

# The Intelligence Process



5

# CHAPTER FIVE

## The Intelligence Process

In defining intelligence, it was previously noted that the key factor that transforms information to intelligence is analysis. The British National Crime Squad, when referring to intelligence, observed the following:

The processing of reliable intelligence is the cornerstone of successful law enforcement. Analysis organizes and interprets the intelligence in a way that significantly enhances its value and the possibility of its success in combating organized crime. Analysis identifies and predicts trends, patterns or problem areas requiring action.<sup>69</sup>

Many larger law enforcement agencies have an intelligence unit, but in too many cases the unit is limited in its utility because of failures in structure or direction.<sup>70</sup> Perhaps the most common limitation is that the unit collects, but does not analyze information. Instead, the information is stored in a database simply awaiting access. For example, in some agencies field interview reports are managed by the intelligence function. While this descriptive report on an intelligence subject typically is forwarded to the intelligence unit, too often it is only entered into a database. When information sits passively in an information system, its use will be limited. If, however, the intelligence unit closely examines, analyzes, and compares the field interview forms with other information, the information can be used more effectively. Having a group of people whose primary job is simply responding to information requests about possible wanted subjects but not providing proactive analysis is not a contemporary intelligence unit.

69 See <http://www.nationalcrimesquad.police.uk>

70 In a survey conducted by the Police Executive Research Forum (PERF) after the September 11 attacks, 60% stated that they needed better intelligence. For further information on this survey, *Local Law Enforcement Role in Preventing and Responding to Terrorism*, see the PERF report at <http://www.policeforum.org/legislative.html#terrorism>.

All too frequently when an intelligence unit performs some type of analysis, no distinction is made within the unit about the different types of intelligence outputs and how they can contribute to the agency's goals. As a result, the unit provides far less support and awareness on crime issues and crime threats than could be done. Moreover, intelligence units too often are treated as a support unit, when they can proactively guide many investigative functions. In reality, a police intelligence unit may be placed best organizationally within an operations unit or division. The direct line of communication and the high degree of interaction required between intelligence analysts and investigators provide a richer interchange of information and ideas, thereby enhancing the quality of analysis.

INTELLIGENCE ANALYSIS starts at the most basic level –  
COLLECTING INFORMATION ABOUT THE “CRIME TRIANGLE”  
– just as in the case of PROBLEM ORIENTED POLICING.

Intelligence analysis starts at the most basic level – collecting information about the crime triangle: the offender, victim/commodity, and location – just

as in the case of problem oriented policing (see Figure 5-1). In a terrorist attack, for example, collecting and analyzing information about the victim and location can lead to information about the offender. Since terrorist groups typically have distinct methods, motives, and targets, these can be derived from the victim and location. With a criminal enterprise, the variable victim would be replaced by the commodity. In each instant, the type of information being sought should be driven by intelligence requirements. Defining the requirements (discussed in detail in Chapter 10) will provide greater efficacy to intelligence processes.

Each piece of information needs to be assessed for its validity and reliability to determine how much weight, if any, it contributes to understanding the crime, identifying suspects, and developing a case that can be prosecuted. Once the dependability of the information is assessed, an assessment of its substantive contribution to the investigation must be made, determining the information's relevance and materiality. This process is done for all evidence and information gathered during the course of an investigation.

Figure 5-1: Crime Triangle



As the body of assessed information accumulates, the intelligence analyst asks two questions:

1. What does this information mean?
2. Can I prove it?

In an example, an analyst receives the following information about a person that represents each activity over a 6-month period:

- A pen register indicating calls made from a targeted suspect's telephone.
- A printout of travel destinations from the suspect's travel agent.
- An accounting of ATM withdrawals from the bank.
- A credit card record of purchases.

In looking at the content of each of these items, the analyst uses both deductive reasoning to develop a hypothesis of what the information means within each type of record, and inductive reasoning to hypothesize what the collective information suggests about the suspect and his or her behavior related to criminality. Examples of questions are as follows:

71 N.B. = "nota bene" means "of particular note"

- Is there a pattern to the telephone calls based on the person called, locations called, and times called?
- Is there a pattern to the travel locations traveled to, days of the week, times of the day, and hotels stayed at?
- Is there a correlation between the telephone calls and the travel on any set of variables?
- Is there any pattern or evidence in the ATM withdrawals or any credit card purchases to show additional travel (such as driving to a location), specific or unique purchases, consistency in cash or credit transactions (either consistent amounts or amounts always ending even, full dollars, no change)?

After determining answers to these questions, the analyst may start drawing conclusions for which additional information is needed: Can the hypotheses be corroborated with other evidence? To corroborate the hypotheses, the analyst may request surveillance of the target(s), conduct an interview, or obtain information from a confidential informant. The analyst must also be looking for evidence of motive (N.B.,<sup>71</sup> motive helps explain the criminality and provide guidance on where to seek additional evidence), intent (N.B., to establish the mens rea or criminal intent) as well as specific criminal transactions (N.B., to document the actus reus or physical act of the crime).

