSIVE ORDNANCE DISPOSAL UNITS (ALL SERVICES)

5-23. EOD companies are on call 24 hours a day to provide emergency response teams in support of military missions, public safety, and law enforcement authorities at the federal, state, and municipal level. Each company can field 5 to 7 response teams depending on the manning configuration of the teams and the mission requirements. Each team is matched with a tailored equipment set and vehicle. Teams with equipment can be airlifted via rotary and fixed wing aircraft. EOD capabilities include—

- Identifying, rendering safe, and disposing of conventional/unconventional explosives and/or CBRNE munitions or devices (U.S. or foreign origin), to include IEDs. (EOD units are the only forces trained and equipped to render safe and dispose of IEDs.)
- Maintaining an EOD incident database located above division in the protect cell.
- Providing technical expertise to EHCCs and EHTs on explosive hazards.
- Acting as the SME for explosive hazards (IEDs, UXO, and CEA) to commanders (BCT, maneuver enhancement [ME] brigades, corps, divisions, and so forth).
- Conducting post blast and crater analysis.
- Conducting on-site assessment/verification for the presence of CBRNE material.
- Formulating a COA to protect forces, citizens, or operations from death, injury, or cessation of operations threatened by UXO, IED, or CBRNE.
- Performing chemical-biological testing in Occupational Safety and Health Administration (OSHA) Level A and Level B protective ensembles, military toxicological agent protective ensembles, or mission-oriented protective posture (MOPP)/joint services lightweight integrated-suit technology (JSLIST). Performing IED and UXO RSPs in ballistic protective “bomb suits” using an array of sets, kits, and outfits for disruption/defeat of devices and extensive technical manuals (CBRNE and conventional munitions/devices).
- Establishing working relationships with the Federal Bureau of Investigation (FBI) Bomb Data and Bureau of Alcohol, Tobacco, and Firearms (U.S.) (BATF) Arson and Explosives National Repository Centers; the Defense Intelligence Agency (DIA) Counterterrorism (CT) Division; the Missile and Space Intelligence Center, National Ground Intelligence Center (NGIC); National Laboratories; the Naval EOD Technical Center; and the Soldier and Biological Chemical Command (U.S. Army) (SBCCOMs) Technical Escort Unit.

UNITED STATES MARINE CORPS CHEMICAL BIOLOGICAL INCIDENT RESPONSE FORCE

5-24. The United States Marine Corps Chemical Biological Incident Response Force (CBIRF) provides a rapid response force for WMD incidents; consequence management support in military and industrial agent identification; downwind hazard prediction; advanced lifesaving support; casualty reconnaissance, extraction and triage; personnel decontamination; medical treatment; and stabilization for incident site management, including ordnance disposal, security, and patient evacuation. An EOD detachment in the CBIRF force protection element provides specialized response capabilities.

FOREIGN MATERIEL INTELLIGENCE GROUP

5-25. At echelons above corps (EAC), the Foreign Materiel Intelligence Group (FMIG) is a battalion-sized organization located at Aberdeen Proving Ground, Maryland. This group is the only active duty TECHINT unit in the Army. Responsibilities of the FMIG include—

- Conducting TECHINT operations.
- Preparing TECHINT reports in support of Army, joint, and combined operations.
- Acting as the Headquarters, Department of the Army (HQDA) executive agent for foreign materiel used for training purposes.

JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT TASK FORCE

5-26. The JIEDD TF focuses all counter-IED efforts within the DOD, while concurrently engaging other outside sources of potential solutions, to defeat current and future IED threats endangering joint and coalition forces. It is chartered to adopt a holistic approach focused on intelligence, TTP, information operations (IO), and the tenets of assured mobility (mitigation, prediction, detection, prevention, and neutralization). The goal is to identify and neutralize enemy leaders, suppliers, trainers, enablers, and executors responsible for the employment of IEDs against coalition forces. At the same time, the TF is focused on training our own forces in the most current TTP being used by the enemy and the best available U.S. TTP to eliminate the IED threat.

