FMI 2-22.9
December 2006
Expires December 2008

OPEN SOURCE INTELLIGENCE

Distribution Restriction: Distribution authorized to U.S. Government agencies and their contractors. This determination was made on 10 July 2006. Other requests for this document must be referred to Directorate of Doctrine, ATTN: ATZS-CDI-D, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017.

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

Headquarters, Department of the Army

FMI 2-22.9

Field Manual Interim
No. 2-22.9

Headquarters
Department of the Army
Washington, DC, 5 December 2006
Expires 5 December 2008

Open Source Intelligence

Contents

Page

Distribution Restriction: Distribution authorized to U.S. Government agencies and their contractors. This determination was made on 10 July 2006. Other requests for this document must be referred to Directorate of Doctrine, ATTN: ATZS-CDI-D, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017.

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

Figures

Tables

Preface

This manual expedites delivery of doctrine that the proponent has approved for immediate use in training and operations. The manual facilitates a common understanding of Army open source intelligence (OSINT) operations. As interim doctrine, it serves as a catalyst for analysis and development of Army OSINT training, concepts, materiel, and force structure. It brings Army intelligence doctrine in line with the characterization of OSINT as an intelligence discipline in Joint Publication 2-0.

This manual supersedes the definition and the description of OSINT in FM 2-0.

This manual provides fundamental principles; initial tactics, techniques, and procedures (TTP); and terminology for Army OSINT operations.

- Chapter 1 provides an introduction to OSINT.
- Chapter 2 describes the fundamentals of Army OSINT, its operations, and organizations.
- Chapters 3 through 5 provide initial TTP of OSINT operations.
- Appendixes provide information that supports or expands upon the information in the chapters.

This manual applies to all Active Army, the Army National Guard/Army National Guard of the United States, and the United States Army Reserve unless otherwise stated. It serves as a reference for personnel who are developing doctrine and TTP; materiel and force structure; and training for intelligence operations. It is also a reference for intelligence personnel at National, Joint, Interagency, other Service, and multinational or coalition partners.

United States Army Training and Doctrine Command is the proponent for this publication. The preparing agency is the Directorate of Doctrine, US Army Intelligence Center. Send written comments and recommendations on Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, ATTN: ATZS-FDD-D (FMI 2-22.9), U.S. Army Intelligence Center and Fort Huachuca, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017. Follow the DA Form 2028 format or submit an electronic DA Form 2028.

Unless otherwise stated, masculine nouns and pronouns do not refer exclusively to men.

Terms that have Joint or Army definitions are identified in both the glossary and the text. The glossary lists most terms used in this manual that have Joint or Army definitions. Terms for which this manual is the proponent manual (the authority) are indicated with an asterisk in the Glossary. 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 manual follows the definition.

This page intentionally left blank.

Chapter 1

Introduction

American military professionals have collected, translated, and studied articles, books, and periodicals to gain knowledge and understanding of foreign lands and armies for over 200 years. The value of publicly available information as a source of intelligence has, however, often been overlooked in Army intelligence operations. This manual provides a catalyst for renewing the Army's awareness of the value of open sources; establishing a common understanding of OSINT; and developing systematic approaches to collection, processing, and analysis of publicly available information.

Though always available, the exponential growth in computer technology and the Internet over the past two decades has placed more public information and processing power at the finger tips of soldiers than at any time in our past. A body of knowledge on culture, economics, geography, military affairs, and politics that was once the domain of grey-beard scholars now rest in the hands of high school graduates. For intelligence personnel, this combination of technology and information enables them to access a large body of information that they need to answer their unit's intelligence requirements. As the following quote illustrates, our reliance on classified databases and external support has, however, often left our soldiers uninformed and ill-prepared to capitalize on the huge reservoir of unclassified information available from open sources.

> *I am deploying to El Salvador in a few months, and will be serving as the S2 Noncommissioned Officer in Charge for the task force there. I need to put together some information for the Task Force Commander on the country and the situation there. Although I have served in Operation IRAQI FREEDOM I, I have no idea how to go about this, for when we deployed to Iraq the country brief was pretty much handed to us.*
>
> *—Sergeant, S2 Noncommissioned Officer in Charge, Engineer Group*

From El Salvador to Iraq, the US Army operates in diverse operational environments around the World. These diverse operational environments mean the development and use of OSINT is not a luxury but a necessity. Open sources possess much of the information that we need to understand the physical and human factors of the operational environments in which we conduct or may conduct military operations. In truth, much of our understanding of these environments, our World, is based on publicly available information that we learned from educators, journalists, news anchors, and scholars.

The US Army Intelligence and Security Command's (INSCOM) Asian Studies Detachment demonstrates the characteristics and the power of sustained OSINT operations. Since 1947, the Detachment has collected, processed, and analyzed publicly available information on capabilities, disposition, and readiness of military forces of China, North Korea, and other potential adversaries. It has also reported on the economic, environmental, political, and social conditions within the region.

In recent years, the Asian Studies Detachment has reported on elevated tensions between China and Taiwan during the Taiwan presidential elections in 2004; security threats to US, allied forces conducting humanitarian relief operations in Indonesia following the December 2004 tsunami devastation; and strategy and tactics employed during the August 2005 Sino-Russian combined counterterrorism Exercise PEACE MISSION 2005.

As testimony to the high value of OSINT analysis and reporting, Asian Studies Detachment's intelligence information reports since 2003 have received 28 "Major Significance" evaluations from the Defense Intelligence Agency (DIA), National Ground Intelligence Center (NGIC), and the US Air Force's National Air and Space Intelligence Center (NASIC) on topics ranging from North Korean underground facilities to Chinese Peoples Liberation Army Air Force air and space science and technology (S&T) developments.

At the tactical level, some units are task organizing their assets into OSINT organizations. The following is an example from the 3d Infantry Division's deployment to Iraq in 2005. It illustrates how intelligence personnel adapt to and succeed at new missions. In the example, the company commander task organized his common ground station (CGS) team into an OSINT team.

> *With their four to five interpreters (two of which are American citizens) and a steady flow of radio, television and newspaper reports, the open source intelligence team produced a daily rollup with analysis. Their office consisted of one television with local and international cable, one laptop connected to the nonsecure internet protocol router network, an amplitude and frequency modulated radio and the daily newspapers, usually ten to fifteen papers per day. Also, the team acquired a video camera recorder and digital video device player to study confiscated propaganda and other media. They understand the importance of local reporting to the success of the brigade combat team campaign and have made it a point to conduct thorough research on topics of local importance. Their product was studied and further analyzed by the intelligence, surveillance, and reconnaissance analysis team at the brigade combat team tactical operations center prior to submission to the brigade combat team S2 and dissemination to battalions or division.*
>
> *— Captain, MI Company Commander, Brigade Combat Team*

This manual serves as a catalyst for defining and describing Army OSINT operations. During its 2-year lifecycle, the TTP in this manual will evolve as the Army and the other members of the US Intelligence Community work to integrate and synchronize OSINT operations between echelons. This evolution will occur in part as the Assistant Deputy Director of National Intelligence (DNI) for Open Source establishes the National Open Source Enterprise which is envisioned as a distributed yet collaborative enterprise.

In the end, the US Intelligence Community will reach consensus about the who, what, where, when, why, and how of OSINT operations. This consensus will take form in future Army and Joint intelligence doctrinal literature as well as DNI guidance in the form of Intelligence Community Directive 301, The National Open Source Enterprise, which will replace Director of Central Intelligence Directive 1/7.

Chapter 2

Fundamentals

2-1. OSINT operations are integral to Army intelligence operations. Directly or indirectly, publicly available information forms the basis of all intelligence operations and intelligence products. The availability, depth, and range of publicly available information enable intelligence organizations to satisfy many intelligence requirements without the use of specialized human or technical means of collection. OSINT operations support other intelligence, surveillance, and reconnaissance (ISR) efforts by providing foundational information that enhances collection and production. As part of a multidiscipline intelligence effort, the use and integration of OSINT ensures decisionmakers have the benefit of all available information.

DEFINITION

2-2. The *National Defense Authorization Act for Fiscal Year 2006* states, “Open source intelligence is produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.” Expressed in terms of the Army intelligence process, OSINT is relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to intelligence requirements. Two important terms in these complementary definitions are—

- **Open Source,** which is any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure.
- **Publicly Available Information,** which is data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

OPEN SOURCE INTELLIGENCE DISCIPLINE

2-3. The source, the information, and the collection means rather than a specific category of technical or human resources distinguish OSINT from other intelligence disciplines (see Figure 2-1). Open sources broadcast, publish, or otherwise distribute unclassified information for public use. The collection means (techniques) for gathering publicly available information from these media of communications are unintrusive. Other intelligence disciplines use confidential sources or intrusive techniques to collect private information. Confidential sources and private information are—

- **Confidential Source**, which is any person, group, or system that provides information with the expectation that the information, relationship, or both, are protected against public disclosure.
- **Private Information,** which is data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization. There are two subcategories of private information: classified information and controlled unclassified information.
  - Classified information requires protection against unauthorized disclosure and is marked to indicate its classified status when in documentary or readable form.
  - Controlled unclassified information requires the application of controls and protective measures, for a variety of reasons (that is, sensitive but unclassified, or for official use only), not to include those that qualify for formal classification.

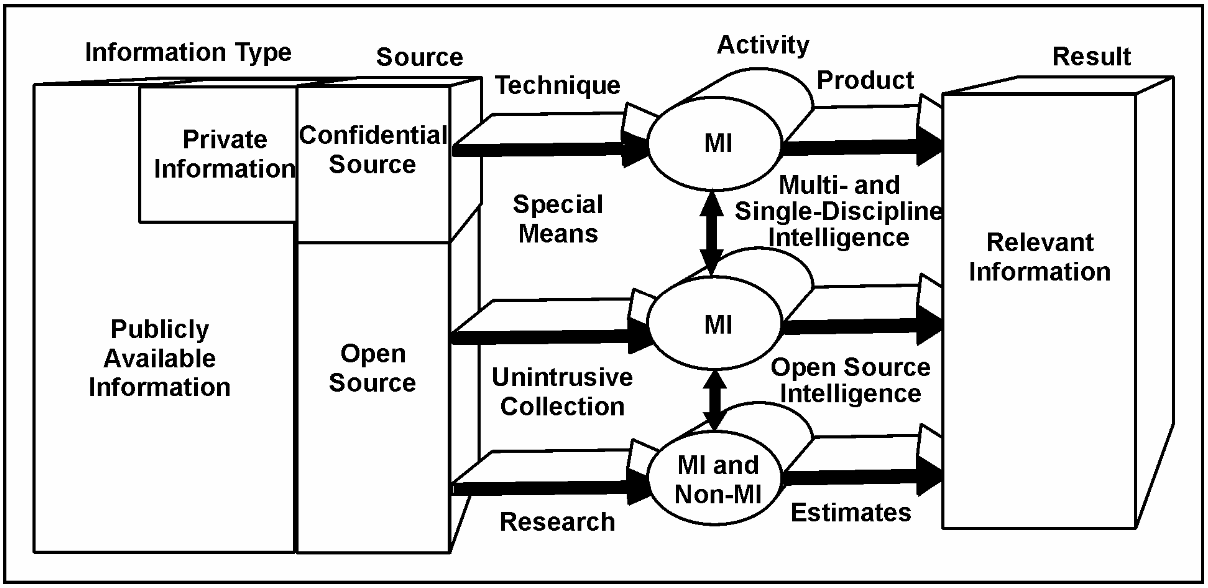


Figure 2-1. Relationship of publicly available information to relevant information

CHARACTERISTICS OF OPEN SOURCE INTELLIGENCE

2-4. The following characteristics address the role of publicly available information and OSINT in Army operations.

- **Provides the Foundation.** Directly or indirectly, publicly available information forms the basis of intelligence and non-intelligence operations. The US social structures, education system, news services, and entertainment industry shape our World view, awareness of international events, and perceptions of non-US societies.
- **Answers Requirements.** The availability, depth, and range of public information enable intelligence and non-intelligence organizations to satisfy many of the commander's critical information requirements (CCIRs) and their own information needs without the use of specialized human or technical means of collection (see Figure 2-1). Given the volume, scope, and quality of publicly available information, OSINT operations can often proceed directly from the planning phase to the production phase of the intelligence process.
- **Enhances Collection.** Open source research and collection support other surveillance and reconnaissance activities by answering requirements and providing foundational information (biographies, cultural information, geospatial information, technical data) that optimizes the employment and performance of sensitive human and technical means of collection.
- **Enhances Production.** As part of single and multidiscipline intelligence production, the use and integration of publicly available information and OSINT ensures decisionmakers have the benefit of all-sources of available information.

OPEN SOURCES AND INFORMATION

2-5. Open sources and publicly available information may include but are not limited to—

- **Academia.** Courseware, dissertations, lectures, presentations, research papers, and studies in both hardcopy and softcopy on economics, geography (physical, cultural, and political-military), international relations, regional security, science, and technology.
- **Governmental, Intergovernmental, and Nongovernmental Organizations (NGOs)**. Databases, posted information, and printed reports on a wide variety of economic, environmental, geographic, humanitarian, security, science, and technology issues.
- **Commercial and Public Information Services.** Broadcasted, posted, and printed news on current international, regional, and local topics.
- **Libraries and Research Centers.** Printed documents and digital databases on a range of topics as well as knowledge and skills in information retrieval.
- **Individuals and Groups.** Handwritten, painted, posted, printed, and broadcasted information (for example, art, graffiti, leaflets, posters, and websites).

OPEN SOURCE MEDIA

2-6. A simple communications model consists of a sender, a message, a medium, and a receiver. The medium is the access point to publicly available information for open source research and collection. The primary media that open sources use to communicate information to the general public are shown in Table 2-1 and discussed below.

Table 2-1. Primary open source media

SYSTEM	COMPONENTS	ELEMENTS
PUBLIC SPEAKING	SPEAKER	• Sponsor • Relationship • Message
	FORMAT	• Conference • Debate • Demonstration • Lecture • Rally
	AUDIENCE	• Location • Composition
PUBLIC DOCUMENTS	GRAPHIC	• Drawing • Engraving • Painting • Photograph • Print
	RECORDED	• Compact Data Storage Device • Digital Video Disk • Hard Disk • Tape

Table 2-1. Public speaking forums (continued)

	PRINTED	• Book • Brochure • Newspaper • Periodical • Pamphlet • Report
PUBLIC BROADCASTS	RADIO	• Low Frequency AM Radio • Medium Frequency AM Radio • VHF FM Radio • L- and S-Band Satellite Radio
	TELEVISION	• Ku Band Satellite Television VHF and UHF Terrestrial Television
INTERNET SITES	COMMUNICATIONS	• Chat • Email • News • Newsgroup • Webcam • Webcast • Weblog
	DATABASES	• Commerce • Education • Government • Military • Organizations
	INFORMATION (WEBPAGE CONTENT)	• Commerce • Education • Government • Military Organizations
	SERVICES	• Dictionary • Directory • Downloads • Financial • Geospatial • Search • Technical Support • Translation • URL Lookup

PUBLIC SPEAKING FORUMS

2-7. Public speaking, the oldest medium, is the oral distribution of information to audiences during events that are open to the public or occur in public areas. These events or forums include but are not limited to academic debates, educational lectures, news conferences, political rallies, public government meetings, religious sermons, and S&T exhibitions. Neither the speaker nor the audience has the expectation of privacy when participating in a public speaking forum unless there is an expressed condition of privacy such as the Chatham House Rule. If invoked, privacy conditions such as the Chatham House Rule change the characterization of the source from an open to a confidential source and may necessitate treating the source and collected information in accordance with human intelligence (HUMINT) or counterintelligence (CI) procedures. Unlike the other open source collection, monitoring public speaking events is done through direct observation and, due to its overt nature, could entail risk to the collector.

PUBLIC DOCUMENTS

2-8. A document is any recorded information regardless of its physical form or characteristics. Like public speaking, public documents have always been a source of intelligence. Documents provide in-depth information about the operational environment that underpin our ability to plan, prepare for, and execute military operations. During operations, documents such as newspapers and magazines provide insights into the effectiveness of information operations. Books, leaflets, magazines, maps, manuals, marketing brochures, newspapers, photographs, public property records, and other forms of recorded information continue to yield information of intelligence value about operational environments. Sustained document collection contributes to the development of studies about potential operational environments. Collection of documents on the operational and technical characteristics of foreign materiel aid in the development of improved US tactics, countermeasures, and equipment.

PUBLIC BROADCASTS

2-9. A public broadcast entails the simultaneous transmission of data or information for general public consumption to all receivers or terminals within a computer, radio, or television network. Public broadcasts are important sources of current information about the operational environment. Television news broadcasts often provide the first indications and warning (I&W) of situations that may require the use of US forces. Broadcast news and announcements enable personnel to monitor conditions and take appropriate action when conditions change within the area of operations (AO). News, commentary, and analysis on radio and television also provide windows into how governments, civilians, news organizations, and other elements of society perceive the US and US military operations. Broadcasts also provide information and insights into the effectiveness of information operations.

INTERNET SITES

2-10. Army intelligence components must use Government computers to access the Internet for official Government business unless otherwise authorized (for example, an Army Reservist participating in the World Basic Information Library [WBIL] program).

2-11. Internet sites enable users to participate in a publicly accessible communications network that connects computers, computer networks, and organizational computer facilities around the world. The Internet is more then just a research tool. It is a reconnaissance and surveillance tool that enables intelligence personnel to locate and observe open sources of information. Through the Internet, trained collectors can detect and monitor Internet sites that may provide I&W of enemy intentions, capabilities, and activities.

2-12. Collectors can monitor newspaper, radio, and television websites that support assessments of information operations. Collectors can conduct periodic searches of webpages and databases for content on military order of battle (OB), personalities, and equipment. Collecting webpage content and links can provide useful information about relationships between individuals and organizations. Properly focused, collecting and processing publicly available information from Internet sites can support understanding of the operational environment.

OPEN SOURCE INTELLIGENCE ORGANIZATIONS

2-13. The Army does not have a specific military occupational specialty (MOS), additional skill identifier (ASI), or special qualification identifier (SQI) for OSINT. With the exception of the Asian Studies Detachment (see Appendix A), the Army does not have base tables of organization and equipment (TOE) for OSINT units or staff elements. OSINT missions and tasks are imbedded within existing missions and force structure or accomplished through task organization.

2-14. The nexus of Army OSINT operations is the theater military intelligence (MI) brigade or group. Each of these INSCOM units conducts sustained, regionally focused intelligence operations in support of their Army Service Component Command (ASCC) and Combatant Command (COCOM) (Figure 2-2). While their OSINT capabilities may vary, each of these theater-level MI units is the focal point within the COCOM for managing Army open source requirements and providing OSINT support to Army tactical units deploying to or operating within the command's area of responsibility (AOR). When open source skills and regional knowledge are not present in these deploying tactical units, personnel from the theater MI brigade or group may deploy with and form the core of the tactical unit's OSINT organization as well as provide the control mechanism for synchronization and information exchange between echelons.

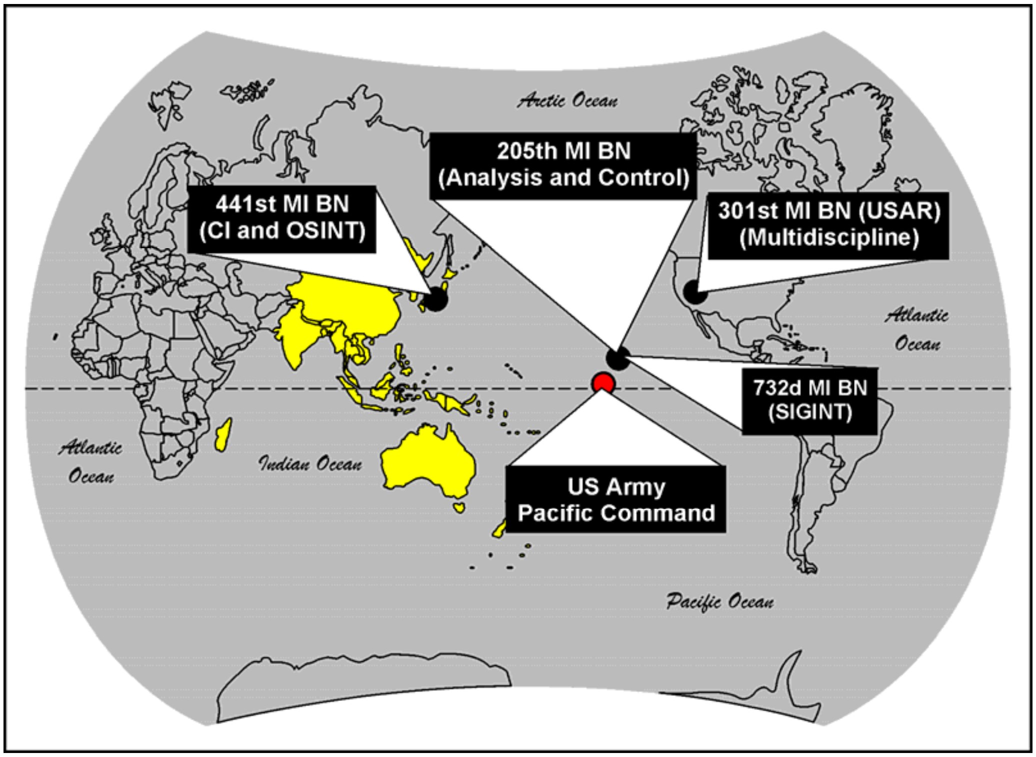


Figure 2-2. Example - 500th Military Intelligence Brigade in US Army Pacific Command

2-15. When task organizing for OSINT operations, intelligence units use the following basic types of organizations or personnel as the basis for organizing and accomplishing open source missions.

- **Command and Control.** Command and control (C2) organizations and personnel provide management and oversight of subordinate production, collection, and processing elements. They are knowledgeable about open source organizations and open source requirements management. They have the skills and knowledge necessary to synchronize collection and production within their organization and between echelons. They understand the open source collection and processing capabilities of intelligence and non-intelligence units within the supported command. These personnel may have additional authority and training in contracting for products and services when commercial vendors provide open source products and services.
- **Collection.** Collection organizations and personnel gather and report publicly available information in accordance with tasking from their C2 organization. They have skills and knowledge in one or more of the open source collection techniques. Depending upon the organization and mission, these personnel may also be regional or subject matter experts with in-depth knowledge of the operational environment and local language. These expert personnel are often capable and responsible for multiple tasks (collection, processing, and production) in their areas of expertise.
- **Processing.** Processing organizations and personnel transform collected data into a form suitable for analysis and intelligence production. Some have the skills and knowledge to quality control the processing and reporting of the information. Processing personnel may have specialized skills and knowledge in areas such as document exploitation (DOCEX), transcription, and translation. Sensitive processing techniques such as imagery interpretation and cryptography are the responsibility of imagery intelligence (IMINT) and signals intelligence (SIGINT) organizations, respectively.
- **Production.** Production organizations and personnel convert information into intelligence. They have skills and knowledge in open source research, intelligence production, and dissemination. Analysts with production organizations use a number of techniques and tools to retrieve, integrate, evaluate, analyze, and interpret information into OSINT or multidiscipline intelligence. They disseminate the results of intelligence production to the users as assessments, studies, estimates, and reports. They also store the products and the supporting research material and metadata in databases accessible to other personnel who manage intelligence operations; collect and process information; produce intelligence; or use publicly available information and OSINT.