This simple example demonstrates the general process of analysis. As diverse pieces of evidence are added to the investigation, the analyst often prepares an illustration which shows the linkages, as established by evidence among people, places, and organizations. This is referred to as link diagram (Figure 5-2). When transactions are involved, such as drug trafficking, illicit weapons sales, or money laundering, the analyst often prepares a diagram called a commodity flow (Figure 5-3). These two analytic tools are useful in visualizing the relationships and process in complex criminal investigations.<sup>72</sup> They not only help guide the investigation but are also useful in presenting the case in court.

As the analysis progresses, the analyst writes reports to describe to administrators, supervisors, investigators, and/prosecutors, the progress that is being made on the case, the direction that the investigation should follow, new information or concerns, and resources or assistance needed to develop the case further. Certain types of information derived from the reports also need to be disseminated to a broader group, for example, giving information to patrol officers and neighboring jurisdictions in the form of BOLOs.<sup>73</sup> If the intelligence is not disseminated, then much of its value is lost.

72 Various commercial software programs are available to aid in preparing these diagrams. Most software permits the user to embed photographs, images of evidence, and even video to further illustrate the relationships within a criminal enterprise or the commodity flow.

73 BOLO = Be On the Look Out.

**Figure 5-2: Link Diagram Illustration**

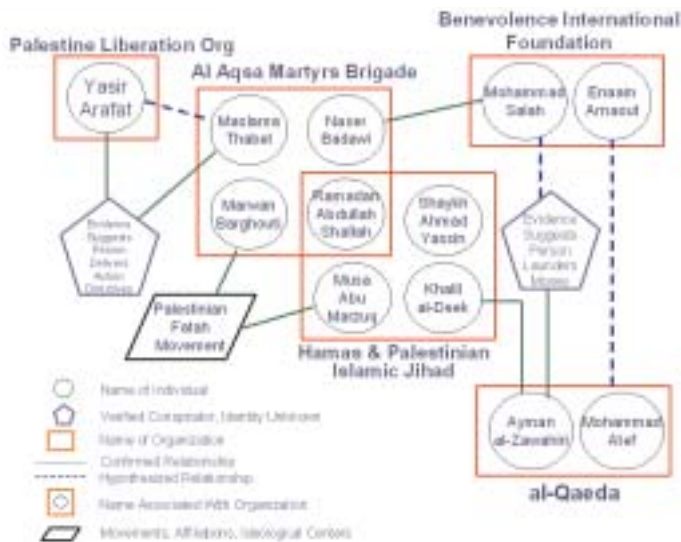
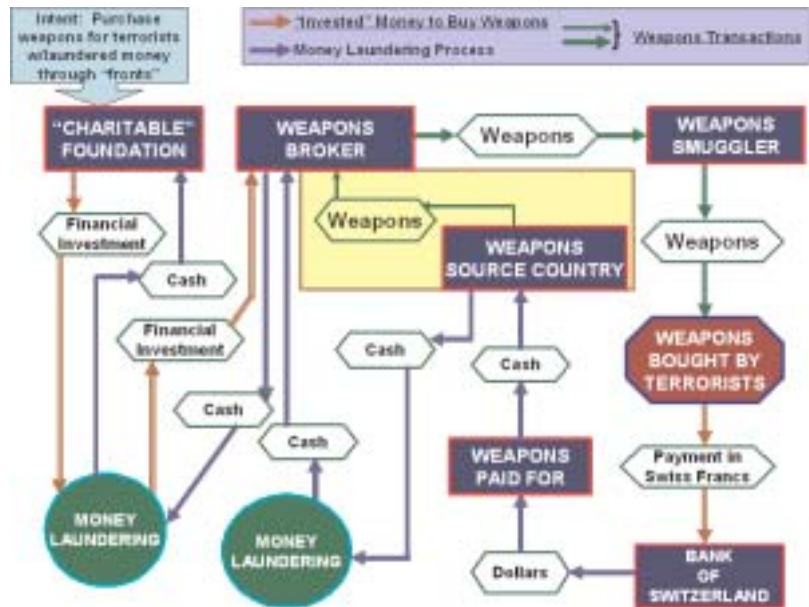