5-27. The JIEDD TF has developed a full spectrum analysis of IEDs that considers and applies multiple DOTMLPF strategies to effectively counter the IED threat. This counter-IED effort is a combined joint service, interagency, multinational program designed to leverage all available resources and technologies in a coordinated campaign to defeat the IED threat. To facilitate this effort a Joint Senior Advisory Group (JSAG) (comprising representatives from all the services, the joint staff, the Office of the Secretary of Defense, and the United Kingdom) has been formed to evaluate issues for decision by the joint IED defeat integrated process team.

MILITARY INTELLIGENCE UNITS

5-28. MI units assist the commander in visualizing his battlespace, organizing his forces, and controlling operations to achieve the desired tactical objectives or end-state. Intelligence supports FP by alerting the commander to emerging threats and assisting in security operations. The commander must understand how current and potential enemies organize, equip, train, employ, and control their forces. Intelligence provides an understanding of the enemy, which assists in planning, preparing, and executing military operations. One of the most significant contributions that intelligence personnel can accomplish is to accurately predict future enemy events. Although this is an extremely difficult task, predictive intelligence enables the commander and staff to anticipate key enemy events or reactions and develop corresponding plans or counteraction. Commanders must receive the intelligence, understand it (because it is tailored to the commander’s requirements), believe it, and act on it.

5-29. Intelligence tasks include—

- Supporting SU, to include—
  - Performing IPB.
  - Performing situational development.
  - Providing intelligence support to FP.
- Supporting strategic responsiveness, to include—
  - Performing indications and warning (I&W) to ensure intelligence readiness.
  - Conducting area studies of foreign countries.
  - Supporting sensitive site exploitation.
- Conducting ISR, to include—
  - Performing intelligence synchronization.
  - Performing ISR integration.
  - Conducting tactical reconnaissance.
  - Conducting surveillance.
  - Providing intelligence support to effects, to targeting, IO, and combat assessment.

NATIONAL GROUND INTELLIGENCE CENTER

5-30. The NGIC produces and disseminates all-source-integrated intelligence on foreign forces, systems, and supporting combat technologies to ensure that U.S. forces have a decisive edge on any battlefield. NGIC provides all-source analysis of the threat posed by IEDs produced and used by foreign terrorist and insurgent groups. NGIC supports U.S. forces during training, operational planning, deployment, and redeployment. NGIC maintains a counter-improvised explosives device targeting program (CITP) portal on the Secure Internet Protocol Router Network (SIPRNET) Web site that provides information concerning IED activities and incidents, and NGIC IED assessments. In the IED fight, NGIC increases the capability of the coalition force to collect TECHINT and provide dedicated intelligence fusion in order to target bomb makers and their networks. NGIC provides weapons intelligence teams (WITs), which are deployed to brigade level to assist with IED incidents.

NAVAL EXPLOSIVE ORDNANCE DISPOSAL TECHNOLOGY DIVISION

5-31. The Naval Explosive Ordnance Disposal Technology Division (NAVEODTECHDIV) exploits technology and intelligence to develop and deliver EOD information, tools, equipment, and their life cycle support to meet the needs of joint service EOD operating forces and other customers. Its core functions are—

- Developing EOD procedures to counter munitions threats.
- Developing tools and equipment to meet EOD operational needs.
- Performing in-service engineering for EOD tools and equipment.
- Performing depot-level management and repair for EOD tools and equipment.
- Maintaining an EOD explosive hazard database.

RAPID EQUIPPING FORCE

5-32. The Rapid Equipping Force (REF) is an organization that takes its operational guidance from the Assistant Chief of Staff, Operations and Plans (G-3) and reports directly to the vice Chief of Staff of the Army. It has a broad mission to rapidly increase mission capability while reducing the risk to Soldiers, Marines, and others. The REF accomplishes this mission in the following three ways:

- Equips operational commanders with off-the-shelf (government or commercial) solutions or near-term developmental items that can be researched, developed, and acquired quickly.
- Inserts future force technology solutions that our engaged and deploying forces require. It does this by developing, testing, and evaluating key technologies and systems under operational conditions.
- Assesses the capabilities and advising Army stakeholders of the findings that will enable our forces to rapidly confront an adaptive enemy.