OPEN SOURCE INTELLIGENCE CONSIDERATIONS

2-16. For the most part, the considerations for OSINT are similar to those of other intelligence disciplines.

- OSINT organizations need clearly stated intelligence requirements to effectively focus collection and production.
- OSINT operations must comply with AR 381-10 and Executive Order 12333 on the collection, retention, and dissemination information on US persons (see Appendix B and Appendix C).
- OSINT organizations can be overwhelmed by the volume of information to process and analyze.
- OSINT operations require qualified linguists for foreign language-dependent collection and processing tasks.

2-17. In addition to the above, personnel responsible for planning or executing OSINT operations must consider the following:

COMPLIANCE

2-18. Under AR 381-10, Procedure 2, Army intelligence activities may collect publicly available information on US persons only when it is necessary to fulfill an assigned function. There must also be a link between the collection of the US person information and the Army intelligence component's assigned mission. Army intelligence components must exhaust the least intrusive collection means before requesting a more intrusive collection means. The following are additional considerations for Internet collection:

- Army intelligence components must use Government computers to access the Internet for official Government business unless otherwise authorized.
- Internet protocol (IP) addresses, uniform resource locators (URLs), and email addresses that are not self-evidently associated with a US person may be acquired, retained, and processed by Army intelligence components without making an effort to determine whether they are associated with a US person as long as the component does not engage in analysis focused upon specific addresses. Once such analysis is initiated, the Army intelligence component must make a reasonable and diligent inquiry to determine whether the data are associated with a US person.

LIMITATIONS

2-19. Intelligence organizations whose principle missions are CI, HUMINT, and SIGINT must comply with applicable Department of Defense Directives and Army Regulations that govern contact with and collection of information from open sources. For example, DOD Directive 5100.20 prohibits SIGINT organizations from collecting and processing information from public broadcasts with exception of processing encrypted or "hidden meaning" passages. AR 380-13 prohibits the assignment of Army personnel, military or civilian, to attend public or private meetings, demonstrations, or other similar activities held off-post to acquire CI investigative information without specific approval by the Secretary or the Under Secretary of the Army.

OPERATIONS SECURITY

2-20. More than any other intelligence discipline, the OSINT discipline could unintentionally provide indicators of US military operations. Information generally available to the public as well as certain detectable activities such as open source research and collection can reveal the existence of, and sometimes details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit US military operations. Purchasing documents, searching an Internet site, or asking questions at public events are examples of detectable open source research and collection techniques that could provide indicators of US plans and operations.

2-21. Using the five-step operations security (OPSEC) process, organizations must determine what level of contact with open sources and which collection techniques might provide indicators that an enemy could piece together in time to affect US military operations. In OSINT operations, countermeasures range from limiting the frequency or duration of contact with a source to prohibiting all contact with a source. If OPSEC so requires, such as to protect a Government computer from hacker retaliation, a major Army command (MACOM) commander may approve nonattributable Internet access.

CLASSIFICATION

2-22. AR 380-5 states that intelligence producers "must be wary of applying so much security that they are unable to provide a useful product to their consumers." This is an appropriate warning for OSINT operations where concern for OPSEC can undermine the ability to disseminate inherently unclassified information. As shown in Table 2-2, the classification of source metadata, collector metadata, collected information, and derivative intelligence differ based the means of collection and the degree of damage disclosure of this information could reasonably be expected to cause to national security.

2-23. Since it is already in the public domain, publicly available information and the source metadata are unclassified. AR 380-5, Chapter 4, directs that Army personnel will not apply classification or other security markings "to an article or portion of an article that has appeared in a newspaper, magazine, or other public medium." For reasons of OPSEC, the classification of collector information is controlled unclassified or classified information. According to AR 380-5, Chapter 2, a compilation of unclassified publicly available information into an intelligence product (estimate, report, or summary) is normally not classified. In unusual circumstances, the combination of individual unclassified items of information into an intelligence product may require classification if the compilation provides an added factor that warrants classification.

Table 2-2. Open source intelligence classification considerations

IF		THEN			
Information Source	Collection Means	Source Metadata	Collector Metadata	Collected Information	Intelligence Report
Confidential	Overt	Classified or Controlled Unclassified	Classified or Controlled Unclassified	Classified or Controlled Unclassified Information	Classified or Controlled Unclassified
	Clandestine	Classified	Classified		
Open	Overt	Unclassified	Controlled Unclassified	Unclassified	Classified, Controlled Unclassified, or Unclassified
	Nonattributable		Classified or Controlled Unclassified		
NOTE: this table is prescriptive not directive. Organizations with original classification authority or personnel with derivative classification responsibilities must provide subordinate organizations and personnel with a security classification guide or guidance for information and intelligence derived from open sources in accordance with the policy and procedures in AR 380-5.					

2-24. AR 380-5, Chapter 6, provides a list of factors or classification considerations which includes but is not limited to the following:

- Intelligence that reveals the identity of a conventional source or method normally does not require classification.
- Intelligence identifying a sensitive source or method is classified, as well as the evaluation of the particular source or method.
- An intelligence requirement is classified when it reveals what is not known, what is necessary to know, and why.

Note: Collection managers create sanitized, unclassified collection tasks from the intelligence requirement since uncleared US and non-US persons make up a significant portion of open source collectors.

- Information that would divulge intelligence interests, value, or extent of knowledge on a subject.
- Information related to political or economic instabilities in a foreign country threatening American lives and installation there.

DECONFLICTION

2-25. During planning, the G2/S2 staff and the G3/S3 staff must deconflict OSINT operations with other activities. Specifically, contact or interaction with open sources may compromise the operations of another intelligence discipline. Open source collection may adversely affect the ability of non-intelligence organizations such as civil affairs (CA), military police (MP), medical, and public affairs (PA) to accomplish their missions. Conversely, overt contact with a source by CA, MP, or other personnel may compromise OSINT operations as well as the safety of the open source or collector. Each of these situations could lead to the loss of access to the open source and information of intelligence value.

DECEPTION AND BIAS

2-26. Deception and bias are of particular concern in OSINT operations. Unlike other disciplines, OSINT operations do not normally collect information by direct observation of activities and conditions within the area of interest (AOI). OSINT operations rely on secondary sources to collect and distribute information that the sources may not have observed themselves. Secondary sources such as government press offices, commercial news organizations, NGO spokespersons, and other information providers can intentionally or unintentionally add, delete, modify, or otherwise filter the information they make available to the general public. These sources may also convey one message in English for US or international consumption and a different non-English message for local or regional consumption. It is important to know the background of open sources and the purpose of the public information in order to distinguish objective, factual information from information that lacks merit, contains bias, or is part of an effort to deceive the reader.

INTELLECTUAL PROPERTY

2-27. AR 27-60 prescribes policy and procedures for the acquisition, protection, transfer and use of patents, copyrights, trademarks, and other intellectual property by the Department of the Army (DA). It is Army policy to recognize the rights of copyright owners consistent with the Army's unique mission and worldwide commitments. As a general rule, Army organizations will not reproduce or distributed copyrighted works without the permission of the copyright owner unless such use is within an exception under US Copyright Law or required to meet an immediate, mission-essential need for which noninfringing alternatives are either unavailable or unsatisfactory.

2-28. According to the US Copyright Office, "fair use" of a copyrighted work for purposes such as criticism, comment, news reporting, teaching, scholarship, or research, is not an infringement of copyright. Implicit with fair use is the documentation and citation of the source of the copyrighted information. The following are four factors in determining fair use:

- Purpose and character of the use. In the context of fair use, intelligence operations are similar in purpose and usage to non-profit news reporting and research organizations.
- Nature of the copyrighted work (see Appendix D).
- Amount and substantiality of the portion used in relation to the copyrighted work as a whole. There is no specific number of words, lines, or notes that may safely be taken without permission. Usually, the amount or portion of copyrighted material is limited to quotations of excerpts and short passages; and summary of a speech or article, with brief quotations.
- Effect of the use upon the potential market for or value of the copyrighted work. The effect on the market or value of copyrighted material relates to reproduction and dissemination of products provided by the owner beyond that authorized the owner's "Terms of Use" or described in contracts and licenses with the US Government.

Chapter 3

Plan and Prepare for Operations

3-1. Like all Army intelligence operations, OSINT operations follow the Army intelligence process described in FM 2-0. The intelligence process enables the systematic execution of Army OSINT operations as well as their integration with Joint, Interagency, and Multinational intelligence operations. As shown in Figure 3-1, the major functions (plan, prepare, collect, process, and produce) of the intelligence process also align with the major functions of the Army's operations process (plan, prepare, execute, and assess) described in FM 3-0. The synchronization and integration of intelligence with operations ensures the delivery of relevant information that facilitates situational understanding and decisionmaking.

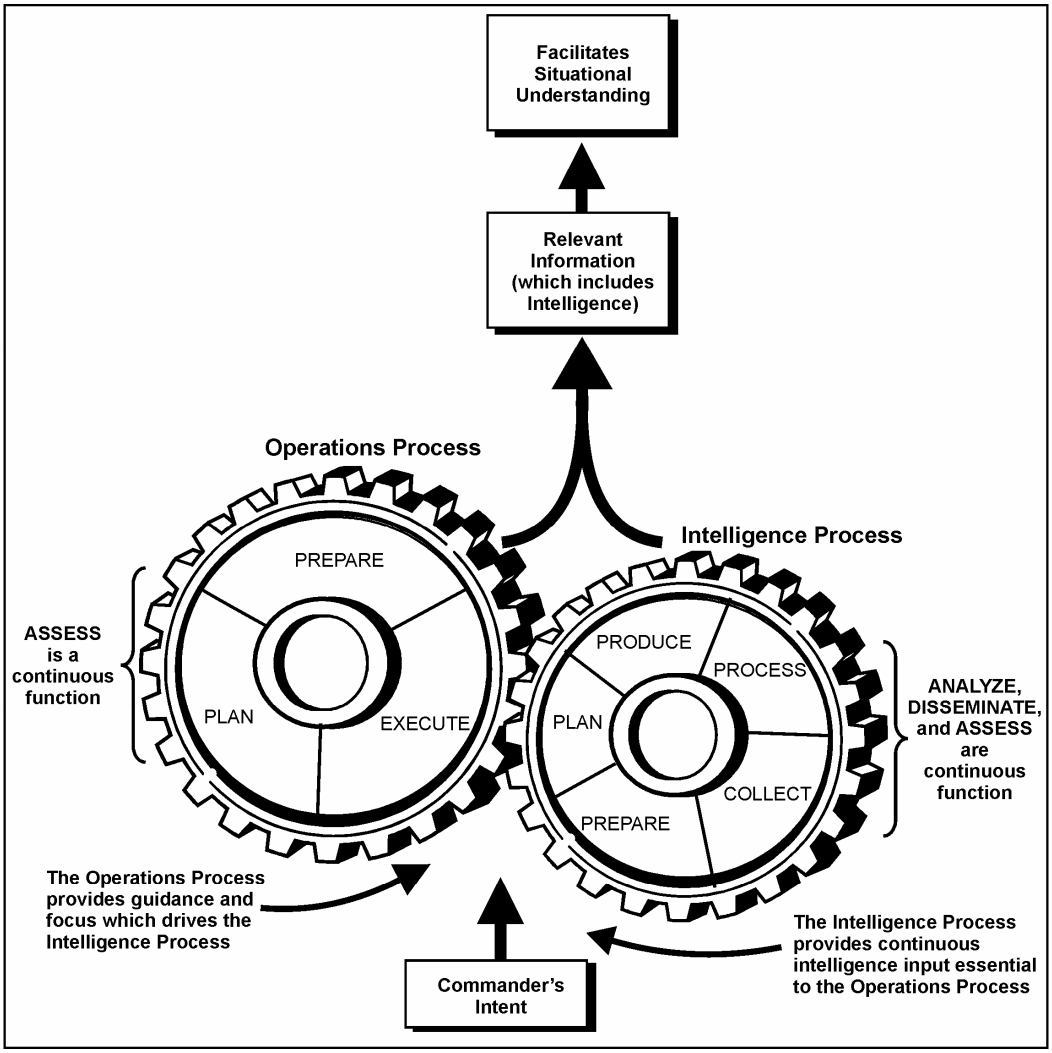

Facilitates Situational Understanding
Relevant Information (which includes Intelligence)
Operations Process
Intelligence Process
PREPARE
PLAN
EXECUTE
ASSESS is a continuous function
PRODUCE
PROCESS
PLAN
COLLECT
PREPARE
ANALYZE, DISSEMINATE, and ASSESS are continuous function
The Operations Process provides guidance and focus which drives the Intelligence Process
The Intelligence Process provides continuous intelligence input essential to the Operations Process
Commander's Intent

Figure 3-1. Operations and intelligence

PLAN OPERATIONS

3-2. OSINT operations begin weeks, months, or years before a corps, division, or brigade receives a warning order (WARNO) for deployment. OSINT plays a critical role in understanding diverse operational environments and building the knowledge required for unit readiness and effective planning. Sustained and proactive overt open source research by intelligence and non-intelligence personnel provides relevant information that enhances understanding of the operational environment and its critical variables that leaders and their subordinates need to effectively plan, prepare for, and execute military operations. In a practical sense, research is the foundation of successful intelligence operations and their support to military operations. Open source research provides much of the information on current and potential operational environments that enables effective planning, preparation for, and execution of military operations.

3-3. OSINT also supports the continuous assessment of military operations. Research during orientation and contingency planning provides insights into how foreign military forces and transnational threats have operated in similar operational environments. During operations, collection and analysis of publicly available information on the enemy's objectives and adaptation in response to US operations aids in the development of improved training, tactics, and materiel. Following operations, research of enemy operations and foreign observations of US operations supports the assessment and the improvement of Army force structure, materiel, training, and TTP.

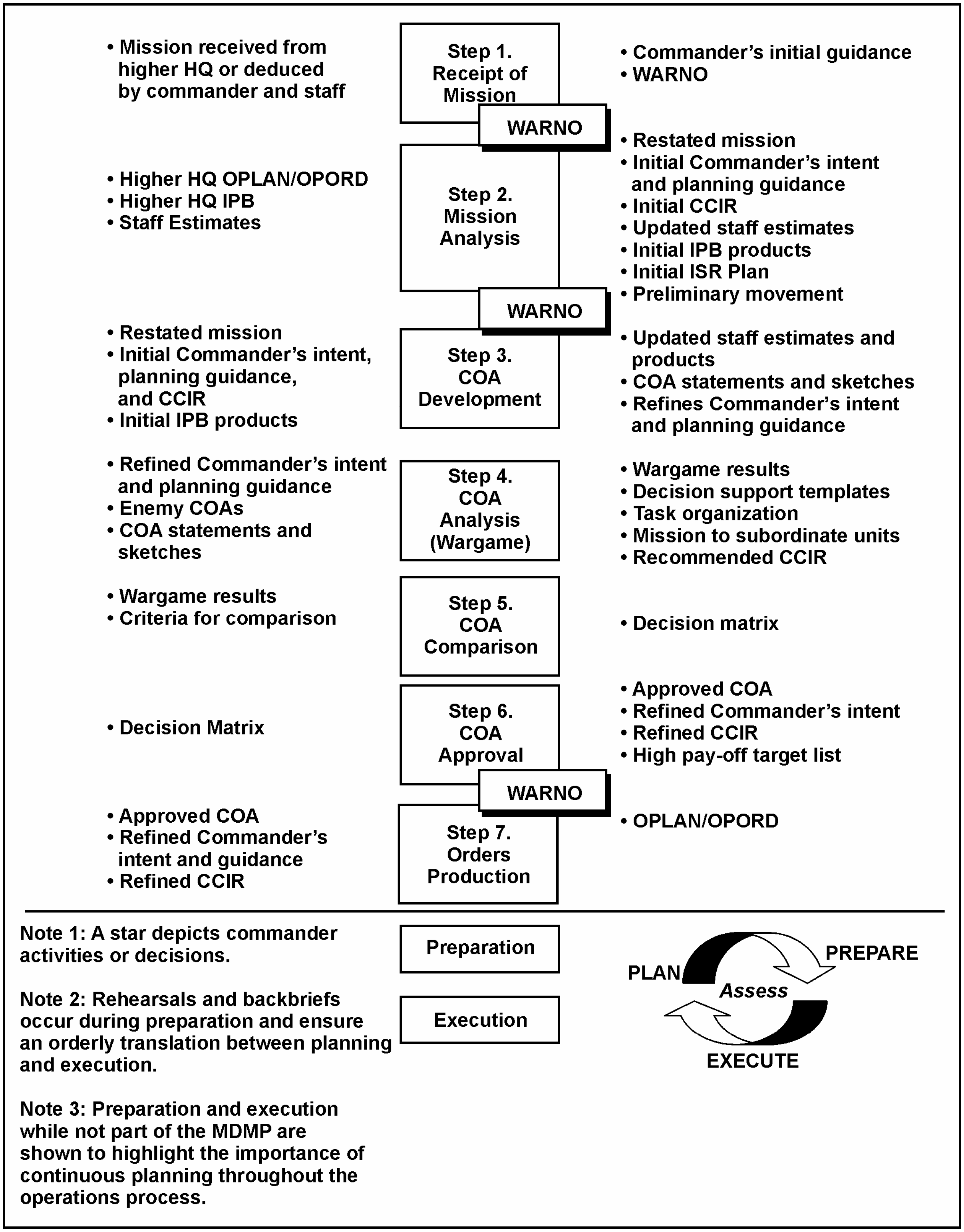
DEVELOP SPECIFIC INFORMATION REQUIREMENTS

3-4. Upon receipt of mission, the commander and staff take the steps necessary to begin the military decisionmaking process (MDMP) (Figure 3-2). These include gathering tools, updating estimates, and performing an initial assessment. This assessment includes determining the time available for planning. In mission analysis, the commander and staff analyze the relationships among the factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). They seek to understand—

- The operational environment, including adversaries, terrain, and civil considerations.
- The desired end state of their higher and next higher headquarters.
- Their mission and how it is nested with those of their higher and next higher headquarters.
- The forces, capabilities, and resources available.

3-5. Following mission analysis, commanders issue their initial intent and planning guidance. These are based on their commander's visualization. The initial commander's intent focuses the rest of the planning process. They describe how the commander envisions the operation's end state and conditions necessary to achieve it. Thinking in terms of desired and undesired effects is useful for commanders developing and issuing planning guidance. It also helps staff members develop courses of action (COAs).

3-6. During planning, intelligence personnel analyze the commander's priority intelligence requirements and information requirements (IRs) of the coordinating and special staff to create specific information requirements (SIRs). SIRs describe what information the analyst requires to answer each intelligence requirement, where the information may be found, and when to collect the information. Each SIR contains indicators that, if observed, provide information on the characteristics of or activities within the AOI. These indicators when linked to a specific location, event, or time form the basis of research, tasks for collection, and requests for information (RFIs).


• Mission received from higher HQ or deduced by commander and staff
Step 1. Receipt of Mission
• Commander's initial guidance
• WARNO
WARNO
• Higher HQ OPLAN/OPORD
• Higher HQ IPB
• Staff Estimates
Step 2. Mission Analysis
• Restated mission
• Initial Commander's intent and planning guidance
• Initial CCIR
• Updated staff estimates
• Initial IPB products
• Initial ISR Plan
• Preliminary movement
WARNO
• Restated mission
• Initial Commander's intent, planning guidance, and CCIR
• Initial IPB products
Step 3. COA Development
• Updated staff estimates and products
• COA statements and sketches
• Refines Commander's intent and planning guidance
• Refined Commander's intent and planning guidance
• Enemy COAs
• COA statements and sketches
Step 4. COA Analysis (Wargame)
• Wargame results
• Decision support templates
• Task organization
• Mission to subordinate units
• Recommended CCIR
• Wargame results
• Criteria for comparison
Step 5. COA Comparison
• Decision matrix
• Decision Matrix
Step 6. COA Approval
• Approved COA
• Refined Commander's intent
• Refined CCIR
• High pay-off target list
WARNO
• Approved COA
• Refined Commander's intent and guidance
• Refined CCIR
Step 7. Orders Production
• OPLAN/OPORD
Preparation
Execution
PLAN
PREPARE
Assess
EXECUTE

Note 1: A star depicts commander activities or decisions.

Note 2: Rehearsals and backbriefs occur during preparation and ensure an orderly translation between planning and execution.

Note 3: Preparation and execution while not part of the MDMP are shown to highlight the importance of continuous planning throughout the operations process.

Figure 3-2. Military decisionmaking process

CONDUCT RESEARCH

3-7. Intelligence analysts attempt to answer the SIRs using existing information and intelligence acquired through open source research and searches of classified databases (Figure 3-3). Open source research is the most effective means of retrieving authoritative and detailed information on the terrain, weather, and civil considerations as well as external variables that affect or influence the operational environment. If the analyst can answer the requirement, he reports the information or intelligence to the originator immediately. When the analyst determines that the required information is not available, he uses the SIR to help the staff develop collection tasks and RFIs. The compilation of the unanswered SIR is the basis of the intelligence, surveillance, and reconnaissance (ISR) plan and subsequent tasks for collection and RFIs.

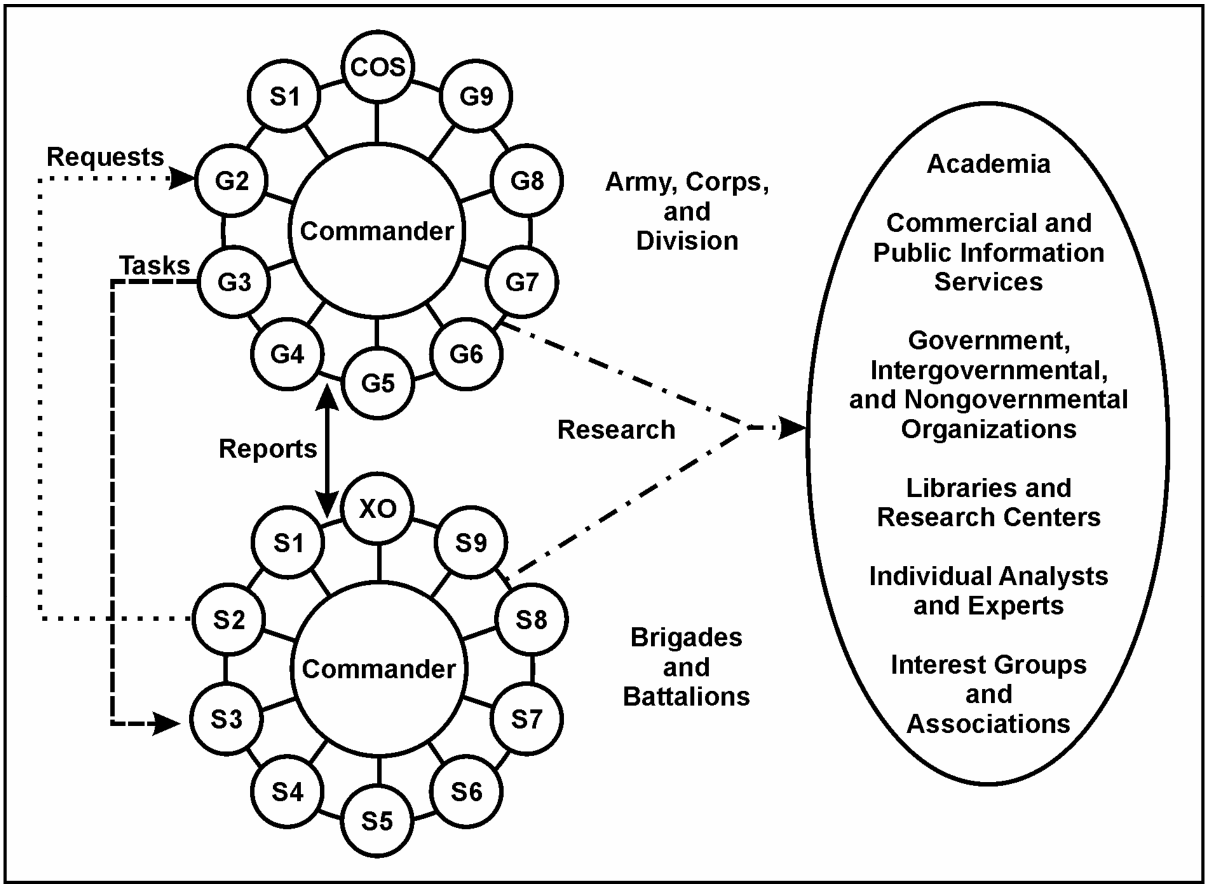

COS
S1
G9
Requests
G2
G8
Commander
Army, Corps, and Division
Tasks
G3
G7
G4
G5
G6
Research
Reports
XO
S1
S9
S2
S8
Commander
Brigades and Battalions
S3
S7
S4
S5
S6
Academia
Commercial and Public Information Services
Government, Intergovernmental, and Nongovernmental Organizations
Libraries and Research Centers
Individual Analysts and Experts
Interest Groups and Associations

Figure 3-3. Open source research, requests, tasks, and reports

3-8. Non-intelligence staff members also research publicly available information to prepare estimates, papers, briefings, plans, orders, and training material. They access, retrieve, analyze, and distribute publicly available information within the scope of their functional areas. Specifically, while the G2/S2 staff has overall staff responsibility for intelligence preparation of the battlefield (IPB), the subject matter experts for CA, engineer, fire support (FS), information operations (IO), law enforcement, logistics, terrain, and weather lay within the other staff elements. This ensures the commander and other staff elements receive timely and accurate information from the responsible and knowledgeable staff personnel. For example:

- **Information Operations.** The G7/S7 staff is responsible for assessing the information environment, describing the information environment's effects on operations, evaluating the threat's information situation, and determines threat COAs in the information environment that influence civil and military activities within the AO.
- **Civil-Military Operations**. The G9/S9 staff is responsible for assessing the civil considerations within the AO based on areas, structures, capabilities, organizations, people, and events.
- **Public Affairs.** The public affairs officer (PAO) is responsible for assessing public support within the AO and providing timely feedback on trends in public opinion based on media analysis, published polling data, and professional assessments.