Figure 5-3: Commodity Flow Chart Illustration



One of the greatest weaknesses in the organizational culture of intelligence units is the unwillingness to share information. Police leadership must ensure that intelligence is proactively shared with the people who need the information, both inside the organization and with external agencies. Too many times, intelligence units act as a sponge, absorbing information from diverse sources, but are reluctant to share what they have gathered and learned. This gate-keeping practice is dysfunctional, wastes resources, and contributes to the reluctance of field personnel to submit information. Having stated that the information must be shared, there are some caveats about disseminating law enforcement intelligence. First, care must be taken to ensure security of the information so that an investigation will not be compromised. While this is a real concern, some intelligence units become overly cautious. Like most things in life, there must be a reasonable balance. A second concern is that tactical and operational intelligence is often accusatory, but not conclusive. The amount of information in a developing case may strongly suggest a person's criminal activity but not meet the standard of probable cause. As such, the intelligence may be used for further inquiry, gathering more information to either expand or conclude the investigation. However, if the intelligence

and related information should become public and cannot be linked effectively to an evidence-based criminal investigation, the agency may risk liability for a civil rights lawsuit.

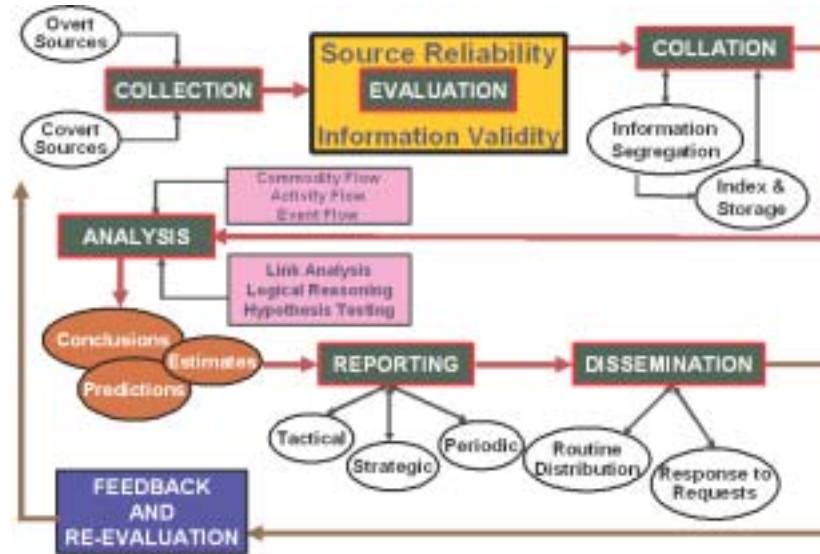
With complex criminal behavior like terrorism, an effective law enforcement intelligence unit can be critical to both the prevention of a terrorist attack and the apprehension of offenders. Law enforcement agencies need to review their intelligence function carefully, ensuring that it is structured, directed, and staffed in a manner that can provide the critical information, through analysis, that is needed. They should give consideration to developing a regional intelligence capacity to develop more comprehensive, multijurisdictional information on community problems and threats. The value of state and regional approaches is multifaceted. First, it is more cost-efficient because there would be just one intelligence structure for multiple agencies sharing resources to operate the intelligence unit. Second, it is more effective because there is a broader array of information input covering a wider geographical area. Third, since criminals regularly cross jurisdictional boundaries, a regional approach gives law enforcement more flexibility in criminal investigations. When all variables are factored in, a regional intelligence capacity is organizationally and operationally the most efficacious approach.

## The Intelligence Cycle

This brief summary of analysis followed a process known as the intelligence cycle (Figure 5-4). It is an ongoing process that seeks continuous input so that every new piece of information which meets the standards of rigor can be added to the evidentiary picture. As is evident, this can be a labor-intensive process which requires eclectic knowledge and strong analytic ability to be successful.

The fundamental point to draw from this discussion is that pieces of information gathered through the collection process are not intelligence. Rather, intelligence is the knowledge derived from the logical integration and assessment of that information and is sufficiently robust to enable law enforcement to draw conclusions related to a particular crime.

Figure 5-4: Intelligence Cycle



74 **NOTE:** Discussion of or reference to specific software products and/or information services in this section should not be considered an endorsement of the product by the author, Department of Justice, or any of its components. Rather, the references are illustrations to supplement discussion of the issues.

As noted previously, the FBI has broad responsibility (and authority) in the intelligence process that integrates both law enforcement and national security intelligence. As a result, the FBI Intelligence Program approaches the cycle somewhat differently. Figure 5-5 provides definitions of the FBI Intelligence Cycle – information that is important for state, local, and tribal law enforcement (SLTLE) personnel to understand to be effective consumers of the FBI intelligence products and communicate effectively on matters related to FBI intelligence operations.

## INFORMATION MANAGEMENT AND INTELLIGENCE PROCESSES<sup>74</sup>

Information is the currency of intelligence. In the era of digital communications and networking, it is virtually impossible to deal with the management and sharing of information without considering technological implications. Technology and information transcend a number of boundaries which are often blurred. Internet protocols (IP), for example, are often critical for collecting, analyzing, and sharing information. The sections that follow serve as a primer for information technology and intelligence. Concepts, trends, resources, and issues are discussed to provide familiarization to the manager.