TECHNICAL ESCORT UNITS

5-33. The technical escort units will, on order, deploy task-organized teams to the continental United States (CONUS) or outside the continental United States (OCONUS) to conduct technical escort, CBRN hazard characterization, monitoring, disablement, and elimination support operations. They provide WMD and CBRN incident emergency response, homeland defense, and contingency support operations to combatant commanders and lead federal agencies. They also provide site remediation and restoration support operations for DOD.

TECHNICAL SUPPORT WORKING GROUP

5-34. The Technical Support Working Group (TSWG) is the United States national forum that identifies, prioritizes, and coordinates interagency and international research and development (R&D) requirements for combating terrorism. The TSWG rapidly develops technologies and equipment to meet the high priority needs of combating the terrorism community (to include IEDs) and addresses joint international operational requirements through cooperative R&D with major allies.

5-35. Since 1986, the TSWG has pursued combating terrorism technologies in the broad context of national security by providing a cohesive interagency forum to define user-based technical requirements spanning the federal interagency community. By harnessing the creative spirit of the U.S. and foreign industry, academic institutions, government, and private laboratories, the TSWG ensures a robust forum for technical solutions to the most pressing counterterrorism requirements. Participants in the ten functional subgroup areas of the TSWG can come to a single table to articulate specific threats and a user-defined approach to the rapid prototyping and development of combating terrorism devices, training tools, reference materials, software, and other equipment.

5-36. The TSWG continues to focus its program development efforts to balance investments across the four pillars of combating terrorism. They include—

- **Antiterrorism.** Antiterrorism is the defense measures taken to reduce vulnerability to terrorist acts.
- **Counterterrorism.** Counterterrorism is the offensive measures taken to prevent, deter, and respond to terrorism.
- **Intelligence support.** Intelligence support is the collection and dissemination of terrorism-related information taken to oppose terrorism throughout the entire threat spectrum, to include terrorist use of CBRN materials or high-yield explosive devices.
- **Consequence management.** Consequence management is the preparation and response to the consequences of a terrorist event.

UNITED STATES AIR FORCE PROTECTION BATTLE LABORATORY

5-37. The United States Air Force Protection Battle Laboratory identifies innovative concepts for advancing joint warfighting. It uses field ingenuity, modeling, simulation, and actual employment of exploratory capabilities in OEs to test new and innovative ideas which can be readily transitioned into the FP arena.

UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND

5-38. The United States Army Intelligence and Security Command (INSCOM) conducts dominant intelligence, security, and IO for military commanders and national decision makers. Charged with providing warfighters the seamless intelligence needed to understand the battlefield and to focus and leverage combat power, INSCOM collects intelligence information in all intelligence disciplines. INSCOM also conducts a wide range of production activities, ranging from IPB to situation development, signal intelligence analysis, imagery exploitation, and science and technology intelligence production. INSCOM also has major responsibilities in the areas of counterintelligence (CI) and FP, electronic and IW, and support to force modernization and training.

5-39. INSCOM is a global command with four brigades that tailor their support to the specific needs of different theaters. Eight other groups or activities located worldwide focus primarily on a single intelligence discipline or function. They are available in a reinforcing role, enabling any combat commander to use INSCOMs full range of unique capabilities.

UNITED STATES ARMY MATERIEL COMMAND

5-40. The United States Army Materiel Command (USAMC) shares responsibility for managing the overt acquisition of foreign materiel for TECHINT purposes. The USAMC buys foreign materiel for exploitation purposes in the United States, as well as through its centers in Europe and the Far East.

UNITED STATES MARINE CORPS WARFIGHTING LABORATORY

5-41. The United States Marine Corps Warfighting Laboratory (MCWL) is the lead United States Marine Corps (USMC) agency for IED defeat. MCWL leads a USMC IED working group made up of representatives from the USMC, beltway agencies, and operating forces. The USMC IED working group works to rapidly identify, evaluate, and facilitate the fielding of materiel and nonmateriel counter-IED solutions to the operating forces. They work in close coordination with the JIEDD TF/integrated product team (IPT) to synchronize DOD IED defeat efforts.

WEAPONS INTELLIGENCE DETACHMENT

5-42. The Weapons Intelligence Detachment is deployed at brigade level. They assist with IED incidents.