TASK AND REQUEST

3-9. The G2/S2 and G3/S3 staffs use the commander's guidance and the PIRs to complete the ISR plan. The staffs use the plan to assign tasks to subordinate units or submit requests to supporting intelligence organizations that achieve the desired ISR objectives (Figure 3-4). Embodied in the ISR plan, these tasks describes how the unit will—

- Request collection, processing, and production support from Joint, Interagency, Multinational, and Service organizations such as the DNI Open Source Center (OSC) (see Appendix E), the NGIC, and the Marine Corps Intelligence Activity.
- Request and integrate collection, processing, and production capabilities from INSCOM and the US Military Intelligence Readiness Command.
- Task organize and deploy organic, attached, and contracted collection, processing, and production assets.
- Request and manage US and non-US linguists based on priority for support, mission-specific skills and knowledge requirements (language, dialect, and skill level), clearance level, and category. Chairman of the Joint Chiefs of Staff Instruction 3126.01 provides specific guidance on language and regional expertise planning.
- Conduct remoted, split-based, or distributed collection, processing, and production.

3-10. When developing ISR tasks for subordinate units, the G2/S2 and G3/S3 staffs use the task and purpose (what and why) construct for developing task statements. Each statement accounts for the following:

- Who is to execute the task (unit or organization).
- What the task is (an intended effect or an action by a friendly force).
- When the task will begin (by time or event) or the task's duration.
- Where the task will occur (AO, objective, grid coordinates).
- Why the force will perform the task (for what purpose or reason).

3-11. The who, where, and when of a task to a subordinate unit are straightforward. The what and why are more challenging to write clearly and can confuse subordinates if not written well. The what is a task expressed in terms of an intended effect or an action by a friendly force. The staff should carefully choose the term that best describes the commander's intended effect for the subordinate force. They should use doctrinally approved tasks and mission-task verbs. Doctrinally approved tasks have recognized meanings, are measurable, and describe results or effects. Using them simplifies orders.

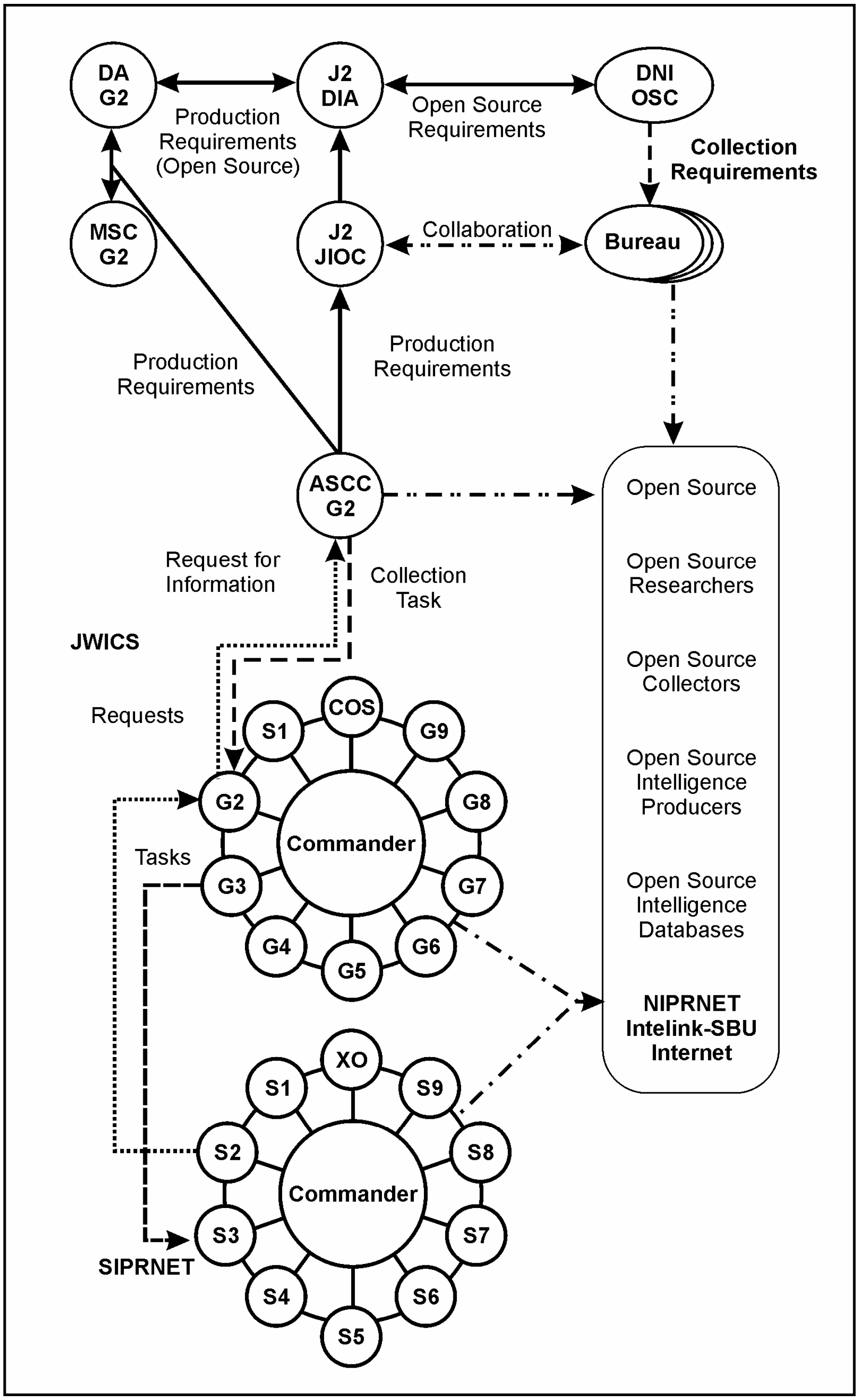


Figure 3-4. Example of open source intelligence information exchange

3-12. The why or purpose of a task statement is also extremely important to mission command and mission orders. The why puts the task into context by describing the reason for performing it. The purpose is normally stated as a descriptive phrase. Often, the purpose is more important than the task. Normally, the staff develops task statement by adding the phrase "in order to" and then provides the task's purpose. Task statements normally do not specify "how." There may be, however, occasions when commanders want to specify an activity (for example, CI, HUMINT, OSINT, aerial reconnaissance, SIGINT, ground surveillance) that provides an overarching doctrinal description of how to accomplish a task. The following are examples of task statements for open source collection tasks.

- No later than 280800Z July 2006, 513th MI Brigade establishes a theater-level broadcast information collection site at Forward Operating Base (FOB) BAYOU VERMILION to monitor regional and local broadcasts. Upon recognition, report indications and incidents of insurgent activity or civil unrest in the vicinity of named area of interest (NAI) ACADIA.
- No later than 192300Z October 2008, 2d Brigade Combat Team (BCT) establishes a document exploitation site at FOB PATHFINDER to collect and process local newspapers. Upon recognition, report indications of planned anti-Coalition rallies in the vicinity of Checkpoint CAPTION.
- 301st MI Battalion monitors the non-English websites and webcasts of international and regional news organizations covering Operation VIGILANT WARRIOR from D-30 to D+5. Provide a daily summary and assessment of news media coverage of US and non-US preparations for Operation VIGILANT WARRIOR. Report each occurrence of news reports on the 39th BCT's deployments for Operation VIGILANT WARRIOR.

3-13. Non-intelligence personnel also collect information. Close cooperation between intelligence and non-intelligence organizations fosters an efficient and supportive environment for appraising all personnel about what and how to report information of potential operational or intelligence value. If not tasked directly, non-intelligence personnel and organizations remain responsible for reporting information of potential intelligence or operational value gathered in the course of executing their missions. Artillery, CA, infantry, MP, psychological operations (PSYOP), PA, Special Forces, supply, transportation, and other personnel observe their environment and gather information as an integral part of developing and maintaining the situational understanding required to accomplish their missions. These personnel use their organization's standard information management procedures, formats, and systems to report their observations to multiple users, including intelligence organizations, within the command.

3-14. Throughout planning, preparation for, and execution of operations, the G2/S2 and G3/S3 staffs use ISR management procedures to integrate and synchronize OSINT operations across echelons. The G2/S2 staff ensures open source collection, processing, and production resources are included in the intelligence synchronization matrix (ISM) and the communications architecture. The G2/S2 works closely with other staff elements to ensure the seamless exchange of OSINT and information gathered by non-intelligence units. The G2/S2's staff works with the OSC bureau, Joint Intelligence Operations Center (JIOC), and theater-level analysis and control element (ACE) to establish, manage, and deconflict open source collection, processing, and production requirements and activities.

PLANNING CONSIDERATION – PUBLIC SPEAKING FORUMS

3-15. Collecting information at public speaking forums requires close coordination to ensure the overt collection is integrated with the information operations plan, and is lawful and synchronized with HUMINT activities. The ISR plan should describe how the unit will—

- Coordinate with the G7/S7 staff, the G9/S9, the PAO, the staff judge advocate (SJA), and the S2X prior to surveillance of public speaking forums.
- Identify additional personnel and equipment to provide force protection (FP) for collection personnel.

- Deploy, operate, maintain, and recover or transfer audio and video surveillance equipment and associated communications and processing systems,
- Describe reporting procedures for organizations that observe public events incidental to the execution of their assigned missions (for example, CA attendance at a city council meeting, MP at a check point, and transportation personnel at a relief center).

3-16. In addition, the operations order (OPORD) should describes how the unit tasked with public speaking forum collection missions will request, allocate, and manage funds to—

- Purchase digital camera equipment.
- Purchase audio recording equipment.
- Purchase computer hardware to play audio and video material.
- Purchase computer hardware and software applications for data storage and computer security.

PLANNING CONSIDERATION – PUBLIC DOCUMENTS

3-17. Organizations within the AO conduct the majority of document collection missions. Once collected and digitized, documents move through the communications and processing architecture to organizations throughout the Intelligence Community that have resources (skills, knowledge, and equipment) to effectively process the information and produce intelligence. The ISR plan should describe how the unit will—

- Coordinate document collection, processing, and analysis activities with those of Joint, Interagency, and Multinational organizations.
- Deploy, operate, maintain, and recover or transfer hardcopy, analog, and digital media processing equipment and associated communications systems (for example, Deployable HARMONY DOCEX Suite).
- Subscribe to or contract for academic and commercial information services for OSINT collection, processing, and production.

3-18. In addition, the OPORD should describes how the unit tasked with document collection missions will request, allocate, and manage funds to—

- Contract for document collection and processing “clipping” services.
- Purchase books, dictionaries, images, maps, newspapers, and periodicals.
- Purchase recorded audio and video material.
- Purchase computer hardware to play audio and video material.
- Purchase computer hardware and software applications for data storage and computer security.
- Purchase digital cameras and scanning equipment and software if not already on hand.
- Purchase commercial data and databases.
- Subscribe to newspapers and periodicals.

PLANNING CONSIDERATION – PUBLIC BROADCASTS

3-19. The DNI OSC collects, processes, and reports international and regional broadcasts. This enables deployed organizations to use their resources to collect and process information from local broadcasts that are of interest to the command or only accessible from within the AO. The ISR plan should describe how the unit will—

- Coordinate broadcast collection, processing, and production activities with those of the OSC.
- Deploy, operate, maintain, and recover or transfer radio and television broadcast receiving, digital media storage, content processing, and communications systems.

- Use Internet collection and processing resources to collect the broadcast from webcasts on the radio and television station's Internet site.

3-20. In addition, the OPORD should describes how the unit tasked with public broadcast collection missions will request, allocate, and manage funds to—

- Purchase antenna and computer equipment to receive, record, and process broadcast information.
- Purchase receivers and computer equipment to receive and convert regional television broadcast formats to US video formats.
- Purchase machine translation services or software, if available, for the target language and dialects.
- Subscribe to satellite radio and television broadcast service providers, both regional and international.

PLANNING CONSIDERATION – INTERNET SITES

3-21. Echelon above corps (EAC) organizations such as the INSCOM's Asian Studies Detachment and the Joint Reserve Intelligence Center-Leavenworth conduct sustained Internet collection, processing, and intelligence production. This enables the deployed organizations to focus their resources on collecting information from public speaking forums, broadcasts, and documents that are only accessible from within the AO. The ISR plan should describe how the unit will—

- Coordinate Internet collection, processing, and analysis activities with those of Joint, Interagency, and Multinational organizations such as the OSC and the Joint Reserve Intelligence Centers.
- Deploy, operate, maintain, and recover or transfer computers and associated communications and data storage systems.
- Provide access to the Intelink-Sensitive But Unclassified (Intelink-SBU) network (see Appendix F) or approved commercial Internet service providers to support OSINT collection, processing, storage, and dissemination requirements (for example, collection, processing, and exchange of digitized text, graphics, and multimedia information via Nonsecure Internet Protocol Network (NIPRNET). This will be done in coordination with the G6/S6 or installation Director of Information Management (DOIM).
- Coordinate a list of authorized US Internet sites for general military use, US and non-US Internet sites authorized for open source research, and non-US Internet sites restricted to authorized intelligence or CI personnel.
- Conduct split-based or distributed Internet information collection and processing.
- Subscribe to or contract for academic and commercial information services for open source information collection, processing, and production.

3-22. In addition, the OPORD should describes how the unit tasked with Internet research or collection missions will request, allocate, and manage funds to—

- Purchase digitized documents, geospatial information, and other information from Internet sites.
- Purchase computer hardware and software applications for saving web content (and metadata), data storage, and computer security.
- Subscribe to academic and commercial online databases.
- Subscribe to online newspapers, periodicals, and references.
- Contract for Internet information collection and processing services.

PLANNING CONSIDERATION – LINGUISTS REQUIREMENTS

3-23. The ability to comprehend information and communicate in foreign languages is critical in OSINT. Language proficiency requirements are primarily in the areas of collection and processing, but other areas may also require foreign language skills and knowledge. Tasks that require or may require language proficiency are—

- **Collection**. Collection of information from broadcasts, documents, Internet sites, and public speaking forums requires language proficiency and target knowledge as well as skills and knowledge of specific collection techniques. The specific level of required listening, reading, and speaking proficiency depends on the medium and the content.
- **Transcription.** Both listening and writing proficiency in the source language are essential for an accurate transcript. A transcript is extremely important when the English language skills of the processing personnel are inadequate for authoritative, direct translation from audio or video into English text.
- **Translation**. Bilingual competence is a prerequisite for creating any translation. The linguist must be able to read and comprehend the source language, write comprehensibly in English, and choose the equivalent expression in English that both fully conveys and best matches the meaning intended in the source language.
- **Research and Analysis**. Reading comprehension in the source language is essential for personnel conducting open source research or analysis in the target language. Listening and speaking proficiency may also be necessary if the analyst interacts with non-English speaking collection and processing personnel.
- **Tasking and Reporting**. If the collector's native language is not English then US personnel must give tasking and receive reports in the collector's native language or the collector must have some level of English language proficiency in listening, reading, speaking, and writing in order to receive tasking and report collected information in English.

3-24. During collection, intelligence personnel detect, identify, locate, and monitor communications modes that distribute public information. These modes include broadcasts, documents, Internet sites, and public speaking forums. Collecting and processing information from these modes requires language proficiency and target knowledge as well as skills and knowledge of specific collection techniques. On the Interagency Language Roundtable scale of 0 to 5, the language proficiency required for open source collection and processing ranges from a Level 2+ (Limited Working Proficiency, Plus) to a Level 5 (Functionally Native Proficiency). The specific level of required listening, reading, speaking, translation, and writing proficiency depends on the mode of communication and the content. If the linguist's native language is not English then Level 2+ or above English language proficiency in listening, reading, speaking, and writing is required if the individual receives tasking and reports collected or processed information in English. Table 3-1 summaries the language proficiency levels and Appendix G provides additional information on the Interagency Language Roundtable's language proficiency skill levels.

3-25. With some exceptions, a US Government Level 3 or above (General or Advanced Professional) linguists should review all information that US and non-US contract linguists transcribe and translate. This ensures US Government control and oversight of contractors as well as consistency with intelligence report formats and standards. Exceptions include operations involving long-term US multinational or coalition partners and US contractors with the requisite skills, performance history, and command confidence. In some cases, the Army will be challenged to find sufficient numbers of US Government linguists to review the translations. Also, there are instances where a native contract linguist's proficiency may far exceed the ability of the US Government linguist. Additionally, there may be languages for which there are no Army linguists (military or civilian). For example, Uighur, which is a language within the Turkic group of the Altaic language family, is spoken by 8.5 million people in Xinjiang Uighur Autonomous Region of China and 500,000 people in the Central Asian Republics of Kazakhstan, Kyrgyzstan, and Uzbekistan. Finally, if stated in the contract, when the contractor is contractually responsible for quality control and contract oversight.

Table 3-1. Interagency language roundtable proficiency levels

Base Level	**Proficiency** (Listening, Reading, Speaking, and Writing)	**Proficiency** (Translation)
0	None	No Proficiency
1	Elementary	Minimal
2	Limited Working	Limited
3	General Professional	Professional
4	Advanced professional	Professional
5	Functionally Native	Professional
Note: Each of the base levels implies control of any previous base level's functions and accuracy. A "plus level" designation is assigned when proficiency substantially exceeds one base skill level and does not fully meet the criteria for the next base level. The plus level descriptions are therefore supplementary to the base level descriptions.		

PREPARE FOR OPERATIONS

3-26. Once the G2/S2, G3/S3, and other responsible organizations have identified, validated, prioritized, and coordinated a collection requirement, the G3/S3 issues the orders to subordinate units to execute their assigned reconnaissance and surveillance missions. Normally this is done through an order or tasking message that contains information the tasked unit needs to execute the mission. It also contains the originator's identification so that the unit with the reconnaissance and surveillance mission can report directly to the originating unit. Reconnaissance and surveillance orders normally are included in paragraph three of the OPORD, as well as in Annex B (Intelligence), and Annex L (Reconnaissance and Surveillance). Tasking usually conforms to the principles of control in that a unit normally tasks one echelon down and tracks units two echelons down. The tasked unit makes the final choice of specific platforms, equipment, and personnel based on operational considerations such as personnel skills and knowledge, system range and survivability; and target characteristics.

3-27. Upon receipt of an order, C2 personnel of the tasked organization use troop leading procedures (TLPs) to evaluate the mission and make recommendations to the supported command on the employment the unit. Once the supported commander approves the ISR plan, the unit completes planning and prepares to execute its assigned missions. During planning and preparation, the unit's C2 personnel attempt to—

- Retain the flexibility to reallocate and reposition assets in response to changes in the mission, concept of operations, scheme of support, and threat.
- Streamline command, control, and communications (C3) between the unit and the supported command to increase responsive of tasking and timeliness of information reporting.
- Provide control teams or personnel that assist the unit in directing and assessing the operations of organic and attached assets.
- Establish logistics and security relationships to sustain and protect personnel and equipment operating beyond the range of unit's organic sustainment and FP capabilities.

ESTABLISH THE ARCHITECTURE

3-28. OSINT organizations can exchange publicly available information on unclassified networks between Army and Joint, Interagency, and Multinational organizations as well as with US federal, state, and local government agencies (see Figure 3-4). Classified networks enable connectivity to the DNI OSC, the JIOCs, the Joint Reserve Intelligence Centers, theater-level Army intelligence organizations, and other organizations that conduct OSINT operations or consume its products (Figures 3-5). The replication or mirroring of websites and databases from unclassified networks to classified networks ensures publicly available information and OSINT are available at the workstation of US, Allied, and Coalition personnel at multiple echelons and locations.