**Figure 5-5: FBI Intelligence Cycle Definitions and Processes**

**FBI INTELLIGENCE PROGRAM  
DEFINITION AND PROCESS OF THE FBI INTELLIGENCE CYCLE**

1. **REQUIREMENTS:** Requirements are identified information needs – what we must know to safeguard the nation. ... Requirements are developed based on critical information required to protect the United States from National Security and criminal threats.
2. **PLANNING AND DIRECTION:** Planning and direction is management of the entire effort from identifying the need for information to delivering the intelligence product to the consumer. It involves implementation plans to satisfy requirements levied on the FBI as well as identifying specific collection requirements based on FBI needs. Planning and direction is also responsive to the end of the cycle because current and finished intelligence, which supports decision making, generates new requirements.
3. **COLLECTION:** Collection is the gathering of raw information based on the requirements. Activities such as interviews, technical and physical surveillances, human source operations, searches, and liaison relationships results in the collection of intelligence.
4. **PROCESSING AND EXPLOITATION:** Processing and exploitation involves converting the vast amount of information collected to a form usable by analysts. This is done through a variety of methods including decryption, language translation, and data reduction. Processing includes the entering of raw data into databases where it can be exploited for use in the analysis process.
5. **ANALYSIS AND PRODUCTION:** Analysis and production is the converting of raw information into intelligence. It includes integrating, evaluating, and analyzing available data, and preparing intelligence products. The information's reliability, validity, and relevance is evaluated and weighed. The information is logically integrated, put in context, and used to produce intelligence. This includes both "raw" and "finished" intelligence. Raw intelligence is often referred to as "the dots". ... "Finished" intelligence reports "connect the dots" by putting information in context and drawing conclusions about its implications.
6. **DISSEMINATION:** Dissemination...is the distribution of raw or finished intelligence to the consumers whose needs initiated the intelligence requirements. The FBI disseminates information in three standard products – FBI Intelligence Information Reports, FBI *Intelligence Bulletins*, and FBI *Intelligence Assessments* described and illustrated in Chapter 11). FBI intelligence customers make decisions – operational, strategic, and policy – based on the information. These decisions may lead to the levying of more requirements, thus continuing the FBI intelligence cycle.

**From:** FBI Office of Intelligence. The FBI Intelligence Cycle: *Answering the Questions...* A desk reference guide for FBI employees. (Pamphlet form). (July 2004).

## Software to Aid the Intelligence Process<sup>75</sup>

Just like any other aspect of police management, there are a number of vendors who will develop proprietary software for intelligence records, analysis, and secure electronic dissemination.<sup>76</sup> Such systems can be expensive to purchase and maintain and may not be a viable option for many medium and small agencies because of fiscal constraints. For most agencies, a wide array of off-the-shelf software can aid the intelligence function. Most obvious are word processing and presentation software programs for preparing reports and briefings. Beyond these, a number of software programs that can be useful to the intelligence function include the following:

75 Of course, software compatibility issues still remain and should be considered in any purchase. One can not assume compatibility. For example, even though a system is operating on Windows XP, if there is some type of proprietary software on the system, it could cause incompatibility issues with off-the-shelf software that would otherwise operate normally with Windows XP. For more information, see *The Law Enforcement Tech Guide: How to Plan, Purchase and Manage Technology (successfully)!* at: [www.cops.usdoj.gov/default.asp?Item=512](http://www.cops.usdoj.gov/default.asp?Item=512). See also, SEARCH technical assistance: [www.search.org/programs/technology/](http://www.search.org/programs/technology/).

76 See the summary of Information Technology Initiatives of the U.S. Office of Justice Programs at [http://it.ojp.gov/topic.jsp?topic\\_id=85](http://it.ojp.gov/topic.jsp?topic_id=85) as well as the International Association of Chiefs of Police Technology Clearinghouse at <http://www.iacptechnology.org/>.

77 For examples of databases, see [dir.yahoo.com/Computers\\_and\\_Internet/software/databases/](http://dir.yahoo.com/Computers_and_Internet/software/databases/).

78 [www.spss.com/](http://www.spss.com/)

- **Databases:** A law enforcement agency can use commercially available databases to create an intelligence records system that is searchable on a number of variables. Most current databases permit the user to custom design the variable fields and include images as well as text.<sup>77</sup>
- **Spreadsheets:** The analytic capacity of most current versions of spreadsheet software is reasonably robust. For example, data from a pen register can be entered and compared, complete with different graphing options, to identify associations and trends. Virtually any kind of data can be analyzed and converted to bar graphs, scatter plots, line charts, area charts, radar graphs, surface charts, and other graphing options to aid in data interpretation and presentation.
- **Mapping Programs:** Inexpensive mapping software, such as Microsoft Streets and Maps, can be useful for both analysis and presentation of intelligence data. The maps can be used for strategic intelligence illustrations of any geographic-based variable of interest (e.g., people, groups, meetings, commodity distribution, trafficking of contraband). In addition, programs such as these have integrated databases which, although typically limited in character, nonetheless provide sufficient capability to include descriptive information about entries on the map. (see Figure 5-6 as an illustration.)
- **Statistical Programs:** For strategic analysis, statistical software with a graphic capability is very useful. Perhaps the best known, and most powerful, is SPSS.<sup>78</sup> To be most effective, the SPSS user must have a sound knowledge of statistics. A number of other statistical analysis

Figure 5-6: Illustration of Descriptive Map - Hate Groups in the U.S.



programs cost less and are somewhat easier to use; however, such programs have fewer analytic features and options.

- **Intelligence Analysis Software:** Software to assist in organizing, collating, integrating, and presenting data for analysis is an invaluable tool. Perhaps the most widely used analytic software is offered by I2 Investigative Analysis Software.<sup>79</sup> As illustrated in Figure 5-7, the software integrates a number of features that aid in the analysis of data. For a law enforcement agency that is able to have an intelligence analyst on staff, analytic software is an essential investment.

79 [www.i2.co.uk/Products/](http://www.i2.co.uk/Products/)

80 See <http://www.cybercrime.gov/> and <http://www.crime-research.org/>.

## Information Technology Management

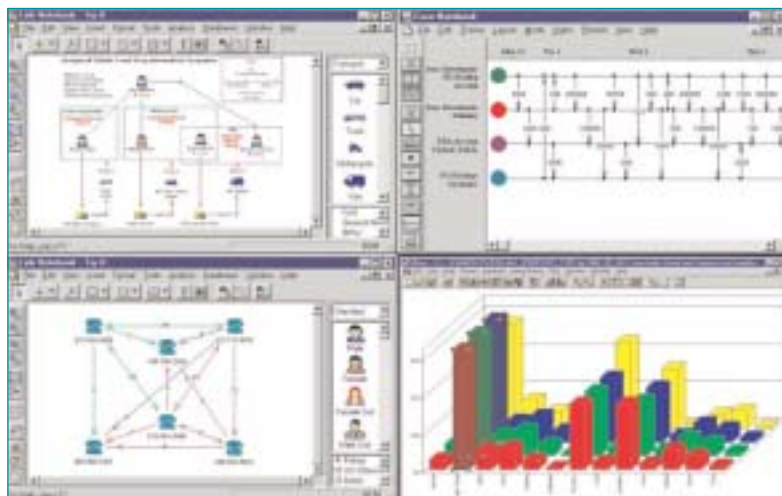
There are additional technology concerns beyond those of software described above. The increasingly lower costs of networking technology, the commonality of Internet Protocols for information sharing, the ability to share not only text but also images, audio, and video, and the ease of access to information contribute to the growth of law enforcement intranets and extranets for secure information sharing. As agencies develop these networks, two important elements must be kept in mind: Security and compatibility.

With the pervasive presence of computer crime and unauthorized network intrusions,<sup>80</sup> it is essential to build exceptional security into any network. The significant growth of wireless networks and Bluetooth<sup>®</sup> peripheral

connections only serve to aggravate the security problem. Among the security issues to be considered are these:

1. **Manual Assurance of Data Handling:** Virtually all data is handled manually at some point. There must be security standards and quality control of data that is entered into the system.
2. **Physical Security:** There must be effective measures in place to ensure the security of the facility housing computer(s), servers, and any other related hardware ( e.g., PDAs) and peripherals (e.g., printers) that have access to the system.
3. **Operations Security:** Processes for quality control of personnel who are system operators/managers as well as security monitoring of people who have access to the secure area where computers and servers are housed. This includes maintenance and custodial personal, clerical personnel, and others who may have access to the secure area.
4. **Management-Initiated Controls:** This includes...
  - Management oversight of system operations.
  - Administrative policy for computer access and use.
  - Fair use policies if a public website is provided.
  - Establishment of data security management policies.
  - Establishing data classification protocols for control and access.

Figure 5-7: Illustration of I2 Analysis Screens\*



\*Copyright © 2004 I2 Ltd. All Rights Reserved. The Visual Space, Capital Park, Fulbourn, Cambridge, CB1 5XH, UK

5. **Computer System Control:** Strict access to the system should be controlled by:
- Authorization of personnel. Defining policies and standards as to who may have access to the system, for what purposes access is granted, and defined standards of acceptable use of the system.
  - Software access controls.<sup>81</sup> Beyond standard user name and password controls, and all the well-known security precautions associated with these, the system should be protected by a Virtual Private Network (VPN) for access control by authorized users.
  - System protection and inoculation. All networked systems should have a multistage firewall and constantly updated virus definitions.
6. **Encryption for wireless devices:** Network encryption should be enabled if wireless devices are used with an intelligence records system or intelligence-related communications.
7. **Access audit controls:** A real-time auditing system should monitor all accesses to the system, user identification, activity during the user period, length of time, and IP number of the computer accessing the system.
8. **Control of remote storage media:** Policies need to be established and technological controls instituted to monitor the use and control of restricted data related to remote storage media (e.g., disks, CDs, thumb drives, etc.).