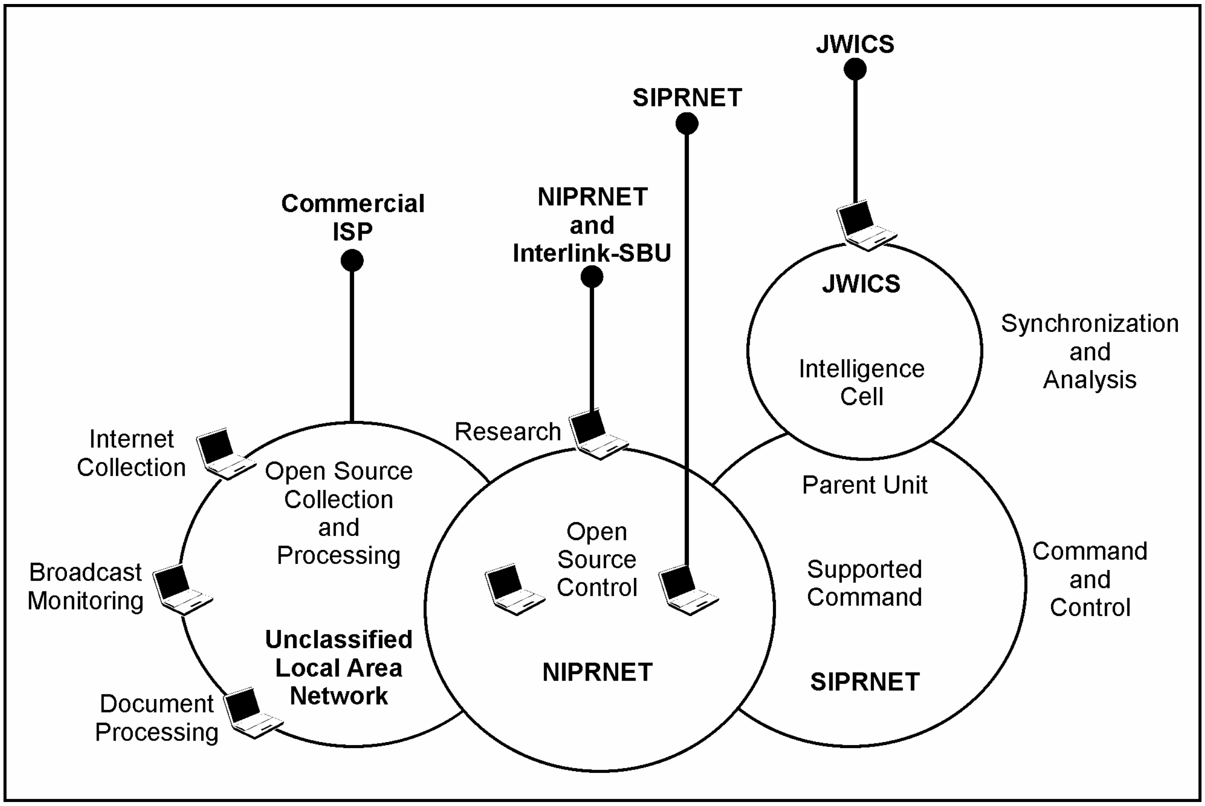


Figure 3-5. Networks supporting open source intelligence operations

3-29. The Joint Worldwide Intelligence Communications System (JWICS) supports the synchronization of OSINT operations, dissemination of OSINT and supporting metadata, and collaboration between deployed and supporting intelligence personnel (see Figures 3-4 and 3-5). The system provides the G2/S2 with a means to access OSINT services and products through the Intelink Central homepage. It allows authorized personnel to view, submit, and track intelligence requirements in the Department of Defense (DOD) requirements system.

3-30. The Secure Internet Protocol Router Network (SIPRNET) is the principal C2 data network at the tactical level (see Figures 3-4 and 3-5). This network provides the means to—

- Maintain situational awareness.

- Task or request open source collection and processing.
- Request OSINT.
- Report collected information and OSINT.
- Collaborate with collection and analysis personnel.
- Disseminate and retrieve documents to and from the HARMONY database.

3-31. The NIPRNET provides controlled access to the Internet. This network is the primary means to—

- Retrieve information from Army Knowledge Online (AKO) sites.
- Access the WBIL and other sites on the Intelink-SBU.
- Access the Intelink-SBU.
- Subscribe to approved nongovernmental and commercial information services or forums.

3-32. In addition to the standard networks, OSINT operations may require the use of special purpose communications networks like the TROJAN Data Network (TDN). TDN provides deployed units with access to sensitive compartmented information (SCI), collateral, and unclassified networks. The TDN also connects remotely operated receivers deployed in or near the AO to collection and processing resources located in the US or other sites outside the AO. This network and similar networks that support remote collection operations reduce the number of personnel and equipment deployed within the AO. These networks also enable Army organizations to leverage the collection and processing capabilities of Joint, Interagency, and Multinational organizations.

3-33. OSINT personnel use the results and by-products of their analysis to populate operational and technical databases. The technical database includes target folders containing a target description, target characteristics, rules of engagement, and reports. In the operational databases, they maintain the status of the collection and processing assets as well as a tracking system that correlates each target to associated tasks and RFIs. The following information describes types of internal databases that support OSINT operations—

- **Operational Information**. The operational information consists of orders, requests, and their status as well as the status of collection and processing resources. The database also has operational graphics and reports on the current situation and future operations within the AO. The operational information helps personnel correlate orders and requests to their associated collection missions and reports.
- **Technical Information.** The technical information consists of unprocessed text, audio, and video files; working and finished translations: and working and finished transcripts. The technical information includes the target folders containing target descriptions, target characteristics, and reports. Working aids, collection schedules, activity logs, and other information that supports collection operations are also part of the database.

3-34. OSINT operations require databases and Internet capabilities to facilitate processing, storage, retrieval, and exchange of information and intelligence. These databases are resident on local area networks (LANs) for internal operations and through Internet sites for information exchange with other intelligence activities and other users of OSINT. The following information describes three systems that support OSINT operations.

- **HARMONY**. HARMONY is the DOD's and the Intelligence Community's media exploitation database. HARMONY is the single, comprehensive bibliographic reference for all available primary source foreign technical and military documents and their translations. The HARMONY database is web-enabled and can be readily accessed, easily used, and responsive to the needs of analysts and other users within the US Government community. The HARMONY database application is supplemented by the Deployable HARMONY DOCEX System application, a field deployable front-end application that facilitates field collection and management of foreign documents.

- **Processing in a Collaborative Environment (PRINCE)**. The OSC's PRINCE system provides web interfaces that enable product creation, editing, and dissemination. Users can direct items for translation, editing, and dissemination from any point in the globe through their Internet access. PRINCE accommodates value-added products, such as open source analysis, in addition to translations. To ensure the broadest possible dissemination, open source products created in PRINCE or Opensource.gov are distributed to classified networks, including JWICS and SIPRNET, as well as customer platforms.
- **World Basic Information Library**. WBIL is a US Intelligence Community program that the US Army Training and Doctrine Command's (TRADOC's) Foreign Military Studies Office (FMSO) manages on behalf of the Community Open Source Program Office. Army Reserve and the Reserve personnel of other Services collect unclassified information from Internet sites then archive the collected information into the WBIL. The archived information on functional threat issues and countries answers basic and background information needs of the US Intelligence Community and operational units. Authorized personnel use the Pathfinder analytic tool suite to access the WBIL on the Intelink-SBU, the SIPRNET, or the JWICS.

TASK ORGANIZE ASSETS

3-35. As tactical units transition from combat to stability operations, they may task organize their organic and attached assets into temporary OSINT organizations to support new missions in a changed operational environment. Figure 3-6 is an example of a possible task organization for an open source analysis team at corps or division. The team leader and requirements managers ensure current intelligence, open source research, and target development analysts are responsive to the command's intelligence requirements. They also assist the G2 and G3 develop open source collection tasks and RFIs.

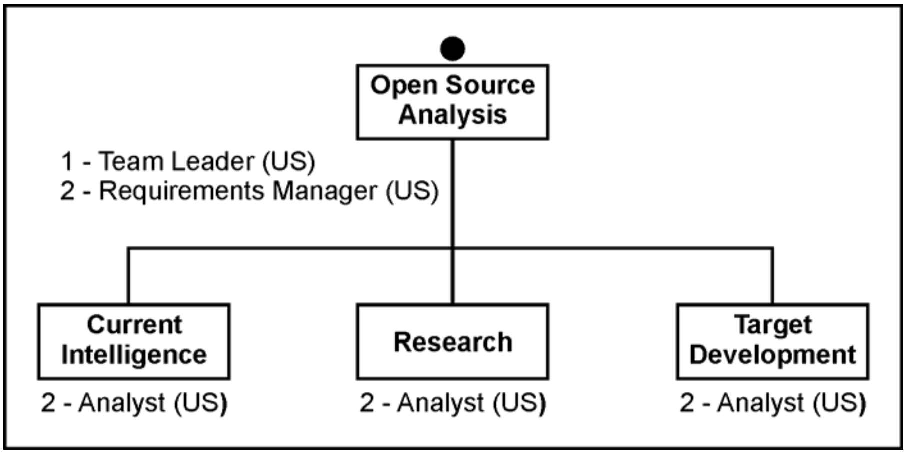


Figure 3-6. Possible open source analysis task organization

3-36. The current intelligence analysts monitor open source reporting and update their portions of the common operational picture (COP). The research analysts attempt to answer the command's intelligence requirements through search and retrieval of publicly available information and OSINT. These analysts also contribute contextual information to support current intelligence, background information to support planning, and detailed information to support target development. Target development analysts identify the components, elements, and characteristics of specific targets. Their analysis enables effects personnel to deliver and measure effectiveness of lethal and non-lethal effects. In addition, target development analysts identify civil considerations (for example, hospitals, religious centers, historical sites) within the operational environment that require protection.

3-37. Figure 3-7 is an example of one possible task organization of MI company assets into a cell or section to collect and process publicly available information within a BCT's AO. In this example, the OSINT cell or section is responsible for monitoring documents (leaflets, newspapers, and graffiti), public speaking events (protests, rallies, and sermons), and local radio (amplitude modulated). The brigade relies on the OSC and higher echelon Army organizations to monitor International and regional broadcasts as well as to collect information from Internet sites.

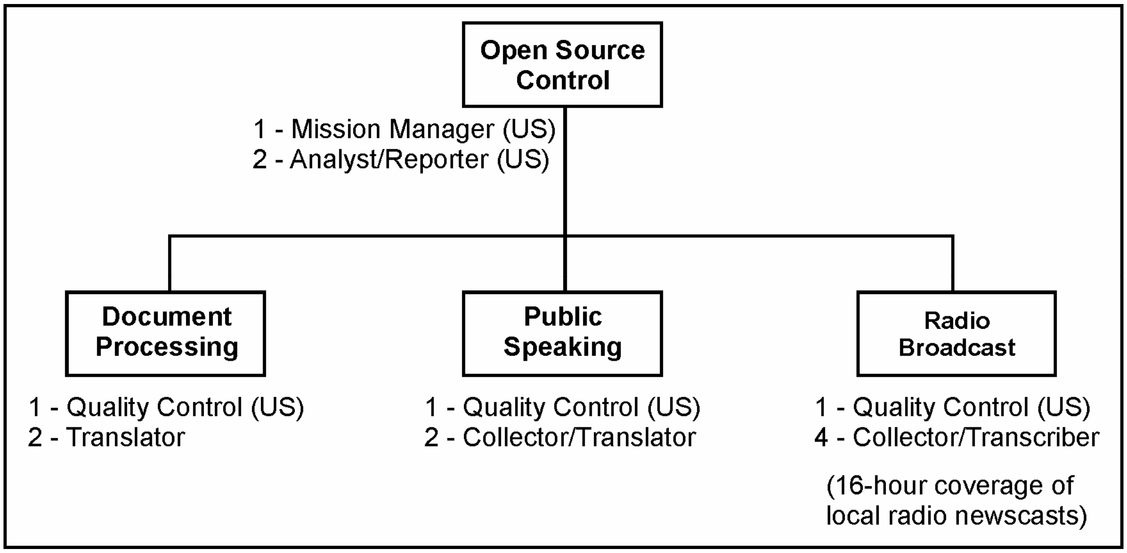


Figure 3-7. Possible open source collection and processing organization

3-38. The control team consists of US MI personnel who manage the three subordinate teams and report the collected information to the brigade's intelligence cell. The collection and processing personnel are a mixture of US and non-US contractor personnel. In each team, a US contractor linguist oversees operations and quality controls transcripts and translations. The number of collection and processing personnel varies based on the number of media being monitored; the number of targeted sources (programs, newspapers, and Internet sites); and required coverage (aperiodic, periodic, or fulltime).

DEPLOY ASSETS

3-39. Deployment of OSINT assets is consistent with unit standing operating procedures (SOPs), orders, and other considerations such as the tactical situation and the availability of transportation. The assets require a secure position with physical proximity to supporting sustainment, FP, and communications resources. They require, as a minimum, connectivity with C2 elements of their unit and supported command. Assets with contractor personnel may have additional FP, logistical, and security considerations that affect deployment of these personnel within the AO.

3-40. The unclassified nature of publicly available information enables open source collection and processing to operate outside classified workspaces. The unclassified open source workspace facilitates the organization of open source collection, processing, and production elements composed of uncleared personnel including non-intelligence military personnel, non-military personnel, and non-US persons. OSINT operations conducted outside sensitive compartment information facilities (SCIFs) support the formation and operations of Coalition Intelligence Centers and state-level Joint Operations Centers. The nature of publicly available information also enables the consolidation and centralized management of open source collection and processing personnel which support of CA, IO, MI, PA, PSYOP, and other users of public information.

ASSESS OPERATIONS

3-41. The G2/S2 and the G3/S3 assess OSINT operations to ensure they are satisfying the supported command's intelligence requirements. The following information describes the basic procedures to assess operations and ensure they are effectively supporting decisions and actions.

- **Monitor Operations.** Monitor the supported unit's operations to ensure responsiveness to the current situation and to anticipate future collection, processing, and reporting requirements. As required, the G2/S2 and G3/S3 prompt the collection, processing, and production personnel to keep their collection, processing, and reporting synchronized with the planning, preparation, and execution of the supported command's operations.
- **Correlate Reports.** Correlate the reports to the original intelligence requirement, collection task, or RFI. Correlation of the reports helps the G2/S2 and the G3/S3 to determine whether the reports satisfied the collection tasks and the RFIs.
- **Screen Reports.** Screen each report for timeliness, completeness, and relevance to the intelligence requirement, collection task, or RFI. If the report fulfills the information need, the G2/S2 and G3/S3 close the requirement and assign units or personnel to a new requirement or mission. A requirement remains active and unsatisfied if the intelligence report or collected information did not answer the intelligence requirement or provide the information specified in the task or request.
- **Cue Production and Collection.** Identify and notify other ISR resources to new information, analytic conclusion, and collection opportunities generated from the open source research, production, and collection. Effective cueing improves the overall ISR effort by keeping organizations abreast of the emerging information and opportunities as well as enabling the use of a multi-discipline approach to confirm or deny information by another information source, collection organization, or production activity.
- **Provide Feedback.** The G2/S2 and G3/S3 must update the supported command as well as production, collection, and processing personnel on the status of the intelligence requirements, collection task, or RFI. After screening the reports, they provide feedback to the production, collection, and processing personnel on what to sustain or adjust in their collection, processing, and reporting. For each adjustment, they work with the unit or personnel to identify the cause of the shortcomings and implement solutions that improve operational effectiveness. Solutions may require additional equipment or personnel, new or modified equipment, or changes to current ISR techniques.

Chapter 4

Produce Intelligence

4-1. Given the volume of existing publicly available information, intelligence analysts can often proceed directly from the planning phase to the production phase of the intelligence process. Intelligence analysts apply intelligence production techniques and procedures to retrieve or receive information, understand its meaning, and report relevant information in response to OSINT requirements. Through assessments, studies, and estimates, intelligence analysts present commanders and subordinates with descriptions and analysis of the operational environment. Effective research planning and production management ensures that commanders and their subordinates receive the timely, relevant, and accurate intelligence that they need to accomplish their assigned missions.

4-2. While relevant alone, OSINT is part of a larger multidiscipline intelligence effort. Personnel from other intelligence disciplines and multidiscipline intelligence activities use publicly available information and OSINT to update and expand upon their own research conducted during the planning and the preparation for operations. They use OSINT in the evaluation of the reliability and credibility of information from confidential sources. Multidiscipline intelligence personnel also integrate OSINT with reports from other intelligence disciplines to ensure their all-source, CI, or technical intelligence (TECHINT) reports are accurate, complete, and objective.

INTELLIGENCE CATEGORIES

4-3. Intelligence analysts follow the phases (integration, evaluation, analysis, and interpretation) of the intelligence production process to create OSINT. Although described sequentially, the following production phases may also take place concurrently. Using the process, analysts produce OSINT that falls into one or more of the five categories of intelligence. The categories relate to the purpose of the intelligence or the need of the user not specific to a specific intelligence. The categories can overlap, and the same intelligence report can support multiple categories. The following information describes each category:

- **Indications and Warnings.** I&W intelligence identifies hostile actions and provides sufficient warning to preempt, counter, or otherwise moderate their outcome. The I&W process depends upon continuous monitoring of world events and specific activities to determine the probability of hostile actions. I&W includes forewarning of enemy actions or intentions; the imminence of attack on the US, its overseas forces, or allied nations; hostile reactions to US activities; terrorist and insurgent attacks; and other similar events. The I&W process also analyzes nonmilitary activity that could alter or otherwise affect the situation within the AOI, such as drastic changes in political, economic, environmental or social situations. At operational and tactical levels, I&W intelligence is indistinguishable from current intelligence.
- **Current Intelligence.** Current intelligence involves the integration, evaluation, analysis, and interpretation of information on the current enemy situation and conditions within the operational environment. It is similar to I&W in that both depend upon continuous monitoring of events and specific activities within the AOI. Current intelligence helps intelligence organizations confirm enemy COAs, identify civil considerations; explain the activity, events, or conditions in relationship to friendly operations; and identify information gaps. Current intelligence and general military intelligence (GMI) efforts are interdependent. Current intelligence in the form of current intelligence reports and IPB products updates GMI while GMI in the form of studies and assessments provides the basis for current intelligence.

- **General Military Intelligence.** GMI includes relevant information about the operational environment as well as information on the organization, operations, facilities, and capabilities of selected military and paramilitary forces including terrorist and insurgent groups. This broad category of intelligence is normally associated with long-term research that supports planning and preparation for military operations, including training and combat development. Kept up to date, GMI products and databases provide the basis for intelligence estimates, IPB of the battlefield products, and current intelligence. Examples of GMI products include capabilities, subject, and CI assessments:
  - Capability assessments identify forces and dispositions, evaluate enemy vulnerabilities, and assess the enemy's ability to employ lethal and non-lethal means to counter friendly forces.
  - Subject assessments include military geography and demography studies. Military geography studies analyze the impact that geographic features may have on planned operations, force deployment, and mobility. Demographic studies contribute to an understanding of the dispersion and cultural composition of the population (for example, language, religion, socioeconomic status, and nationality or ethnic groups) in the AOI.
  - Multidiscipline counterintelligence (MDCI) threat assessment evaluates all foreign intelligence and security services disciplines, terrorism, foreign-directed sabotage, and related security threats.
- **Target Intelligence.** Target intelligence entails the analysis of the operational environment to identify and nominate specific enemy assets or vulnerabilities for attack, reattack, or exploitation (for intelligence). It consists of two mutually supporting production tasks: target development and battle damage assessment (BDA).
  - Target development is the systematic evaluation and analysis of target systems, system components, and component elements to determine high value targets (HVTs) for potential lethal or non-lethal attack. A special operations target intelligence package is an example of one type of target intelligence product. A complete special operations target intelligence package contains multi-source information describing the target; the climate, geography, or hydrography; the demographic, cultural, political, and social features of the operations area; and the enemy, to include force disposition of military, paramilitary, or other indigenous forces and security or police forces of danger to US elements. The target intelligence package must also contain current imagery of the target and AO, as well as accurate geospatial products and information.
  - Once attacked, BDA, a component of combat assessment, provides a timely and accurate estimate of the affects of the application of military force (lethal or non-lethal) on targets and target systems based on predetermined objectives.
- **Scientific and Technical Intelligence.** Scientific and technical intelligence (S&TI) looks at foreign scientific and technical developments that have or indicate a warfare potential. This includes medical capabilities; weapon system characteristics, capabilities, vulnerabilities, limitations, and effectiveness; research and development activities related to those systems; and related manufacturing information. In counterterrorist and counterinsurgency operations (COINs), S&TI also supports detection and countering of weapons of mass destruction (WMDs) and improvised explosive devices (IEDs). During peace and war, S&TI precludes scientific and technological surprises and advantages by an enemy that could be detrimental to friendly personnel and operations.

CONDUCT RESEARCH

4-4. During operations planning and preparation, open source research answers intelligence requirements, identifies information gaps, and facilitates optimum employment of military resources. The results of research populate and update national, regional, and local intelligence databases. These databases coupled with the skills and knowledge acquired in their development, enable intelligence analysts to respond quickly and accurately to demands for intelligence during the MDMP and subsequent preparation for and execution of military operations. With the knowledge the operational environment, commanders and their subordinates are better able to ask the "right questions" that drive the actions and results of the intelligence warfighting function (WFF) throughout planning, preparation, execution, and assessment of military operations.

PRACTICAL RESEARCH

4-5. Intelligence analysts use open source research to answer the SIRs. Most intelligence analysts conduct practical research as opposed to field research. In field research, personnel from academic, governmental, intergovernmental, and NGOs collect new or current data from primary sources as well as retrieve data and information from secondary sources (see para 4-23). In practical research, analysts retrieve existing data and information from secondary sources to answer intelligence requirements.

4-6. Practical research begins with the analyst's determining the research question regarding a given topic followed by developing a research plan and retrieving information. In intelligence operations, the research question is based on anticipated or stated intelligence requirements (for example, commander's guidance, PIRs, RFIs). The analyst breaks the research question into statements (SIRs) that define the variables and the environment in which the variables interact. The analyst uses the statements to develop the research plan and retrieve information. The analyst integrates, evaluates, and analyzes the retrieved information then interprets the results of analysis to answer the question (see Figures 4-1 and 4-2). The analyst reports the conclusion or answer to the research question and other relevant information as intelligence in the form of briefings, estimates, studies, and other formats.

DETERMINE RESEARCH QUESTION

4-7. During orientation and contingency planning, analysts develop research questions to identify critical variables and their relationship within potential and planned operational environments. During operational planning, the analyst refines or updates the research questions based on the commander's guidance, PIRs, and questions raised during mission analysis, COA analysis, and COA evaluation.

PLAN RESEARCH

4-8. Once analysts determine their principal research questions, they develop a research plan to answer the question. Planning begins with the analyst determining the research strategy then identifying variables and potential sources. The variables are the factors that the analyst uses in the chosen research strategy to answer the research question. Coupled with the research question, the variables define the information about the operational environment or subject that the analyst needs to retrieve from secondary sources or, in the case of field research, primary sources. According to *Political Analysis: Technique and Practice*, there are several types of research strategies including historical research, comparative research, and hypothesis testing.

- A historical research strategy uses inductive reasoning to reach a general theory about the meaning of patterns in an event or series of events within one area or subject.
- A comparative research strategy uses inductive reasoning to develop a theory about patterns by looking for similarities or differences in multiple areas or subjects.
- Hypothesis testing uses deductive reasoning to prove or disprove established theories or theories generated during historical and comparative research.

4-9. In practical research, the potential secondary sources are normally newspapers, periodicals, published research, online and offline databases, and libraries. These give the analyst access to sources and publicly available information described in Chapter 2. In addition to these secondary sources, the analyst may identify primary sources for open source collection operations based on known information gaps in the research plan or gaps identified during integration and analysis. As part of the plan, the analyst identifies information sources, how to access those sources, a format for compiling the data, the research methodology (techniques), and report format. All of these factors comprise the research plan and should be organized into a chart, spreadsheet, or other project management tool in order to track progress.

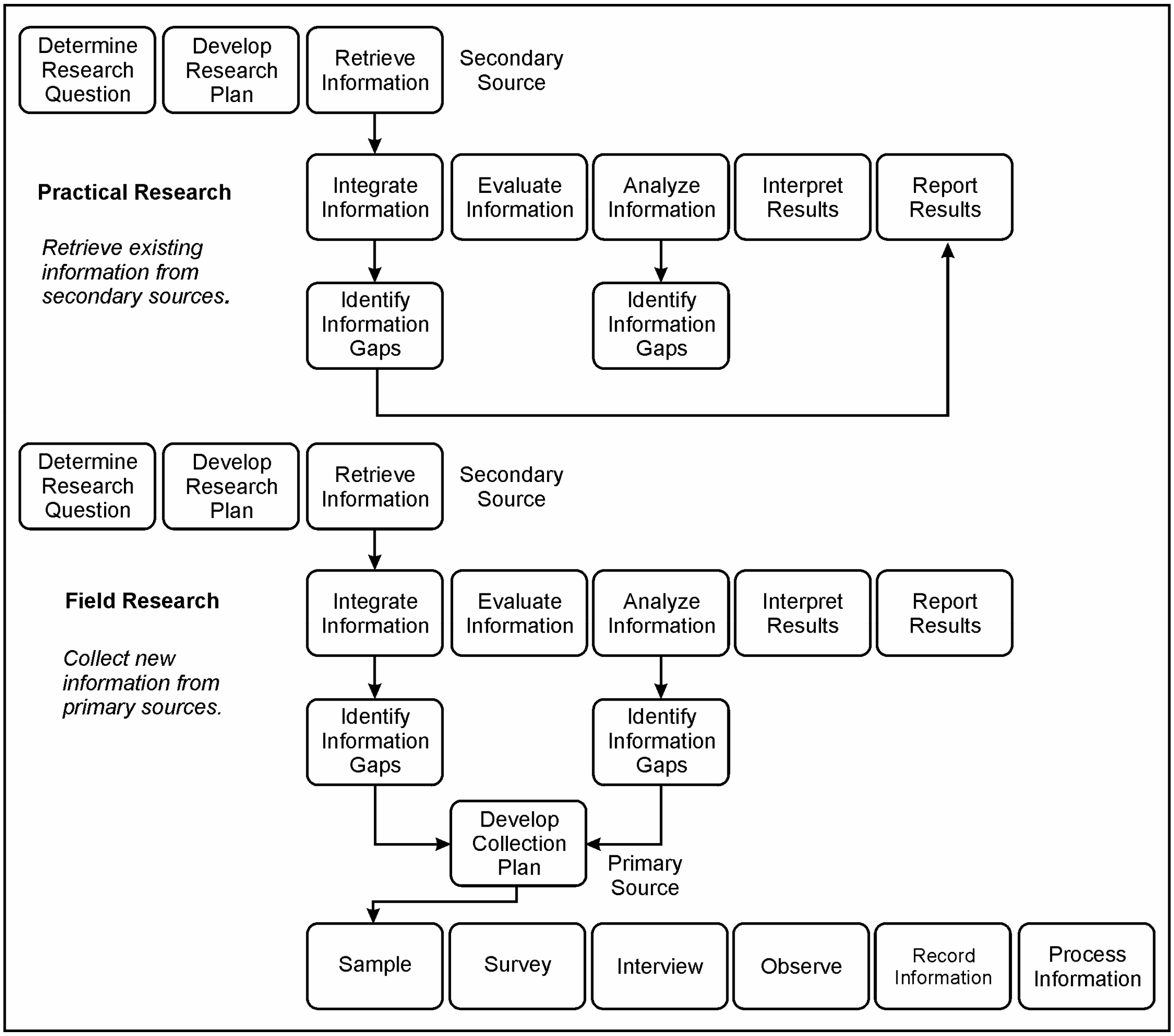


Figure 4-1. Practical and field research

RETRIEVE INFORMATION

4-10. In practical research, the analyst conducts an initial search of likely sources using the terms and the area or the subject in the research question. The initial search may lead to existing information that answers the research question (see Appendix H for a basic list of resources). If not, the initial search is the first of potentially many subsequent searches for data and information that the analyst retrieves and records in accordance with the research plan (see Appendix I for basic Internet search techniques). The analyst must set limits and make judgments about how long to search open sources and retrieve information since these tasks can become a near continuous activity as the search of one source or the resolution to one question gives rise to others.

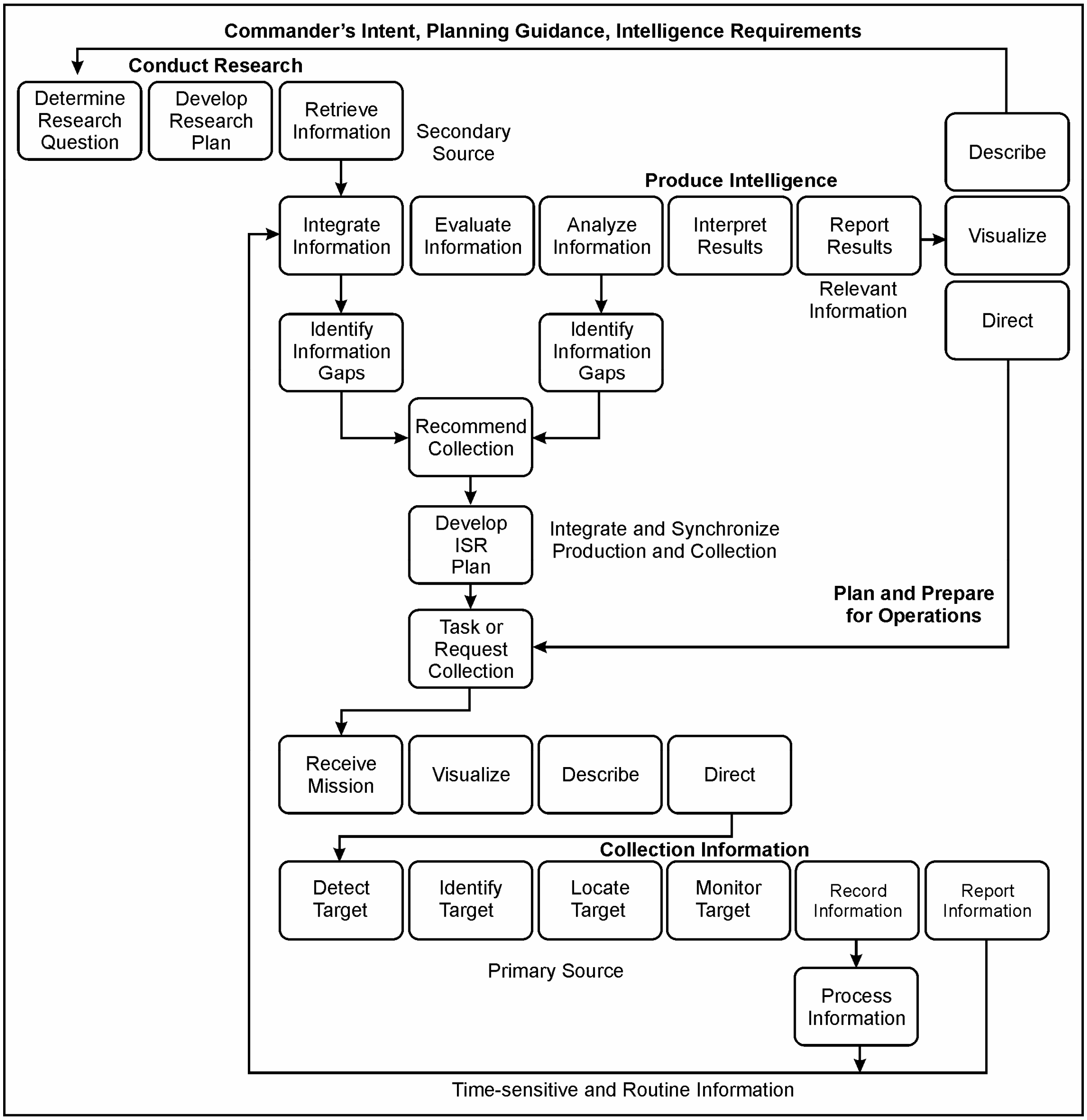


Figure 4-2. Research and the intelligence process

4-11. Once retrieved, the analyst integrates the information into the appropriate digital or analog database in preparation for the remaining phases of the production process (evaluation, analysis, and integration). During the integration and analysis, the analyst identifies the information gaps that affect the outcome of the research. Depending upon their criticality, these information gaps become the basis of collection tasks and RFIs (see Figure 4-2). As a minimum, the analyst ensures these gaps are included and their impact noted in the intelligence reports.

OPERATIONAL ENVIRONMENT ASSESSMENT

4-12. An operational environment assessment is an example of a methodology that uses open source research to focus research and support understanding (see Appendix J). Open source research, coupled with an understanding of the contemporary operational environment (COE), is the basis for an operational environment assessment. An operational environment assessment is a technique designed to apply the COE variables to a specific region, nation states, or non-state actors. It encompasses all the conditions, circumstances, and influences that affect the employment of military forces and the decisions of the unit commander.

4-13. The operational environment assessment consists of a detailed examination and analysis of the eleven critical variables of the COE, and their interaction and reciprocal relationships. Based on this analysis, the operational environment assessment identifies trends and issues with which units may have to grapple during their planning, preparation for, and execution of operations. As an unclassified document (in whole or part), the operational environment assessment also serves as a useful tool for individual and collective training during preparation for operations in a specific area.

COUNTRY STUDY

4-14. The area or country study is an example of a historical research strategy that intelligence analysts use to understand the cultural characteristics and their influences on military operations. Some the considerations in the study also appear as part of the eleven critical variables of the COE. The following is a model or considerations for a study similar to those of the FMSO publications, the US Marine Corps (USMC) Intelligence Activity’s Country Handbooks, the Central Intelligence Agency’s (CIA’s) World Fact Book, and the Federal Research Division’s Country Studies.

- Statement of the national problem.
- Relevant national interests.
- Stated or perceived military mission.
- Nature of the physical environment.
- Nature of society.
- Nature of external forces.
- Nature of the crisis.
- Impact of time.
- Host nation support agreements.
- Significant logistics support considerations.
- General types of US support actions contemplated.
- Legal status of US personnel in the operational area.

4-15. The nature of society considerations include—

- History.
- Population and demographics.
- General cultural characteristics.
- Religions and Sects.
- Economy.
- Politics

- Infrastructure.
- Military and security forces.
- Potential destabilizing factors.
- Factions vying for power, influence, or control.
- Nongovernmental factions (leadership, ideology, organization, external support, strategy, and tactics).
- Government response (national strategy; development activities; social mobilization; intelligence; effectiveness of civil-military structure, services, and criminal justice; use of force).

4-16. The nature of crisis considerations include—

- Critical events.
- Economic problems.
- Natural disasters.
- Governmental actions or reactions (trust versus mistrust).
- Recent military defeat or victory.
- Religious influences.
- Tribal or ethnic conflicts, hatreds, feuds.
- Agitators and mobilizers.

Research Resources

4-17. Analysts have access to a number of resources during their research of operational environments. Within DOD, these resources include but are not limited to the DIA and Service organizations such as the NGIC, the Marine Corps Intelligence Activity, the National Maritime Intelligence Center, and the NASIC, which conduct open source research as part of their all-source intelligence production missions. Open source research is also an essential mission of organizations such as the DOD Centers for Regional Security Studies and the Army's FMSO.

4-18. The DOD Centers for Regional Security Studies enhance security, foster partnerships, improve national security decisionmaking, and strengthen civil-military relationships through education, exchanges, research, and information sharing. A core regional center mission is to support DOD's policies and priorities by assisting military and civilian leaders in the region in developing strong defense establishments and strengthening civil-military relations in a democratic society. The regional centers are—

- George C. Marshall European Center for Security Studies, US European Command.
- Asia-Pacific Center for Security Studies, US Pacific Command.
- Africa Center for Strategic Studies, National Defense University.
- Center for Hemispheric Defense Studies, National Defense University.
- Near East-South Asia Center for Strategic Studies, National Defense University.

4-19. Education, research, and outreach are the National Defense University's main missions. The University's three regional centers mentioned above foster international understanding and promote the development of cooperative relations in such areas as national security strategy, civil-military relations, and defense economics. Through its research centers, the National Defense University produces policy analyses, research and other support to the Joint Chiefs of Staff, the Office of the Secretary of Defense, Combatant Commanders from major military commands, and other US Government agencies. The research centers are—

- Center for the Study of Weapons of Mass Destruction.
- Center for Technology and National Security Policy.

- Institute for Homeland Security Studies.
- Institute for National Strategic Studies.

4-20. TRADOC's Deputy Chief of Staff for Intelligence has two elements that conduct open source research:

- **Foreign Military Studies Office.** The FMSO is a research and analysis center which manages and operates the Fort Leavenworth Joint Reserve Intelligence Center and conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments around the world. Joint Reserve Component personnel and units—operating at the Fort Leavenworth Joint Reserve Intelligence Center and in distance drilling analytical teams around the US and abroad—make substantial contributions to all FMSO production efforts. More information about the FMSO, as well as access to its products and research links, are available at http://fmso.leavenworth.army.mil/index.htm.
- **Contemporary Operational Environment and Threat Integration Directorate.** The Contemporary Operational Environment and Threat Integration Directorate develops, publishes, validates, and applies COE conditions that support all Army training and leader development programs; develops and maintains a COE and threat information repository regarding equipment, organization, tactics, doctrine, and material for training; and prescribes a methodology for developing current and predictive operational environment assessments to support all Army training. This directorate's products are available at https://dcsint-threats.leavenworth.army.mil/default.aspx

4-21. The Federal Research Division of the Library of Congress is another resource available to analysts. It provides directed research and analysis on domestic and international subjects to agencies of the US Government, the District of Columbia, and authorized Federal contractors. As expert users of the vast English and foreign-language collections of the Library of Congress, the Division's area and subject specialists employ the resources of the world's largest library and other information sources worldwide to produce impartial and comprehensive studies on a cost-recovery basis. The Division's website at http://www.loc.gov/rr/frd includes the following open source research studies and profiles:

- **Country Studies.** The Country Studies series presents a description and analysis of the historical setting and the social, economic, political, and national security systems and institutions of countries throughout the world. The Country Studies website contains the online versions of books previously published (1988-98) in hardcopy under the Country Studies/Area Handbook Program sponsored by the DA. Because the original intent of the series' sponsor was to focus primarily on lesser-known areas of the world or regions in which US forces might be deployed, the series is not all-inclusive.
- **Country Profiles.** The Country Profiles series of foreign nations is part of the Country Studies Program. The profiles offer brief, summarized information on a country's historical background, geography, society, economy, transportation and telecommunications, government and politics, and national security. In addition to being featured in the front matter of published Country Studies, they are now being prepared as stand-alone reference aides for all countries in the series, as well as for a number of additional countries of interest. The profiles offer reasonably current country information independent of the existence of a recently published Country Study and will be updated annually or more frequently as events warrant.

EVALUATE INFORMATION

4-22. Deception and bias are of particular concern in OSINT operations. Secondary sources such as government press offices, commercial news organizations, political campaign staffs, research center publications, and others who publish or broadcast information can intentionally or unintentionally add, delete, modify, or otherwise filter the information they make available to the public. It is important to evaluate the reliability of open sources in order to distinguish objective, factual information from that lacking merit, containing bias, or is part of an effort to deceive the listener or viewer.

4-23. Analysts evaluate each new item of information with respect to the reliability of the source and the credibility of the information (Table 4-1). An alphanumeric rating is assigned to each piece of information to indicate the degree of confidence the evaluator places on the information. This rating is based on the subjective judgment of the evaluator and the accuracy of previous information produced by the same source. The capabilities and performance of the collection resource may also be a factor in the evaluation. Intelligence personnel must assess the reliability of the source and the credibility of the information independently of each other to avoid the possibility of one factor evaluation biasing the other.

Table 4-1. Types of sources

TYPE	DESCRIPTION	FACTORS
Primary Source	Has direct access to the information and conveys the information directly and completely.	**Access**. Did the source have direct access to the even or information? **Mediation**. Does the source provide a direct and complete view of the event or information? **Responsibility**. The more immediately, continuously, and directly a controller controls a source, the more responsible the source is to its controller and the more authoritative it is in presenting the controller's view. **Track Record**. Analysis of the source based on source's past behavior.
Secondary Source	Conveys information throught various types of filters: • Uses intermediary sources. • Summarizes, paraphrases, or excerpts. • Translates from the vernacular.	
Authoritative Source	Accurately reports information because it is known to be accountable to or has a track record demonstrating accuracy in reporting information from the leader, government, ruling party, or other element.	

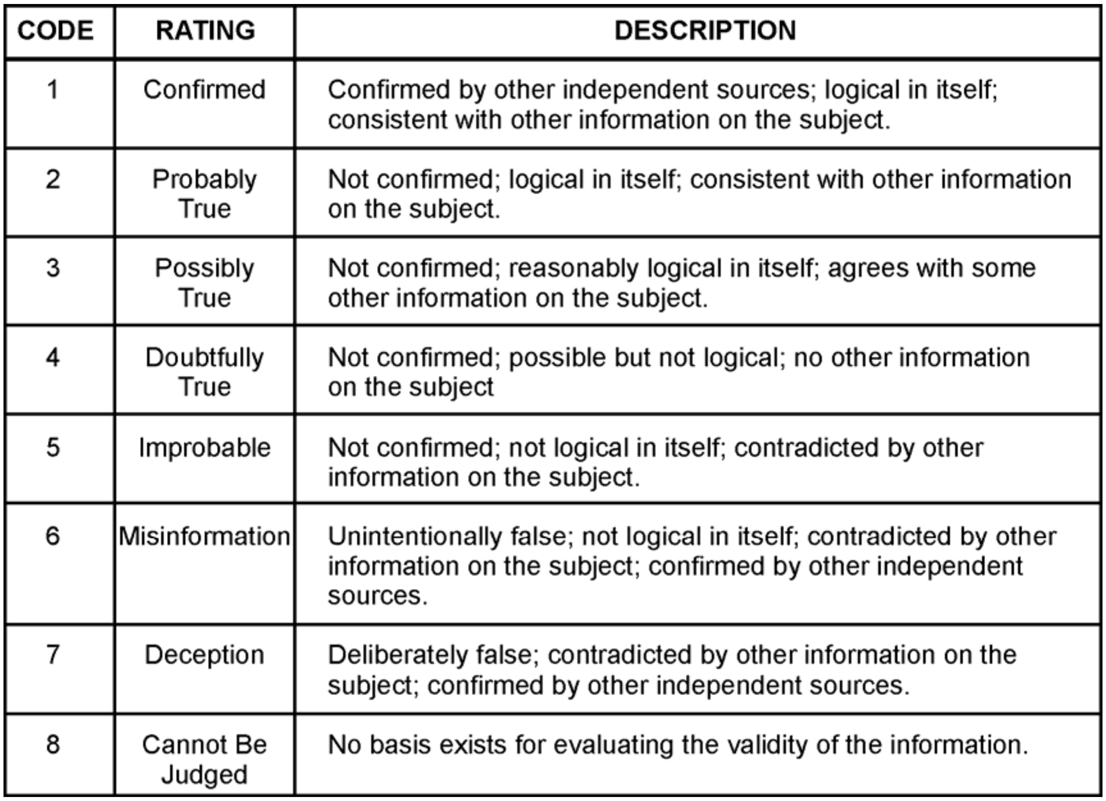
4-24. Source reliability ratings range from A (Reliable) to F (Cannot Be Judged) as shown in Table 4-2. If the source is new, they rate the source as F (Cannot Be Judged). An F rating does not necessarily mean the source is unreliable but that the collection and processing personnel have no previous experience with the source upon which to base a determination.

Table 4-2. Source reliability

CODE	RATING	DESCRIPTION
A	Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability; usually demonstrates adherence to known professional standards and verification processes.
B	Usually Reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time; may not have a history of adherence to professionally accepted standards but generally identifies what is known about sources feeding any broadcast.
C	Fairly Reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past.
D	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past.
E	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information.
F	Cannot Be Judged	No basis exists for evaluating the reliability of the source; new information source.

4-25. Information credibility ratings range from 1 (Confirmed) to 8 (Cannot Be Judged) as shown in Table 4-3. If the information is new, they rate the content as 8 (Cannot Be Judged). An 8 rating does not necessarily mean the information is not credible but that the collection and processing personnel have no means of verifying the information.

Table 4-3. Information credibility



CODE	RATING	DESCRIPTION
1	Confirmed	Confirmed by other independent sources; logical in itself; consistent with other information on the subject.
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject.
3	Possibly True	Not confirmed; reasonably logical in itself; agrees with some other information on the subject.
4	Doubtfully True	Not confirmed; possible but not logical; no other information on the subject
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject.
6	Misinformation	Unintentionally false; not logical in itself; contradicted by other information on the subject; confirmed by other independent sources.
7	Deception	Deliberately false; contradicted by other information on the subject; confirmed by other independent sources.
8	Cannot Be Judged	No basis exists for evaluating the validity of the information.

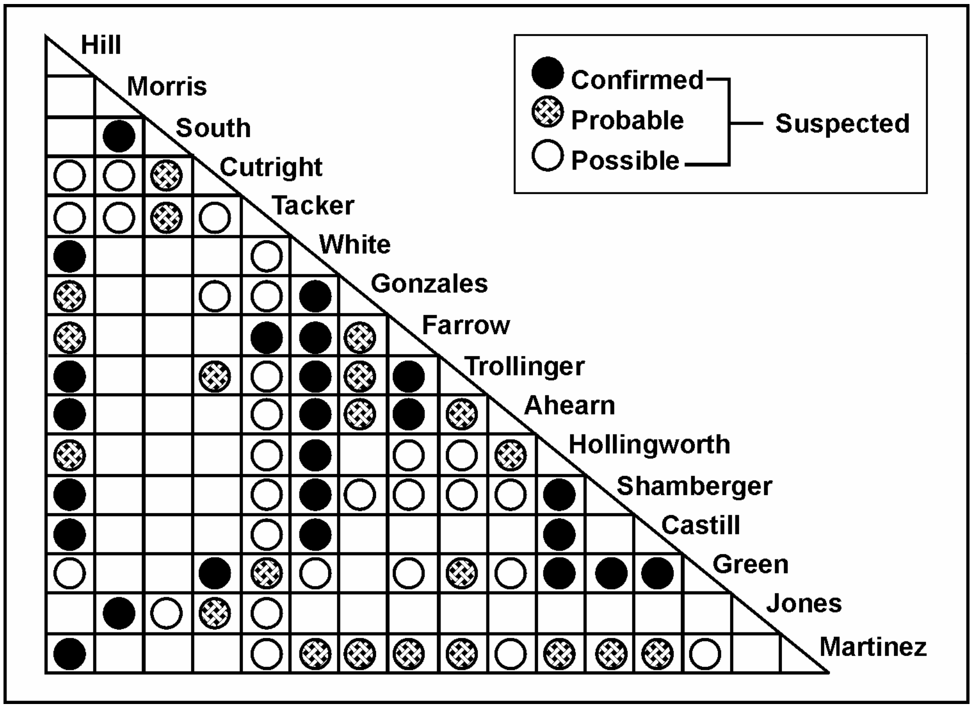
4-26. Media source analysis is the systematic comparison and analysis of the content and behavior of different media sources over time. It is fundamental to media analysis (see Appendix K). Systematic efforts to identify patterns in differences among media have traditionally yielded rich insights into basic policy and leadership disputes. Comparison of trends in the content of individual media with shifts in official policy has suggested that some media, at least more than others, will continue to mirror the dominant policy line. By establishing a track record for different media that suggests which are vulnerable to pressure to follow the central policy line, analysts will still have a powerful tool for identifying policy and recognizing policy shifts.

ANALYZE INFORMATION

4-27. During analysis, intelligence personnel use a variety of analysis techniques to discern facts, indicators, patterns, and trends in information and relationships between variables. The techniques apply inductive or deductive reasoning to understand the meaning of past events and predict future actions. Each technique is based on facts, observations, or assumptions about the operational environment. Intelligence personnel are mindful of injecting US or US military cultural bias into their analysis, particularly their assumptions. FM 33.4 (FM 34-3) and FM 2-01.3 (FM 34-130) provide more information about intelligence analysis techniques and procedures.