Following these procedures will not only protect intelligence records, they will meet the data security standards of 28 CFR Part 23.

On the issue of compatibility, a report from the Global Justice Information Sharing Initiative observed the following:

During the past 30 years, the lack of standards for linking justice information systems has been responsible for a substantial part of the high costs involved with information exchange and has contributed significantly to the associated difficulties of exchanging information between justice agencies. Now that a variety of organizations have acknowledged the importance of data exchange standards, it is critical that the adoption of justice

81 At this writing, the Bureau of Justice Assistance is developing a "Trusted Credentials Project" that would identify a process (which may include both software and hardware) that would allow different systems to recognize and accept any credential previously identified as trustworthy. For example a LEO user could pass seamlessly between networks with a single sign-on once that user was validated to the network. This would enable network users to integrate between networks without the need to sign on and off each of them separately.

information exchange standards take into account emerging technologies which will serve as the basis for information exchange in a broad spectrum of industry sectors.<sup>82</sup>

As a result, the initiative has done a significant amount of work in developing consistent definitions, protocols, and data standards – including the XML standard for IPs – to ensure system compatibility. The results will increase connectivity, interoperability, and, consequently, better information sharing.<sup>83</sup>

## Information Technology Resources

Other resources are available that will aid in training and program development for the intelligence function. While these resources address issues broader than intelligence, per se, they are nonetheless valuable for the intelligence manager. The websites contain training resources, documents, and links that are useful.

- National White Collar Crime Center<sup>84</sup>
- SEARCH - The National Consortium for Justice Information and Statistics<sup>85</sup>
- Crime Mapping Analysis Program<sup>86</sup>
- Crime Mapping and Problem Analysis Laboratory of the Police Foundation<sup>87</sup>
- Office of Justice Program Information Technology Website.<sup>88</sup>

## Open-Source Information and Intelligence

Volumes of information have been written on open-source intelligence.<sup>89</sup> The intent of the current discussion is to simply familiarize the law enforcement manager with the open-source concept and its application to a law enforcement agency.

Open-source *information* is any type of lawfully and ethically obtainable information that describes persons, locations, groups, events, or trends. When raw open source information is evaluated, integrated, and analyzed it provides new insight about intelligence targets and trends – this is open-

82 *Technology Considerations in the Development of Integrated Justice Data Exchange Standards*. A report of the Global Justice Information Sharing Initiative, p. 1. <http://it.ojp.gov/technology/files/IIIS-Standards.pdf>.

83 For more information, see the OJP Information Technology Initiatives website at [http://it.ojp.gov/topic.jsp?topic\\_id=85](http://it.ojp.gov/topic.jsp?topic_id=85), the Global Justice XML website at [http://it.ojp.gov/topic.jsp?topic\\_id=43](http://it.ojp.gov/topic.jsp?topic_id=43) and the report: National Law Enforcement and Corrections Technology Center. (2001). *A Guide for Applying Information Technology to Law Enforcement*. Washington, DC: Office of Science and Technology, National Institute of Justice (Available at: <http://www.nlectc.org/pdf/files/infotechguide.pdf>.)

84 <http://www.nw3c.org/>

85 <http://www.search.org/>

86 <http://www.nlectc.org/cmap/justnet.html>

87 [http://www.policefoundation.org/docs/crime\\_mapping.html](http://www.policefoundation.org/docs/crime_mapping.html)

88 <http://it.ojp.gov/index.jsp>

89 As one example, see <http://www.oss.net>.

source intelligence. Open-source information is wide-ranging and includes the following:

- All types of media<sup>90</sup>
- Publicly available data bases<sup>91</sup>
- Directories<sup>92</sup>
- Databases of people, places, and events<sup>93</sup>
- Open discussions, whether in forums, classes, presentations, online discussions on bulletin boards, chat rooms, or general conversations
- Government reports and documents<sup>94</sup>
- Scientific research and reports<sup>95</sup>
- Statistical databases<sup>96</sup>
- Commercial vendors of information<sup>97</sup>
- Websites that are open to the general public even if there is an access fee or a registration requirement
- Search engines of Internet site contents.<sup>98</sup>

90 See <http://newslink.org/>.

91 See as an example <http://www.searchsystems.net/> and <http://www.factfind.com/datab ase.htm>.

92 One of the most extensive directories is in <http://www.yahoo.com>. However, other sources of directories exist, such as <http://www.search-it-all.com/all.aspx>.

93 See as an example <http://www.namebase.org/>, <http://www.searchsystems.net/> and <http://www.crimetime.com/online.htm>.

94 See [http://www.clearinghouse.net/cgi-bin/chadmin/viewcat/Government\\_Law/](http://www.clearinghouse.net/cgi-bin/chadmin/viewcat/Government_Law/)

Importantly, OPEN-SOURCE INFORMATION about individuals must still meet the CRIMINAL PREDICATE REQUIREMENT to be retained in an agency's INTELLIGENCE FILES.

The main qualifier that classifies information as open source is that no legal process or clandestine collection techniques are required to obtain the data. While open-source data has existed for some time, networking has increased its accessibility significantly. For example, if an analyst was preparing a strategic intelligence report on trends in international terrorism, the analyst may go to the websites of the U.S. Department of State Counterterrorism Office,<sup>99</sup> the FBI terrorism reports,<sup>100</sup> and the Israeli Defense Force terrorism statistics center<sup>101</sup> to download the various reports and data. If the analyst was preparing a report on right-wing extremists, he or she may visit the Southern Poverty Law Center<sup>102</sup> to download reports or

[government?kywd, http://www.thecre.com/links/fedgov-links.html](http://www.thecre.com/links/fedgov-links.html), [http://www.firstgov.gov/Topics/Reference\\_Shelf.shtml](http://www.firstgov.gov/Topics/Reference_Shelf.shtml) and <http://www.firstgov.gov/Citizen/Topics/PublicSafety.shtml>.

95 See <http://www.fas.org>.

96 See <http://www.lib.umich.edu/govdocs-stats-pilot/> and <http://www.ojp.usdoj.gov/bjs/>.

97 See as an example <http://www.accudatalists.com/index1.cfm>.

98 Beyond the commonly used Internet search engines such as Google, Lycos, Yahoo, Ask Jeeves, and others, a unique web search site is <http://www.itools.com/>.

go to a white supremacy website, such as Stormfront<sup>103</sup> to read the information, conduct further research by reading materials, and following hyperlinks to gain more raw data to prepare an independent report.

Raw information obtained from open sources tends to fall into two categories that have important significance for an SLTLE agency: (1) Information about *individuals* and (2) *aggregate* information. As a general rule, civil rights attach to open source information about individuals, such as a credit report or a legal notice in a newspaper about a lawsuit, *when it is in the intelligence records system* of an SLTLE agency. As a general rule, no civil rights attach to aggregate information, such as the advocacy of terrorism against the U.S. on an Islamic radical website or the threat by a radical environmental group to burn down a university research facility. If, however, individuals are named in an aggregate information source, such as a news story about radical anarchists, some civil rights protections may attach. These instances must be assessed on case-by-case before being retained by the law enforcement agency.

See pg. 71

99 <http://www.state.gov/s/ct/>

100 <http://www.fbi.gov/publications/terror/terroris.htm>

101 <http://www1.idf.il/DOVER/site/homepage.asp?clr=1&sl=EN&id=-8888&force=1>

102 <http://www.splcenter.org>

103 <http://www.stormfront.org/>

Importantly, open-source information about individuals must still meet the criminal predicate requirement to be retained in an agency's intelligence files. The key is not the source of the information, but *what is being retained* by a law enforcement agency about a person. Illustrations of issues to consider include the following:

- What types of open-source information about a person should be kept on file by the police concerning a "person of interest" who is not actually a suspect?
- How aggressive should a police agency be in gaining open-source information on people who expressly sympathize and/or support a terrorist group as determined by statements on a web page, but do not appear to be part of a terrorism act nor active in the group?
- How does a police agency justify keeping information on a person when a suggestive link between the suspicious person and a terrorist group has been found through open-source research, but not a confirmed link through validated and corroborated evidence?

Creating intelligence dossiers is both tempting and easy using open-source data. The question to consider, however, is whether it is proper. The reader is asked to reflect on the earlier discussion of history and the lessons learned. Among those lessons was the fact that the police cannot retain intelligence dossiers on persons for whom a criminal predicate is not articulated in the facts. Essentially, by applying the Terry<sup>104</sup> test, if the police do not have an articulable reason to link a suspect to a crime, they cannot keep these records in a dossier. As noted previously, the issue is not whether the information was from an open source, but whether the police could properly keep the information. Law enforcement agencies must consider the reason for which information is being retained, not the *source*.