ASSOCIATION MATRIX

4-28. Intelligence analysts use the association matrix to establish known or suspected associations between individuals. Direct connections include, for example, face-to-face meetings or confirmed telephonic conversations. Figure 4-3 provides a one-dimensional view of the relationships and tends to focus on the immediate AO. Analysts can use association matrixes to identify those personalities and associations needing a more in-depth analysis in order to determine the degree of relationship, contacts, or knowledge between the individuals. The structure of the threat organization is formed as connections between personalities are made.

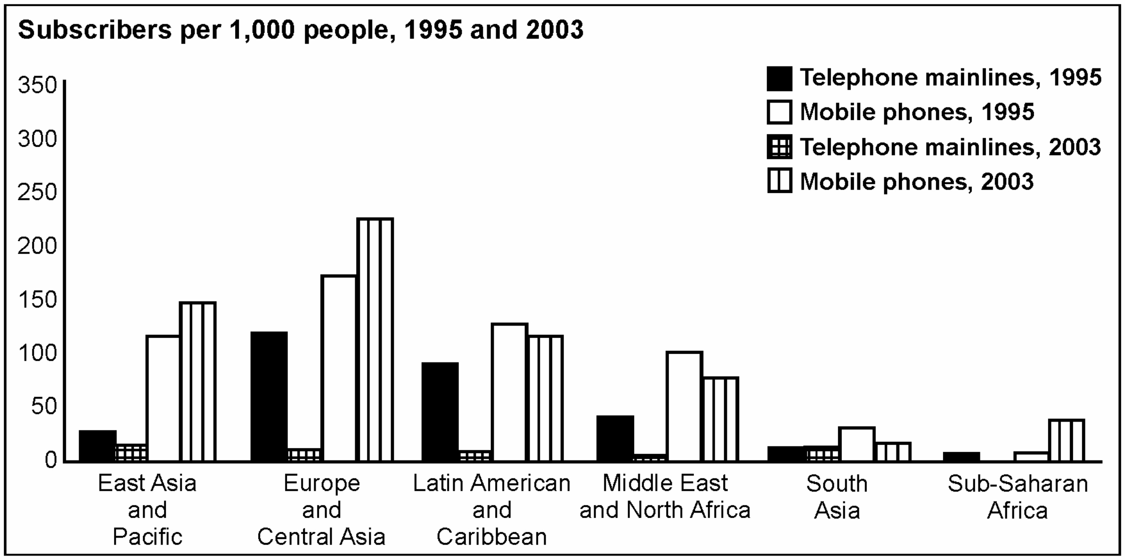

● Confirmed
◍ Probable
○ Possible
Suspected

	Hill	Morris	South	Cutright	Tacker	White	Gonzales	Farrow	Trollinger	Ahearn	Hollingworth	Shamberger	Castill	Green	Jones
Morris															
South		●													
Cutright	○	○	◍												
Tacker	○	○	◍	○											
White	●				○										
Gonzales	◍			○	○	●									
Farrow	◍				●	●	◍								
Trollinger	●			◍	○	●	◍	●							
Ahearn	●				○	●	◍	●	◍						
Hollingworth	◍				○	●		○	○	◍					
Shamberger	●				○	●	○	○	○	○	●				
Castill	●				○	●					●				
Green	○			●	◍	○		○	◍	○	●	●	●		
Jones		●	○	◍	○										
Martinez	●				○	◍	◍	◍	◍	○	◍	◍	◍	○	

Figure 4-3. Example of an association matrix

CHARTS, GRAPHS, AND TABLES

4-29. Intelligence analysts use bar graphs, x/y graphs, pie charts, and tables to depict, identify, and measure changes in patterns or trends throughout the statistical analysis. Using spreadsheets, researchers and analysts can integrate and analyze large amounts of data retrieved from secondary sources or collected through direct observation. Open sources are an important source of data and finished products. Figure 4-4 is an example of a bar chart retrieved from the World Bank website that depicts changes in mobile phone access.



Source: World Bank. (2005) *World Development Indicators 2005*.
Retrieved from: http://www.worldbank.org/data/wdi2005/

Figure 4-4. Example of a bar graph

INFRASTRUCTURE OVERLAYS

4-30. Intelligence analysts use infrastructure overlays to identify infrastructure and assets that are critical or key to military operations and the civilian population. National critical infrastructure and key assets are the infrastructure and assets vital to a nation’s security, governance, public health and safety, economy, and public confidence. They include telecommunications, electrical power systems, gas and oil distribution and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations.

4-31. Critical infrastructure overlays can be useful for identifying protected terrain. Protected terrain encompasses areas that should not be destroyed, attacked, or occupied, or that have other use restrictions based on international treaties, rules of engagement, and common sense—such as schools, hospitals, areas with large amounts of phone or electrical wiring, and buildings with many stories. For example, medical facilities may be depicted on their own key infrastructure overlay. Medical facilities are generally “no fire” areas for friendly forces and protected from damage or destruction so that they can continue to take care of the local population once friendly forces have secured the urban area. Inadequate health care for the local population can lead to both a negative perception of friendly forces and an uncontrolled increase in disease, which can affect friendly forces personnel working in the urban environment directly.

4-32. Like population status overlays, this type of overlay is a group of products rather than a single product. Figure 4-5 is an example of one type of infrastructure overlay, a logistics sustainability overlay. In rural areas, a logistics sustainability overlay could depict potable water supplies, farms, orchards, growing seasons, and other relevant items. In built-up areas, this overlay could depict supermarkets, food warehouses, pharmacies, hospitals, clinics, and residences of doctors and other key medical personnel. Key to preparing this overlay is knowledge of infrastructure within the AO; the disposition of military forces (friendly and enemy) and civilians; their sustainment requirements, and the availability and location of resources (materiel and personnel) to meet these requirements.

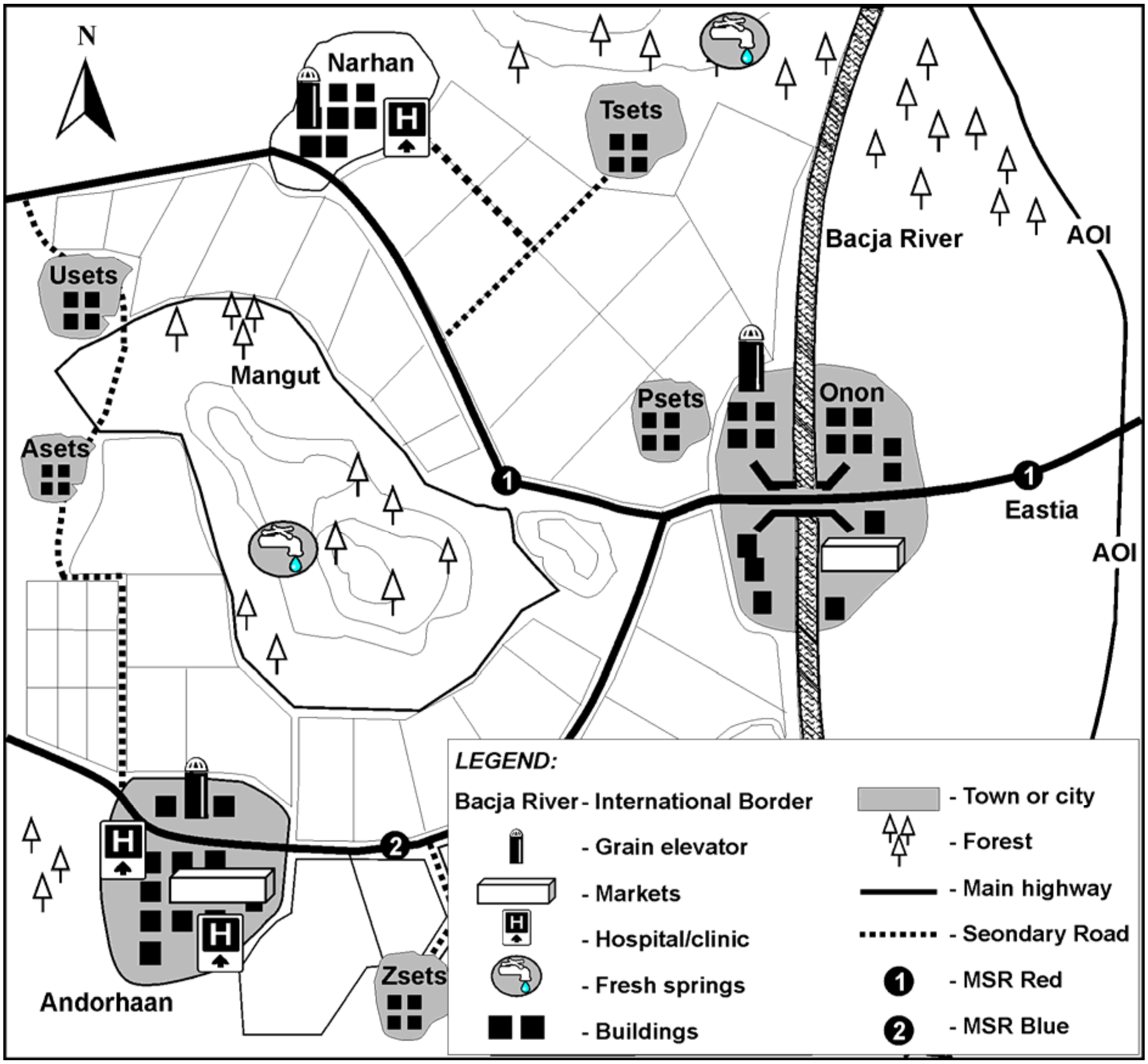


Figure 4-5. Example of a logistics sustainability overlay

LINK (NETWORK) DIAGRAM

4-33. Intelligence analysts use the link diagram to identify relationships between organizations, individuals, events, or other factors deemed significant in any given situation. Link diagrams can depict C2, financial, and social relationships as networks. In OSINT, the diagram can map the relationship between the source and the broadcast station or what websites link to a specific homepage. They can help the analyst determine nodes within networks; status or purpose of nodes; critical nodes or individuals within the network; and interaction of nodes with external networks. Figure 4-6 is an example of a link (network) diagram.

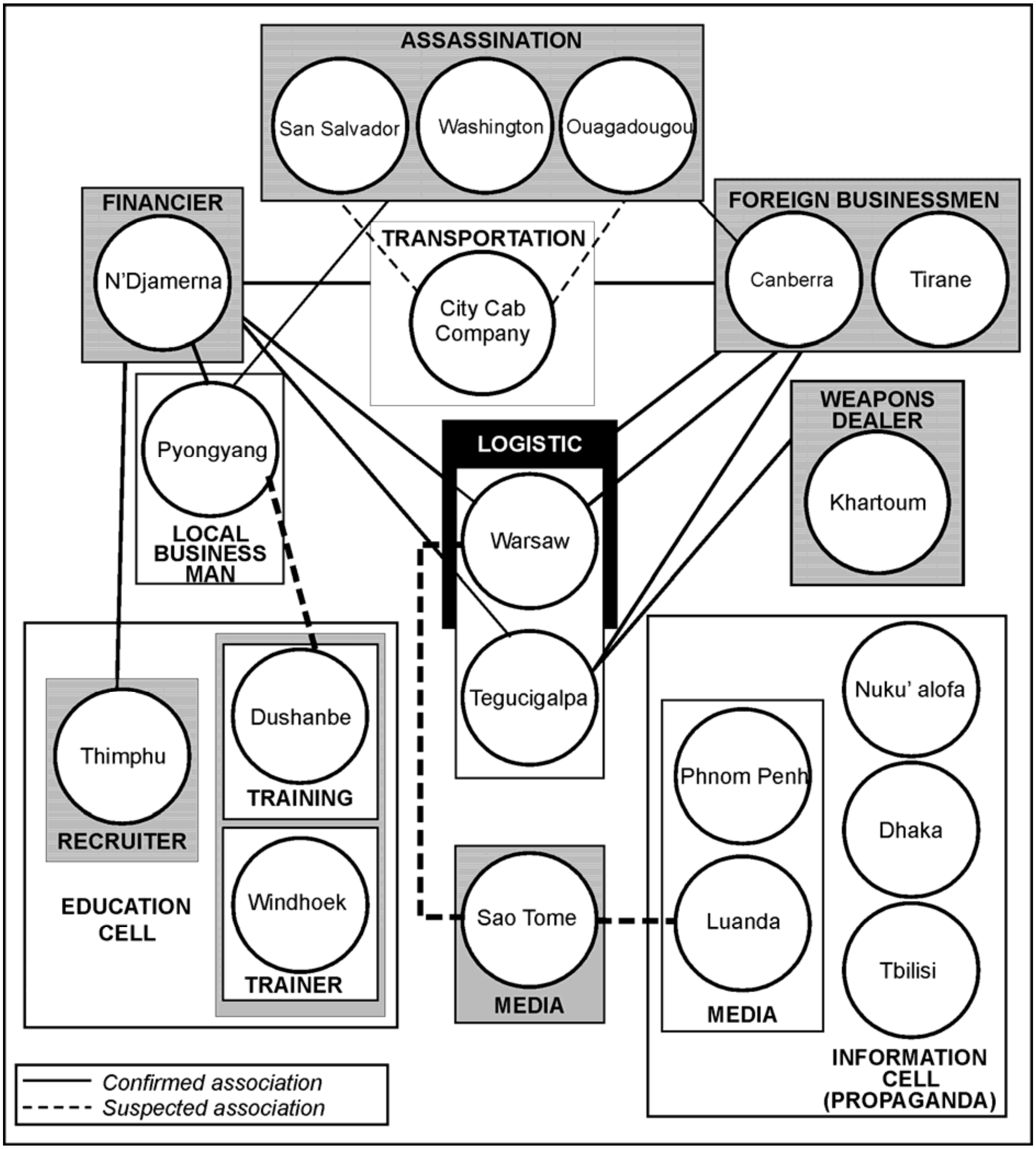


Figure 4-6. Example of a link diagram

PERCEPTION ASSESSMENT MATRIX

4-34. Intelligence analysts use the perception assessment matrix to establish the relationship between actions and perceptions. The matrix aids the analysts in understanding how the others (enemy, civilian population, multinational or coalition partners) perceive friendly forces, themselves, the operational environment, and their success criteria. An in-depth knowledge and understanding of the national, regional, and local cultures helps the analyst understand the operational environment and the reactions of the enemy and populace friendly force activities. Table 4-4 is an example of a perception assessment matrix. There are several means to measure perceptions:

- Determine demographic and cultural factors that shape perceptions and reactions.
- Identify patterns and indicators from previous expectations and reactions in a society's history.
- Compare reported reactions to determine if they were based on real or perceived conditions.
- Monitor editorial and opinion pieces of relevant newspapers for changes in tone or opinion shifts that can steer or may be reacting to the opinions of a society, organization, or group.

Table 4-4. Example of perception assessment matrix

Condition	Cultural Norm	Friendly Force Action	Population Perception	Cause of Perception	Consequence if Unchanged
Food	Rice	Provided meat and potatoes	Inadequate and inconsiderate	Practical (no experience with potatoes) and cultural (dietary rules on meat)	Starvation and riots
Armed Civilian	All men carry weapons	Confiscated all weapons	Unfair and demeaning	Practical (safety) and cultural (symbol of manhood)	Risk of violence between US forces and armed civilians
Government Structure	Tribal	Established military administration (hierarchical	Tolerable as long as the authority fulfils needs	Historical (previous experience with Western or military forms of government)	Loss of credibility and eventually control if needs are not met

POPULATION STATUS OVERLAY

4-35. Intelligence analysts use the population status overlays to identify points of potential conflict between segments of a society; bases of support or sustainment for enemy forces; or areas that are neutral or favorable to US military operations. Based on open source research and updated during operations, the population overlays depict the characteristics and the disposition of the civilian population within the operational environment. Figure 4-7 is an example of a population status overlay that depicts the sectors of the population that are pro-government, anti-government, pro-threat, anti-threat, and uncommitted or neutral.

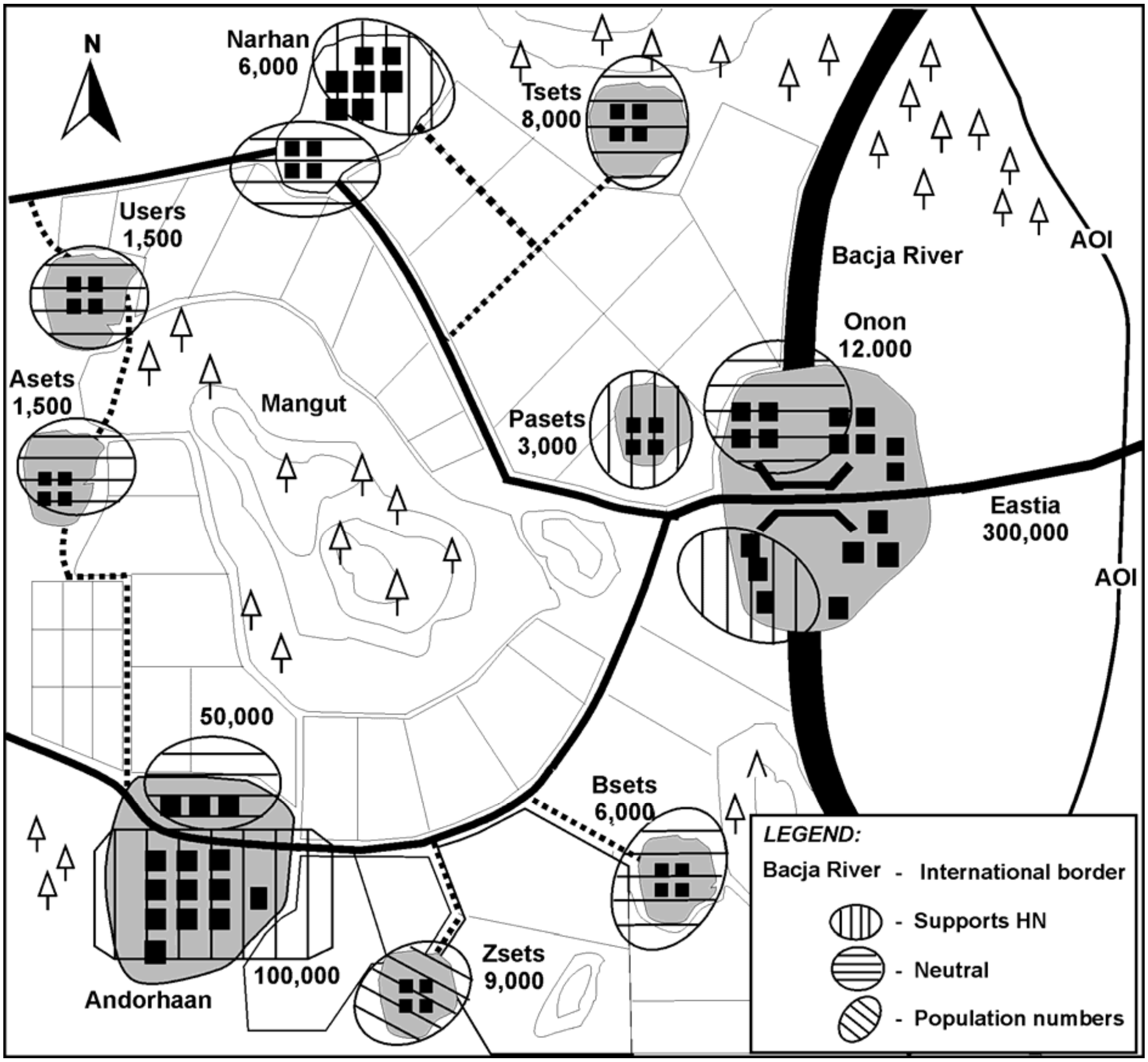
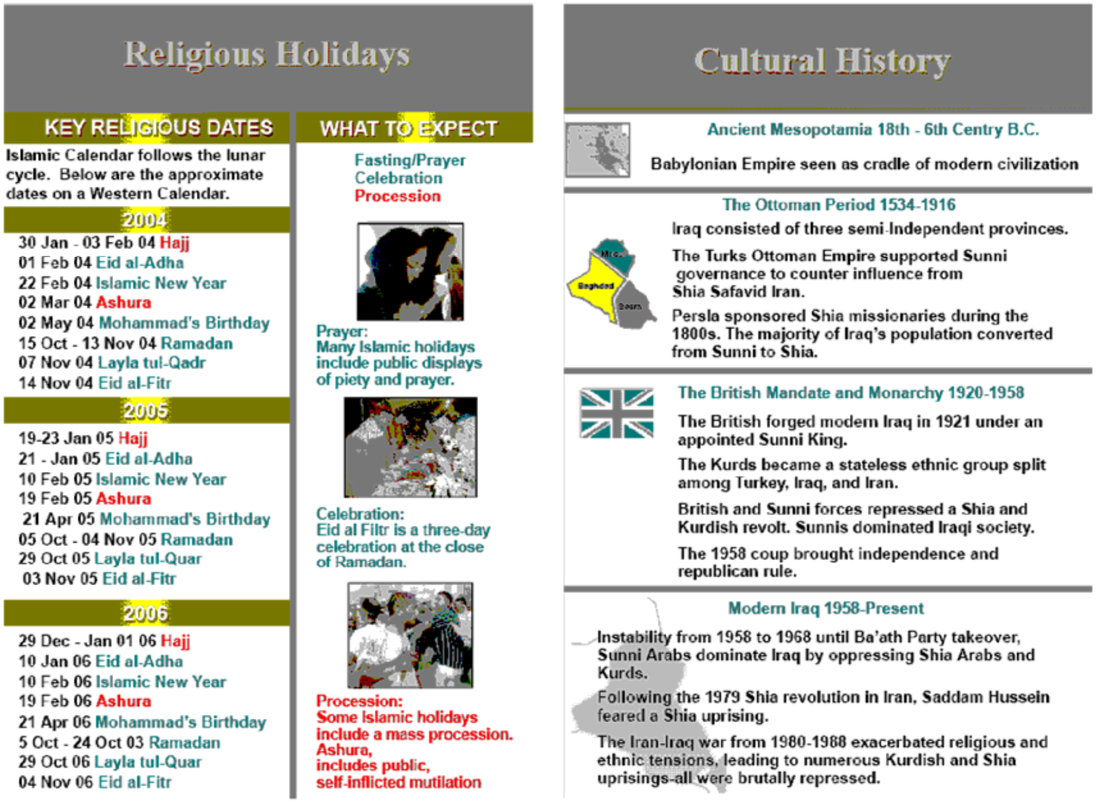


Figure 4-7. Population status overlay

TIMELINES OF KEY DATES

4-36. Intelligence analysts use timelines to identify key local national holidays, historic events, and significant cultural and political events (Figure 4-8). Timelines help the analyst anticipate and inform the unit as to how key sectors of the population might react to given circumstances. These timelines could include descriptions of population movements or political shifts that are relevant to the operational area. They could also include a brief historical record of the population or area, highlighting the activities of a certain population sector. For example, in Bosnia, weddings were often held on Fridays and celebratory fire was a common occurrence on Friday afternoons and late into the night. Timelines—a list of significant dates along with relevant information and analysis—seek to provide a context to operational conditions.



Religious Holidays

KEY RELIGIOUS DATES

Islamic Calendar follows the lunar cycle. Below are the approximate dates on a Western Calendar.

2004

30 Jan - 03 Feb 04 Hajj
01 Feb 04 Eid al-Adha
22 Feb 04 Islamic New Year
02 Mar 04 Ashura
02 May 04 Mohammad's Birthday
15 Oct - 13 Nov 04 Ramadan
07 Nov 04 Layla tul-Qadr
14 Nov 04 Eid al-Fitr

2005

19-23 Jan 05 Hajj
21 - Jan 05 Eid al-Adha
10 Feb 05 Islamic New Year
19 Feb 05 Ashura
21 Apr 05 Mohammad's Birthday
05 Oct - 04 Nov 05 Ramadan
29 Oct 05 Layla tul-Quar
03 Nov 05 Eid al-Fitr

2006

29 Dec - Jan 01 06 Hajj
10 Jan 06 Eid al-Adha
10 Feb 06 Islamic New Year
19 Feb 06 Ashura
21 Apr 06 Mohammad's Birthday
5 Oct - 24 Oct 03 Ramadan
29 Oct 06 Layla tul-Quar
04 Nov 06 Eid al-Fitr

WHAT TO EXPECT

Fasting/Prayer
Celebration
Procession

Prayer:
Many Islamic holidays include public displays of piety and prayer.

Celebration:
Eid al Filtr is a three-day celebration at the close of Ramadan.

Procession:
Some Islamic holidays include a mass procession. Ashura, includes public, self-inflicted mutilation

Cultural History

Ancient Mesopotamia 18th - 6th Centry B.C.

Babylonian Empire seen as cradle of modern civilization

The Ottoman Period 1534-1916

Iraq consisted of three semi-Independent provinces.

The Turks Ottoman Empire supported Sunni governance to counter influence from Shia Safavid Iran.

Persla sponsored Shia missionaries during the 1800s. The majority of Iraq's population converted from Sunni to Shia.

The British Mandate and Monarchy 1920-1958

The British forged modern Iraq in 1921 under an appointed Sunni King.

The Kurds became a stateless ethnic group split among Turkey, Iraq, and Iran.

British and Sunni forces repressed a Shia and Kurdish revolt. Sunnis dominated Iraqi society.

The 1958 coup brought independence and republican rule.

Modern Iraq 1958-Present

Instability from 1958 to 1968 until Ba'ath Party takeover, Sunni Arabs dominate Iraq by oppressing Shia Arabs and Kurds.

Following the 1979 Shia revolution in Iran, Saddam Hussein feared a Shia uprising.

The Iran-Iraq war from 1980-1988 exacerbated religious and ethnic tensions, leading to numerous Kurdish and Shia uprisings-all were brutally repressed.

Source: US Marine Corps Intelligence Activity. *Iraq Culture Smart Card.* November 2004.

Figure 4-8. Examples of timelines of key dates

INTERPRET INFORMATION

4-37. Interpretation is an objective mental process based on common sense, life experience, military knowledge covering both enemy and friendly forces and existing information and intelligence. This mental process involves the identification of new activity and a postulation regarding the significance of that activity. The process also results in an understanding of the activity as viewed from the enemy's or source's perspective.

CULTURAL AWARENESS

4-38. A challenge in the intelligence operations is to interpret foreign military and political objectives, capabilities, needs, and actions without viewing the research or collected information through the American cultural lens that injects American cultural bias and preconceived ideas into our analysis. Instead, analysts need to recognize their cultural bias and attempt to mitigate its effects through cultural awareness. Cultural awareness enables the analyst to consider the perspective of the enemy, the local population, or other non-American perspective when planning research, performing analysis, and interpreting the results of analysis. Quite literally, analysts should ask: "How will the enemy perceive this development, and therefore what is he likely to do next?" rather than "How would we (the US) perceive this development, and how would we respond?" In military lexicon, analysts need to think "red," not "blue."

4-39. In essence, it is important to consider, if not understand, foreign perception of the US, its armed forces, and its operations when attempting to determine the enemy's or civil population's objectives and probable actions. Moreover, many other countries, organizations, or potential enemy factions depend on open sources for their intelligence. Our understanding of what others perceive, therefore, needs to be derived from the same material. This approach will help avoid costly, mistaken assumptions about the enemy during mission planning and execution, and its importance is reflected by the Army's heightened interest in raising the level of cultural awareness among today's troops.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

4-40. IPB is a technique for analyzing and interpreting the results of analysis in a specific operational environment, normally from the enemy's perspective. It builds on the baseline knowledge and databases created during research and the development of GMI products such as the operational environment assessment. The technique supports the development and integration of intelligence during the MDMP. Applying the IPB technique helps the G2/S2 staff support the commander in applying and protecting his forces at critical points in time and space in the operational environment. The G2/S2 staff uses IPB to describe the operational environment in which the unit is operating and the effects of the environment on the unit's operations. The IPB technique supports the G2/S2 staff in identifying enemy capabilities, strengths, weaknesses, probable objectives, and potential COA. IPB also addresses the civil considerations of manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within an AO on the conduct of military operations.

4-41. During IPB, it is in the "Determine Threat Courses of Action" step that the analyst interprets the results of analysis to reach an objective conclusion. The results of this step which drive the MDMP are valid only if the analyst established a good foundation during the first three steps of the IPB technique. Given the characteristics of the operational environment, coupled the enemy's capabilities, what are the enemy's likely objectives and the COAs? The analyst develops COA models that depict the available enemy COAs. The enemy COAs that the analyst develops in this step are the products the G2/S2 staff will use to portray the enemy in the MDMP and monitor during situation development. The analyst cannot produce these COAs and effectively predict the enemy COAs, unless he—

- Thoroughly considers what the enemy is capable of and what he prefers to do in like situations if unconstrained by the operational environment.
- Identifies the physical limits of the AO and AOI.
- Identifies the characteristic of the operational environment that might affect the operation.
- Understands the friendly mission throughout the time duration of the operation.
- Identifies the opportunities and constraints the operational environment offers to enemy and friendly forces.

SITUATION DEVELOPMENT

4-42. Situation development is a technique for producing current intelligence by interpreting the activity or conditions within a specific operational environment or about a specific subject. The technique depends upon the products developed during IPB and the continuous monitoring of activities in the unit's area of intelligence responsibility (AOIR). The technique helps the G2/S2 staff to provide I&W; confirm enemy COAs; explain the enemy activity's relationship to the operational environment and US operations; and identify information gaps. The current intelligence products developed through the situation development technique help the unit commander to understand the current enemy situation within the context of the operational environment. The G2/S2 staff conducts situation development during the preparation for and execution of the unit's operations.

4-43. The analyst interprets the results of analysis against the predicted enemy COAs, civilian actions, and friendly situation. Interpretation includes verifying the existence or nonexistence of indicators. The lack of information relating to specific indicators may signify that the COA is incorrect. The lack of information or reporting may also point to either an information gap regarding one or more indicators, or to a deception effort. If the analyst identifies either of these situations then he must consider recommending adjustments to the ISR effort. Ultimately, the G2/S2 must determine the significance of the enemy and civilian information as it relates to the following basic questions:

- Does the information confirm or deny forecasted COAs?
- Does the information confirm or deny predicted objectives?
- Does the information identify new COAs and objectives?
- Does the information answer the commander's requirements?

REPORT RESULTS

4-44. The objective in reporting or presenting information is to provide relevant information to support planning, preparation, execution, and assessment of operations. Table 4-5 lists the three general methods that the staff uses to present information and meet its information objective. Digital systems contain standard report formats, maps, and mapping tools that assist the staff in presenting information in written, verbal, and graphic form. Audio and video systems like large format displays and teleconferencing systems enable the use of a combination of the methods in multimedia presentations.

Table 4-5. Reporting methods and products

METHOD	PRODUCTS
Written	Reports, Estimates, and Studies
Graphic	Charts, Overlays, and Situation Map
Verbal	Briefing (information, decision, mission, and staff)

WRITTEN REPORTS

4-45. Analysts reports information in accordance with unit SOPs and reporting guidance. Report formats include standardized reports such as the size, activity, location, unit, time, and equipment (SALUTE) report and specialized intelligence reports such as tactical report (TACREP) or information intelligence report (IIR). Analysts consider the following guideline when preparing reports:

- **Timely Information.** Upon recognition, report immediately time-sensitive information such as warning of hostile action against US and non-US civilians or US, allied, and coalition forces. Report the information in accordance with reporting guidance including, if authorized, directly to affected units. Do not delay reports for the sole purpose of assuring the correct format.
- **Relevant Information.** Reports should contain only relevant information. The information should answer or contribute to the answering of the IRs in the task or the request. Limiting reports to relevant information reduces the time and effort spent collecting, organizing, and transmitting reports. Send only lines of the report that contain new information or changes.
- **Complete Information.** Reports have prescribed formats to ensure completeness of transmitted information. The unit SOPs should outline the format for each report. It should also explain under what conditions to submit each report.

GRAPHIC DISPLAYS

4-46. The situation map (SITMAP) is the primary graphic display product within command posts and operations centers. An effective SITMAP ensures personnel do not get overwhelmed, improves decisionmaker confidence, and improves presentation of information. Personnel create analog and digital SITMAPs during the initial steps of the MDMP using existing databases and graphics from higher headquarters. They update the map with information received and retrieved during the preparation and execution of operations. Interaction with other staff sections and management of SITMAPs are essential to maintaining situational awareness and an accurate COP. In OSINT operations, this requires developing unclassified graphics or overlays that the intelligence staff can exchange with other staff sections, non-intelligence personnel, and open source collection personnel who normally operate in unclassified workspaces.

WEB-BASED REPORTS

4-47. Web-based reporting is an effective technique for disseminating written reports and graphics to multiple users both within and outside the AO. Through the website, the analysts can collaborate and provide visibility on the status of RFIs and production tasks. The analysts can also post information to technical databases that help personnel collect, process, and analyze information from open sources. Figure 4-9 provides an example of the format of a web-based OSINT report. The metadata accompanying the report in Figure 4-9 included—

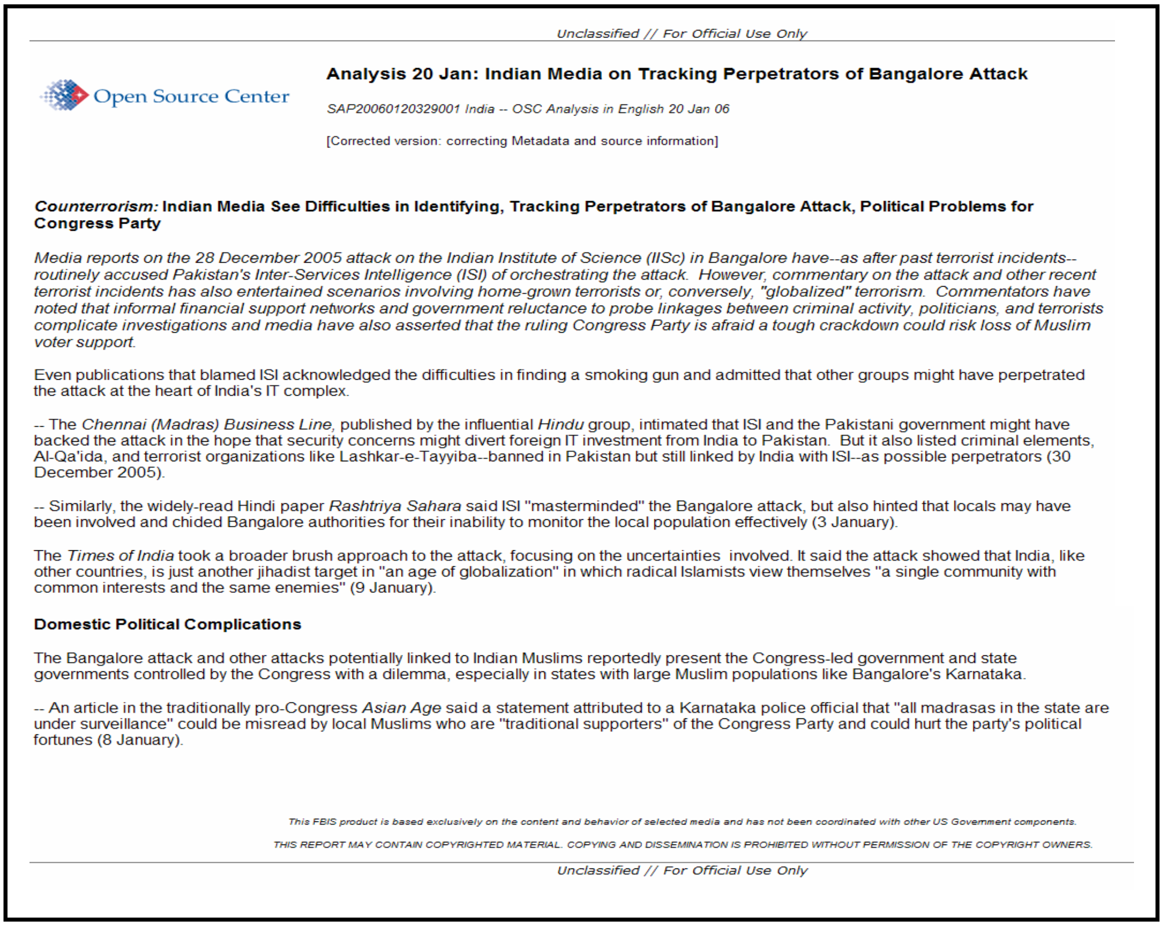
- Product Type.
- Source Date.
- Regions.
- Sub-Regions.
- Countries.
- Topics.
- Document Identification.

PRESENTATION GUIDELINES

4-48. The example in Figure 4-9 complies with standard guidelines for producing and reviewing intelligence reports. Regardless of the type of report and method of presentation, each report should always have a clear bottom-line message that addresses stated or anticipated intelligence requirements. The following are additional guidelines for web-based intelligence reports:

- Create precise, informative subject line or headline conveying key point of the report.
- Convey all key points in summary paragraph; content tracks with summary paragraph.
- State clear topic sentences for each key point.
- Present evidence clearly with compelling analytic statement; no internal contradictions.
- Present information logically with clear transitions between sections and sentences; no inclusion of extraneous "interesting" information.
- Highlight important information, changes, or trend comparison, up front.
- Highlight relevant aspects of open source environment to put source message or commentary into context.
- Anticipate reader's questions; note when relevant information is not found or addressed.
- Distinguish clearly between analyst's voice and that of open source.
- Use sound judgment when choosing sources (use primary sources versus secondary sources)
- Use appropriate source citations and dates.
- Use source descriptors or explanations about sources (including what is not known about a source) to put information into context.

- Remain faithful to the citation in its original meaning within context or to its grammar and syntax.
- Provide proper comparisons between events, people, open source treatments.
- Use appropriate use of multimedia; no "eye-candy."
- Use active voice whenever possible or appropriate.
- Use prescribed formats for margins and font.
- Observe prescribed stylistic rules, including transliteration rules.
- Review for misspellings or typographical errors and incorrect or awkward English grammar.



Unclassified // For Official Use Only

Open Source Center

Analysis 20 Jan: Indian Media on Tracking Perpetrators of Bangalore Attack

SAP20060120329001 India -- OSC Analysis in English 20 Jan 06

[Corrected version: correcting Metadata and source information]

***Counterrorism:* Indian Media See Difficulties in Identifying, Tracking Perpetrators of Bangalore Attack, Political Problems for Congress Party**

Media reports on the 28 December 2005 attack on the Indian Institute of Science (IISc) in Bangalore have--as after past terrorist incidents--routinely accused Pakistan's Inter-Services Intelligence (ISI) of orchestrating the attack. However, commentary on the attack and other recent terrorist incidents has also entertained scenarios involving home-grown terrorists or, conversely, "globalized" terrorism. Commentators have noted that informal financial support networks and government reluctance to probe linkages between criminal activity, politicians, and terrorists complicate investigations and media have also asserted that the ruling Congress Party is afraid a tough crackdown could risk loss of Muslim voter support.

Even publications that blamed ISI acknowledged the difficulties in finding a smoking gun and admitted that other groups might have perpetrated the attack at the heart of India's IT complex.

-- The *Chennai (Madras) Business Line,* published by the influential *Hindu* group, intimated that ISI and the Pakistani government might have backed the attack in the hope that security concerns might divert foreign IT investment from India to Pakistan. But it also listed criminal elements, Al-Qa'ida, and terrorist organizations like Lashkar-e-Tayyiba--banned in Pakistan but still linked by India with ISI--as possible perpetrators (30 December 2005).

-- Similarly, the widely-read Hindi paper *Rashtriya Sahara* said ISI "masterminded" the Bangalore attack, but also hinted that locals may have been involved and chided Bangalore authorities for their inability to monitor the local population effectively (3 January).

The *Times of India* took a broader brush approach to the attack, focusing on the uncertainties involved. It said the attack showed that India, like other countries, is just another jihadist target in "an age of globalization" in which radical Islamists view themselves "a single community with common interests and the same enemies" (9 January).

Domestic Political Complications

The Bangalore attack and other attacks potentially linked to Indian Muslims reportedly present the Congress-led government and state governments controlled by the Congress with a dilemma, especially in states with large Muslim populations like Bangalore's Karnataka.

-- An article in the traditionally pro-Congress *Asian Age* said a statement attributed to a Karnataka police official that "all madrasas in the state are under surveillance" could be misread by local Muslims who are "traditional supporters" of the Congress Party and could hurt the party's political fortunes (8 January).

This FBIS product is based exclusively on the content and behavior of selected media and has not been coordinated with other US Government components.

THIS REPORT MAY CONTAIN COPYRIGHTED MATERIAL. COPYING AND DISSEMINATION IS PROHIBITED WITHOUT PERMISSION OF THE COPYRIGHT OWNERS.

Unclassified // For Official Use Only

Figure 4-9. Example of a web-based open source intelligence report

OTHER CONSIDERATIONS

4-49. Considerations in reporting OSINT include—

- Write-to-release; without compromising security, write at the lowest classification level to facilitate the widest distribution of the intelligence.
- Separate paragraphs and paragraph classifications markings to distinguish unclassified OSINT intelligence in classified reports.

- Tearline report formats to facilitate the separation of classified and unclassified information for users operating on communications networks of differing security levels.
- Perform a sensitive check to ensure the report content and distribution is not counterproductive to effective Joint, Interagency, and Multinational operations.
- Provide collector and analyst comments on the source reliability and information credibility.
- Provide capability to notify users of changed or cancelled reports.

This page intentionally left blank.

Chapter 5

Collect and Process Information

5-1. Distinct from open source research, open source collection consists of the unintrusive collection of publicly available information in the course of authorized and assigned missions with the intent to use or retain the information for foreign intelligence or CI purposes. Publicly available information includes, but is not limited to, foreign language documents, radio and television broadcasts, Internet sites, and public speaking forums.

5-2. Collection responds to reconnaissance and surveillance missions levied on intelligence and non-intelligence organizations through tasks and requests. Focused and synchronized through collection management, open source collection resources know who, what, when, where, and why to collect publicly available information and essential metadata (date, time, location, language, frequency, station identification, newspaper name, author). Essential metadata includes temporal and geospatial data that enables tracking and visualization of activity, changes in the operational environment, and coverage of reconnaissance and surveillance resources.

CONDUCT TARGET DEVELOPMENT

5-3. If not provided in the OPORD, analysis of the task statement identifies the target (information source), their target systems (media of communications), and reporting guidance (Table 5-1). During target development, analysts or collectors research the target and target systems to determine the target components and the elements. They also identify the target characteristics or technical data of each target element to support synchronization of collection between echelons and subordinate organizations as well as tasking individual collectors or programming collection systems. In addition, the results of target research and analysis provide the basis for management of collection assets and criteria for assessing the effectiveness of collection.

Table 5-1. Target development

STEP	DESCRIPTION
Identify Target System	Identify the target systems that support the dissemination of public information in the area of operations or about the area of interest (see Table 2-1 through 2-4).
Identify Target Components	Identify the target components of the target system. A system component is a set of targets within a target system performing a similar function. Example - The components of a broadcast target system are radio and television networks.
Identify Target Elements	Identify the target elements. A target component element is the smallest identifiable activity or function of a target component. Just as a components are essential parts of a target system, target elements are the essential parts of a target component. Example - The elements of television include satellite and terrestrial broadcasts.
Identify Target Characteristics	Identify the target characteristics. A target characteristic is an observable feature of the target element. These characteristics are the metadata that collection resources need to detect, identify, locate, and track a target. Example - The characteristics of a terrestrial television broadcast include the audio standard, the broadcast schedule, the channel, the frequency, the radio reception area, the regional video format, the station or network ownership, the target audience language, the satellite broadcast service provider, and the satellite reception “footprint.” It is also important to identify whether the radio or television broadcast is available on an Internet site or through a cable television service provider.

COLLECT INFORMATION

5-4. Once positioned, C2 personnel task the appropriate collection and processing assets based on their evaluation and correlation of target characteristics, team capabilities, and team availability. The tasks and requests describe the collection objective and reporting guidance. In addition to reporting guidance, SOPs describe what information and essential metadata (date, time, location, language, frequency, station identification, newspaper name, author, meeting chairperson) to retain and report.

5-5. Essential metadata includes temporal and geospatial data that enables tracking and visualization of the collected information and metadata in time and space. SOPs also provide instructions on how to properly label collected information; keep accurate files and logs, and transfer or destroy collected information and associated records.

5-6. Collection personnel conduct an initial reconnaissance of the information environment followed by surveillance of specific targets (Table 5-2). As required, collection personnel forward collected information to linguists, DOCEX personnel, or other elements for processing. They report time-sensitive information and other reportable information to control personnel. Control personnel evaluate the collected and processed information then disseminate the relevant, reportable information in accordance with the reporting guidance in the task statement or RFI (Figure 5-1). SOPs should provide instructions on how to properly label collected information; keep accurate files and logs, and transfer or destroy processed information and associated records.