Data can also be gathered on individuals through open-source information on the Internet (often for a fee). Companies such as AutoTrack,<sup>105</sup> Accurint,<sup>106</sup> and Lexis-Nexis<sup>107</sup> have merged a wide array of public databases coupled with data migration techniques to permit merging of extraordinarily detailed information about people into a summary report. Marketing data available through subscription from many companies and even news searches – notably through the comprehensive databases of Lexis-Nexis<sup>108</sup> – can provide a surprising amount of detail about people which, when analyzed, presents a detailed profile that may be useful in varying aspects of an investigation. In addition, university libraries offer a wide array of research and resource tools that are often available at no cost.<sup>109</sup>

The fact that information is open source should not dissuade a law enforcement officer or analyst from using it. Indeed, there is often very high-quality, insightful evidence available from open sources. So much so, that the 9/11 Commission, in its Final Report, recommended that a new Open Source Agency be added to the U.S. intelligence structure.<sup>110</sup> For example, news services have global networks of sophisticated communications and informants with trained staff to conduct research and investigate virtually all issues that would be of interest to a consuming public. As a general rule, responsible news organizations also have editorial policies to ensure that the information is valid, reliable, and

104 This refers to the U.S. Supreme Court “stop and frisk” case of *Terry v. Ohio* 392 US 1 (1968) wherein the Court held that police officers could stop, detain, and frisk a person whose actions, based on the experience of a police officer, suggested that the person was committing, had committed, or was about to commit a crime.

105 <http://www.autotrack.com/>

106 <http://www accurint.com>

107 <http://www.lexis-nexis.com/risksolutions/lawenforcement/>

108 <http://www.lexis-nexis.com/>

109 As an example, see <http://www.lib.msu.edu/harris23/crimjust/index.htm> and <http://er.lib.msu.edu/>.

110 National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report. Washington, DC: U.S. Government Printing Office, p. 413. Also available in full online at <http://www.9-11commission.gov/report/911Report.pdf>.

corroborated. As such, the news media is a tremendous source of information that should be part of a law enforcement agency's "intelligence toolkit."

As an illustration, the Anti-Terrorism Information Exchange (ATIX), a website operating on the Regional Information Sharing Systems secure network, RISS.net, is designed to provide groups of defined users with secure interagency communication, information sharing, and dissemination of terrorist threat information. Part of the ATIX site includes news stories on all aspects of terrorism (Figure 5-8). Not only does this help users stay up-to-date on focused terrorism-related news stories, but the ongoing consumption of this news develops an "intellectual database" wherein the user becomes aware of issues, trends, locations, and methodologies related to terrorism.

Open-source information can be a tremendous resource for a law enforcement agency and should be incorporated as part of an agency's intelligence plan. The important caveat, however, is to ensure that all file requirements are applied to open-source data.

## CONCLUSION

This chapter familiarized the reader with terminology and concepts that transform information to intelligence. Most law enforcement officers will not be involved in the analytic process; however, understanding that process provides important insights into understanding the kinds of information an intelligence analyst needs and what kind of output can be expected.

Police LEADERSHIP must ensure that intelligence is proactively SHARED with the people who need the information—both inside the ORGANIZATION and with EXTERNAL AGENCIES.

Figure 5-8: Illustration of Open-Source News Stories on RISS ATIX

**ATIX News** Archive

**National Organizations Partner to Launch National Preparedness Month**  
The U.S. Department of Homeland Security (DHS), The America Prepared Campaign, the American Red Cross, the National Association of Broadcasters and the U.S. Department of Education have joined a coalition of more 50 national organizations to engage Americans in emergency preparedness by launching National Preparedness Month on September 9. Post:08/11/04

**New Terror Threat Info Warns of Plans With Helicopters, Limos**  
The FBI is warning that al-Qaeda could attempt to commandeer helicopters, limousines and other rental vehicles to launch attacks inside the United States. Post:08/04/04

**Vaccine Protects Mice Against Ricin**  
U.S. military researchers say they have produced a vaccine that protects mice from the deadly effects of inhaled ricin – one of the most toxic substances known. Post:07/26/04

**Major Exercises Set For NORAD and USICRTHCOM**  
Two major exercises, Amalgam Vigil 04 (AV04) & Determined Promise 04 (DP04), kick off this week for the North American Aerospace Defense Command and the U.S. Northern Command to test the commands' response to terrorist events on a national, state, and local level. Post:08/03/04

**Intelligence Agencies Next in Line for Reorganization**  
With the president's endorsement yesterday of a national intelligence czar, the government appears on track for another major restructuring. Post:08/02/04



This led into a discussion of software and technology issues that may be used in support of the SLTLE intelligence function. Needs will vary by agency; hence, the discussion was a broad buffet of software and technology tools from which a manager may begin making resource decisions. Finally, transcending the line between analysis and technology, open-source information and intelligence was discussed with respect to its use, value, resources, and limitations.

The reader should take away from this chapter a thorough understanding of information management and analysis issues as they relate to the development of an intelligence function.