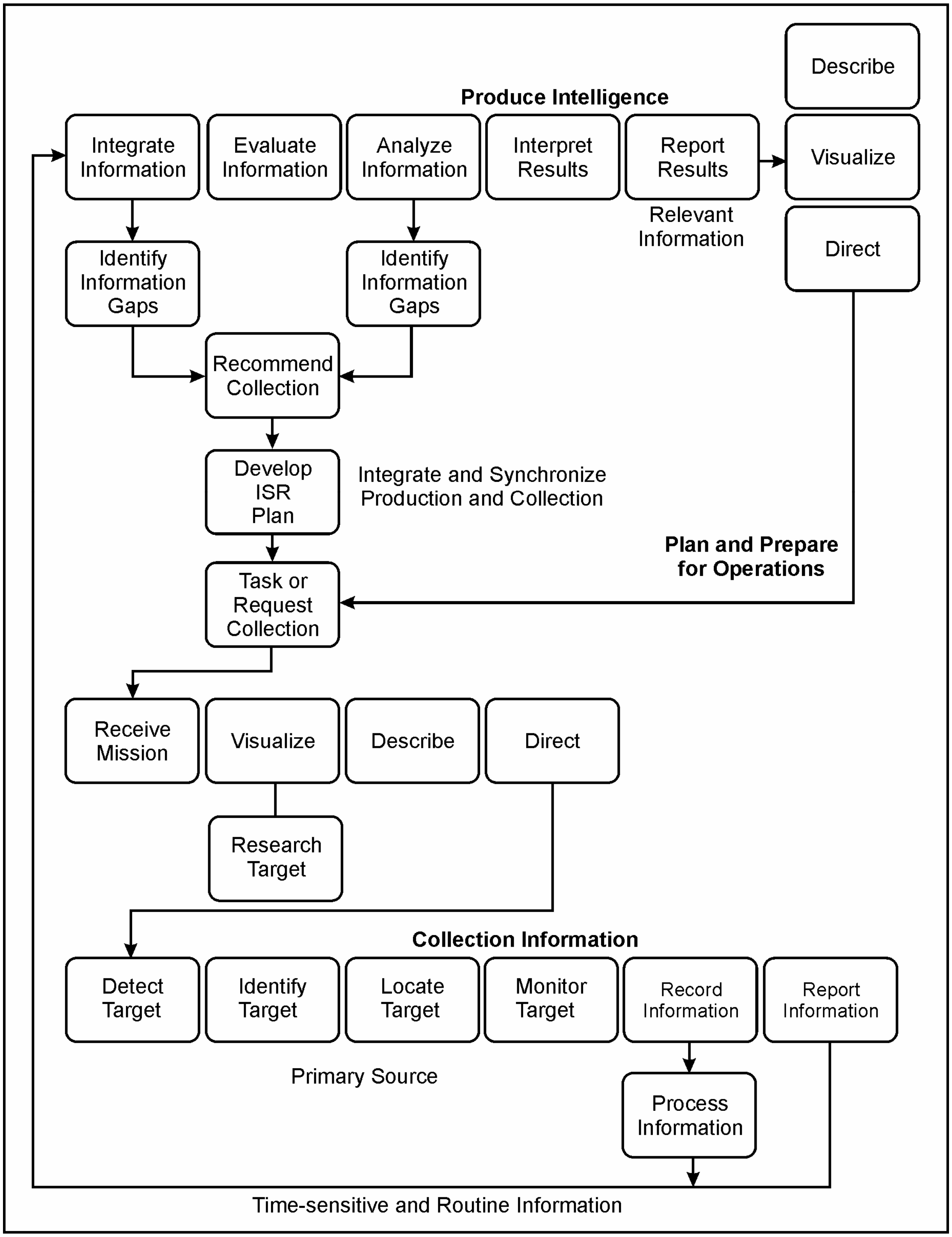


Figure 5-1. Collect and process information

Table 5-2. Basic collection procedures

PROCEDURE	DESCRIPTION
Detect	Detect the target by external target characteristics such as— • Publication type or format. • Frequency, channel, or program. • Physical description.
Identify	Identify the target based on— • Language and content. • Network, sation, or program name. • Title, name, company name, logo, nickname.
Locate	Locate the target by— • References in the content. • Emitter mapping. • URL address. Location and time of activity are essential to displaying and understanding geospatial and temporal relationships.
Monitor	Monitor the target for information and metadata that meets the reporting criteria in the collection task— • Aperiodically as information becomes available. • Periodically during specific timeframes. • Fulltime to support I&W or ensure complete collection of all information.
Record	Record collected information by— • Tagging and bagging documents. • Photographing graffiti, large objects, and activity. • Saving audio and video to analog tape or digital files. • Saving or downloading webpage content. • Transferring handwritten meeting notes to the text files. Include data and comments on the circumstance of collection such a the vendor's name and location; background activity and sounds; pop-up advertisements and links; audience behavior.
Report	Report time-sensitive information by— • Voice message with follow-on text message report. • Text message. Reports may include extract of the content if directed in the reporting guidance or required to enhance understanding of the reported information. Store and forward collected information in accordance with unit SOPs.

5-7. Reconnaissance missions require the collection personnel to detect, identify, locate, and report all sources of publicly available information in the AOI. The AOI may be a specific geographic area, portion of the radio frequency spectrum, or family of foreign languages. The initial reconnaissance mission confirms the presence of planned targets and establishes a baseline of activity or information sources within the AOI. The baseline provides an initial level of understanding that supports the identification of

HVTs and future surveillance missions. Periodically, collection personnel search the AOI to verify the baseline and locate new sources of information.

5-8. After their initial reconnaissance, collection personnel begin surveillance of the targets in the collection task, as well as approved new targets identified during reconnaissance. Each collection task for surveillance missions includes the SIRs or collection objectives, a priority for collection, timeframe of expected activity, latest (or earliest) time or event the information is of value, and reporting instructions. Surveillance missions require collection personnel to detect, identify, and locate the target; monitor and record the target activity or content; and report the content and characteristics (metadata) of the target.

PUBLIC SPEAKING FORUMS

5-9. Open source collection personnel use the basic collection procedures described in Table 5-2 to collect information during public speaking forums (see Table 2-1). In addition, C2 personnel brief and debrief collection personnel on the event, the speakers, specific information required, and other observed activity. In permissive or corporative environments, personnel attend conferences, lectures, public meetings, and working groups with the consent or invitation of the event's sponsor. Attending these and similar events are opportunities to build relationships with non-military professionals and their organizations.

5-10. In all environments, collection personnel require a thorough understanding of the local culture and laws to ensure their activities are unintrusive and do not violate local customs or laws. During tactical operations, open source collectors face situations similar to those of war correspondents and photojournalists. In those situations, the collector requires situational awareness as well as cultural awareness since overt monitoring and recording of public speaking forums may lead to—

- Modification of speaker's message.
- Expulsion from the event or area.
- Denial of access to future events.
- Assault on the collector or the collection equipment.
- Hostile opinion or actions against US operations and personnel.

PUBLIC DOCUMENTS

5-11. Open source collection personnel use the basic collection procedures described in Table 5-2 to collect documents (see Table 2-2). Like collecting information at public speaking forums, personnel must be aware of the local environment and use a collection technique that is unintrusive and appropriate for the situation. These techniques include but are not limited to—

- Copying or photographing documents available in public forums such as town halls, libraries, and museums.
- Finding discarded documents in a public area such as streets, markets, and restrooms.
- Photographing documents in public areas such as banners, graffiti, posters, and other large documents.
- Purchasing documents directly from street vendors, newspaper stands, book stores, and publishers.
- Purchasing documents through a third party such as a wholesale distributor or book club.
- Receiving documents upon request without charge from the author, conferences, trade fairs, direct mail advertising.

5-12. Once collected, the collection personnel tag each document and complete an inventory of a group of documents. Completing the document tag and inventory establishes accountability and traceability for the collected documents. The collection personnel should protect the document from damage by placing the documents in a weatherproof container (box or plastic bag). If a DD Form 2745 (Enemy Prisoner of War

[EPW] Capture Tag) is not available, record the required data on any piece of paper or other field expedient method. As a minimum, the collection personnel should record the following information:

- Collecting unit identification.
- Date and time of collection in date-time group (DTG) format.
- Location of collection including 8-digit map coordinates and a detailed description of the location.
- Identity of the person or organization that provided the document.
- Summary of the circumstances of collection.

5-13. If not already completed, collection personnel inventory all collected documents to ensure accountability. If the document has a tag, the personnel use the information on the tag to complete the document inventory. They should indicate attempts to process and report information on the inventory. This prevents unnecessary duplication of effort by document processing personnel. The format for a document inventory is in accordance with unit SOPs and reporting guidance, but it should contain at least the following information:

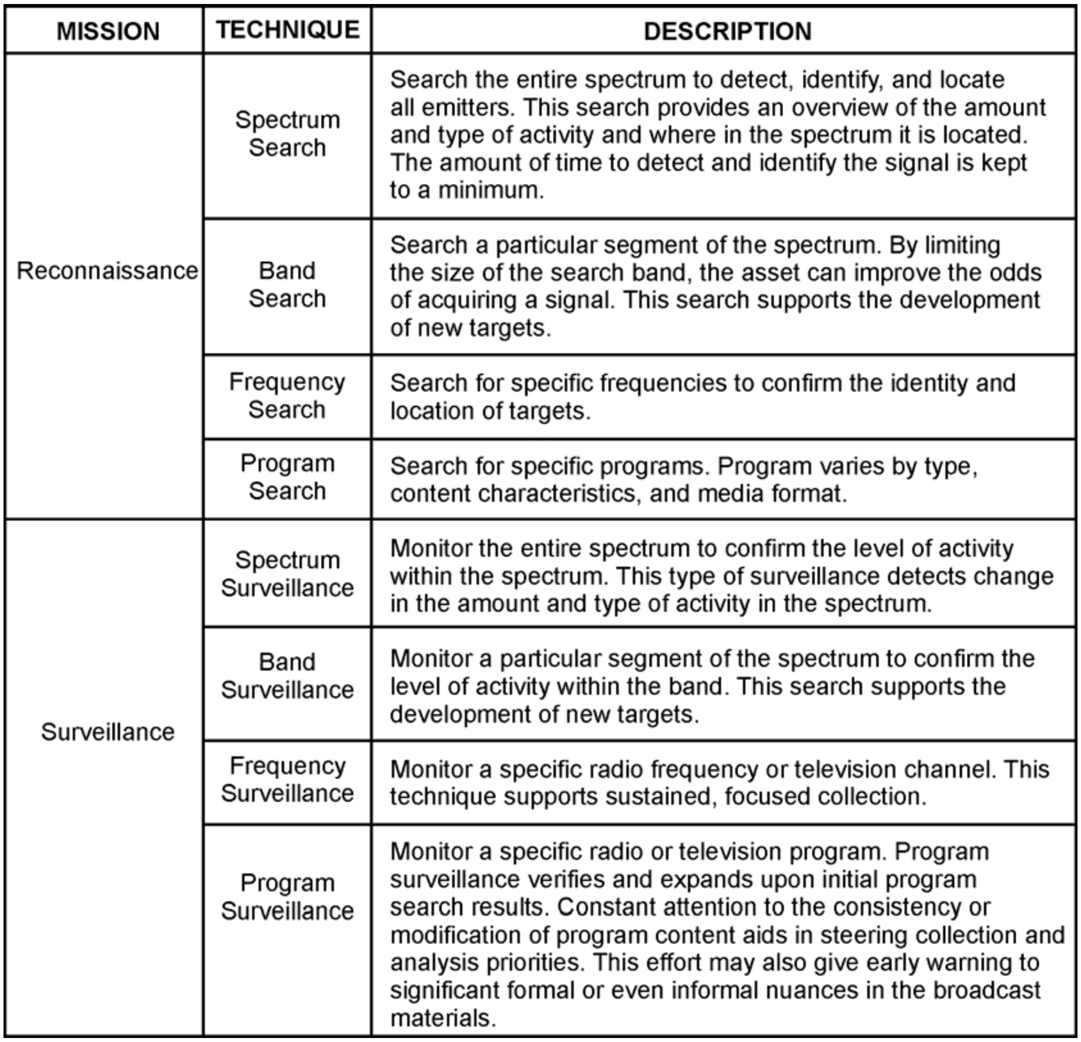
- Collecting unit identification.
- Collection date, time, and location.
- List of documents, by serial number if using DD Form 2745, Part C.
- Destination unit identification.
- Screening category, if applicable.
- Remarks including serial number and DTG of reports based on the documents.

PUBLIC BROADCAST

5-14. Regional bureaus of the DNI OSC collect, process, and report on international and regional broadcast networks in accordance with standing and ad hoc open source IRs. Their coverage of international and regional broadcasts enables deployed Army organizations to use, if necessary, their tactical assets to collect and process information from local radio and television broadcast targets that are only accessible from within the AO. Close coordination between the OSC, the JIOCs, the theater-level Army intelligence centers, and the deployed unit ensure the synchronization of collection and the dissemination of information from public broadcasts between echelons.

5-15. During collection operations, there are four primary reconnaissance techniques to search for public broadcasts (Table 5-3). For best results, collection personnel use these techniques in combination rather then independently. The selection of the techniques depends on the mission, the number of collection personnel, and their capabilities. Following the initial reconnaissance, collection personnel begin surveillance of public broadcast targets. During surveillance, collection personnel detect, identify, and locate the broadcast signal; monitor and record the broadcast content; and report the content and characteristics (metadata) of the broadcast. There are four primary surveillance techniques to monitor broadcasts. As during reconnaissance, collection personnel use the techniques in combination and the specific techniques depend on the mission, the number of collection assets, and their capabilities.

Table 5-3. Broadcast reconnaissance and surveillance techniques



MISSION	TECHNIQUE	DESCRIPTION
Reconnaissance	Spectrum Search	Search the entire spectrum to detect, identify, and locate all emitters. This search provides an overview of the amount and type of activity and where in the spectrum it is located. The amount of time to detect and identify the signal is kept to a minimum.
	Band Search	Search a particular segment of the spectrum. By limiting the size of the search band, the asset can improve the odds of acquiring a signal. This search supports the development of new targets.
	Frequency Search	Search for specific frequencies to confirm the identity and location of targets.
	Program Search	Search for specific programs. Program varies by type, content characteristics, and media format.
Surveillance	Spectrum Surveillance	Monitor the entire spectrum to confirm the level of activity within the spectrum. This type of surveillance detects change in the amount and type of activity in the spectrum.
	Band Surveillance	Monitor a particular segment of the spectrum to confirm the level of activity within the band. This search supports the development of new targets.
	Frequency Surveillance	Monitor a specific radio frequency or television channel. This technique supports sustained, focused collection.
	Program Surveillance	Monitor a specific radio or television program. Program surveillance verifies and expands upon initial program search results. Constant attention to the consistency or modification of program content aids in steering collection and analysis priorities. This effort may also give early warning to significant formal or even informal nuances in the broadcast materials.

INTERNET SITES

5-16. Like international and regional broadcasts, the regional bureaus and local collection assets of the DNI OSC collect, process, and report on international and regional news posted or webcast on Internet sites. The JIOCs and the theater level Army intelligence centers also search and monitor the Internet for local, regional, and international news and other information on AOR and associated AOI. These sustained collection activities and the nature of the Internet enable deployed Army organizations to rely on support relationships with these external organizations for Internet collection. If the deployed organizations determine that an organic Internet site collection is necessary then they work closely with the supporting theater level Joint and Army intelligence centers to deconflict targets, synchronize coverage, and disseminate information between echelons as well as the OSC.

5-17. The initial mission of collection personnel is to conduct a reconnaissance of the Internet (Table 5-4). While broadcast collection is primarily surveillance, reconnaissance missions dominate Internet collection. The Internet is a dynamic information environment consisting of stationary and moving targets (sites) containing a mixture of old and new content. Reconnaissance is required to locate new sites and information. The reconnaissance or search uses the basic techniques and procedures described in Appendix F. For OPSEC, a commander of a major subordinate command may approve nonattributable Internet access to support authorized open source collection activities. The recommended system for nonattributable access is the Intelink-SBU. A commercial Internet service provider can provide nonattributable access; however, use of a local provider comes with its own OPSEC risks.

PROCESS INFORMATION

5-18. If required, collection personnel or a separate processing element transforms collected information into a form suitable for analysis. The degree that the tactical level sites process the collected information depends on the site's resources and its mission. When the requirements exceed organic and attached processing capabilities, the unit can request support from the NGIC's Reach Language Support Program or the National Media Exploitation Center (NMEC).

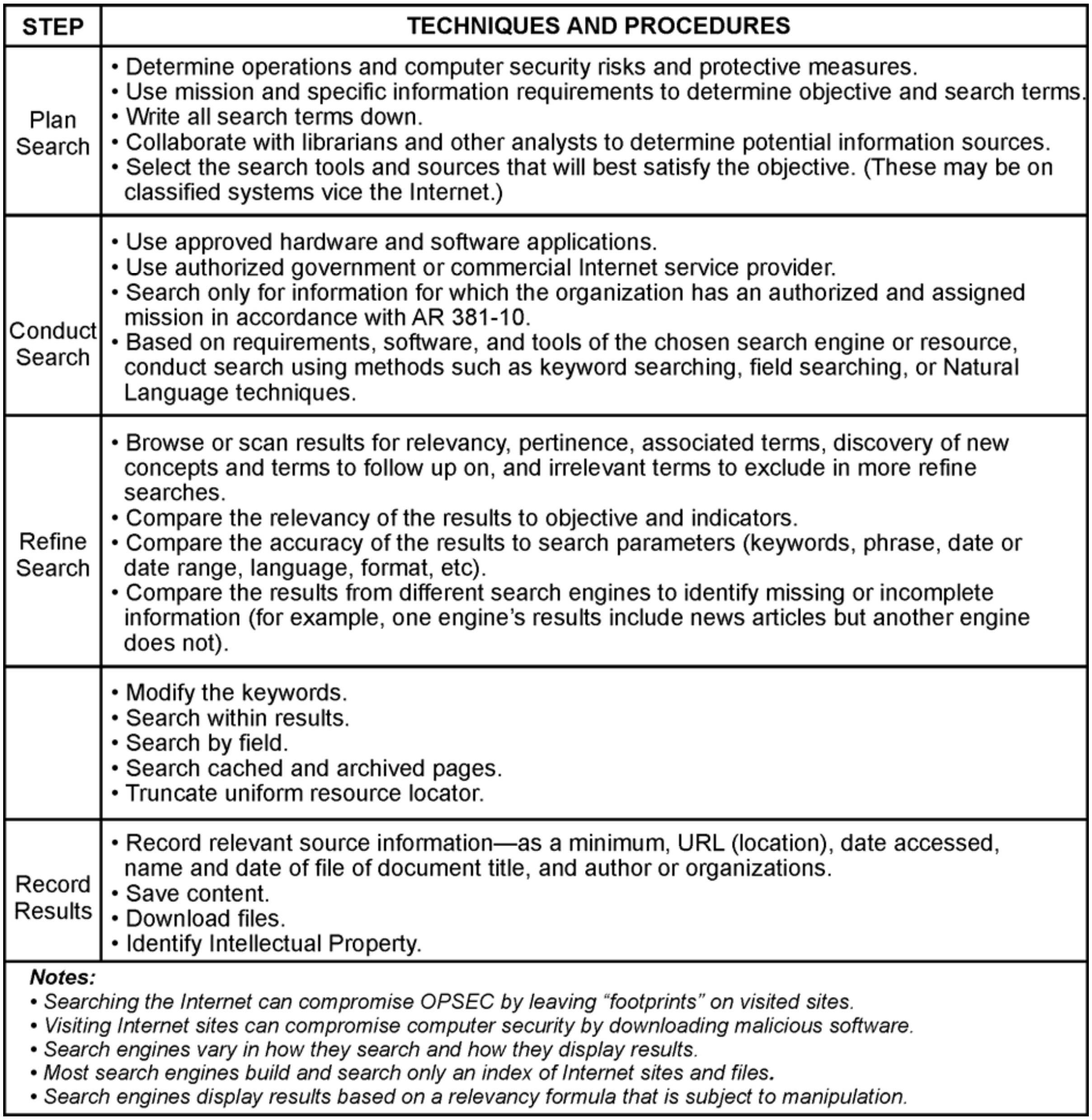
5-19. The majority of document processing involves digitizing, transcribing, and translating non-English graphics, recordings, and textual documents into English text format. Language capability is therefore essential to processing non-English language documents. In addition, language-based processing activities require procedures and management to ensure transcripts and translations are timely, accurate, complete, and free of bias.

5-20. At the tactical level, processing personnel may not possess the assets for digital media extraction; computer forensics; voice recognition and identification; comparative analysis of video content; and cryptanalysis. The skills, knowledge, and equipment for specialized processing are available at Intelligence Community organizations. Units can request support from DIA, NGIC, CIA, the Federal Bureau of Investigation (FBI), and other Intelligence Community organizations to use specialized techniques and procedures to extract additional information from the collected audio and video information. Application of specialized processing techniques and procedures may require the classification of the processed information and restriction of its distribution.

DIGITIZE INFORMATION

5-21. If not already in a digital format, processing personnel create a digital record of documents by scanning or taking a digital photograph. Personnel must annotate or otherwise include all the information about the document with digitized documents to ensure document accountability and traceability. Specifically, SOPs should provide instructions on how to properly label processed information, keep accurate files and logs, and transfer or destroy processed information and associated records. Digitization enables the dissemination of the document to external database (for example, HARMONY) and organizations where linguists such as those in the NMEC, the Army's Reach Language Support Program, and the Joint Reserve Intelligence Center-Leavenworth can transcribe and translate the document. Digitization also enables the use machine translation tools to screen documents for key words, names, and phrases as well as to provide a rough translation or gist of the document.

Table 5-4. Internet search techniques and procedures



STEP	TECHNIQUES AND PROCEDURES
Plan Search	• Determine operations and computer security risks and protective measures. • Use mission and specific information requirements to determine objective and search terms. • Write all search terms down. • Collaborate with librarians and other analysts to determine potential information sources. • Select the search tools and sources that will best satisfy the objective. (These may be on classified systems vice the Internet.)
Conduct Search	• Use approved hardware and software applications. • Use authorized government or commercial Internet service provider. • Search only for information for which the organization has an authorized and assigned mission in accordance with AR 381-10. • Based on requirements, software, and tools of the chosen search engine or resource, conduct search using methods such as keyword searching, field searching, or Natural Language techniques.
Refine Search	• Browse or scan results for relevancy, pertinence, associated terms, discovery of new concepts and terms to follow up on, and irrelevant terms to exclude in more refine searches. • Compare the relevancy of the results to objective and indicators. • Compare the accuracy of the results to search parameters (keywords, phrase, date or date range, language, format, etc). • Compare the results from different search engines to identify missing or incomplete information (for example, one engine's results include news articles but another engine does not).
	• Modify the keywords. • Search within results. • Search by field. • Search cached and archived pages. • Truncate uniform resource locator.
Record Results	• Record relevant source information—as a minimum, URL (location), date accessed, name and date of file of document title, and author or organizations. • Save content. • Download files. • Identify Intellectual Property.

Notes:

- *Searching the Internet can compromise OPSEC by leaving "footprints" on visited sites.*
- *Visiting Internet sites can compromise computer security by downloading malicious software.*
- *Search engines vary in how they search and how they display results.*
- *Most search engines build and search only an index of Internet sites and files.*
- *Search engines display results based on a relevancy formula that is subject to manipulation.*

5-22. If necessary, processing personnel recover documents by cleaning soiled documents, reassembling document fragments, decrypting coded documents, and extracting information from electronic devices or storage media. Extracting information from electronic devices and storage media is done at the NMEC, a Joint Document Exploitation Center, or other site with specialized training, equipment, and software. At these sites, the processing personnel work with TECHINT personnel to process electronic devices or storage media. In addition to special resources, processing at the DOCEX sites prevents the introduction of corrupt, malicious, and unstable software from entering US communications and processing networks.

TRANSCRIBE AND TRANSLATE INFORMATION

5-23. Transcription and translation capabilities are essential to processing non-English publicly available information. Military, government civilian, and contract linguists must possess source language and, for translators, English language skills and subject matter knowledge commensurate with the materiel they are processing. In addition, language-based processing activities require procedures to ensure transcripts and translations are accurate, complete, and free of bias.

- **Transcription.** A transcript is a verbatim, native language rendering of the information in an audio or video recording. Both listening and writing proficiency in the source language are essential for an accurate transcript. A transcript is extremely important when the English language skills of the processing personnel are inadequate for authoritative, direct translation from audio or video into English text. During processing, the linguist transcribes all information in the recording into a standardized format. The transcript, particularly of video files, includes descriptions of the activity, background, and conditions that the transcriber hears in the audio and observes in the video.
- **Translation.** A translation, unlike a transcript, is not verbatim but an approximation of the literal and implied meaning of the written language. Bilingual competence is a prerequisite for creating any translation. The linguist must be able to read and comprehend the source language, write comprehensibly in English, and choose the equivalent expression in English that both fully conveys and best matches the meaning intended in the source language. During processing, a linguist creates an extract, a summary, or a full translation of the original document or transcript. The linguist provides an extract or summary when time and resources are insufficient for a full translation or the content does not meet reporting criteria. A full translation requires the linguist to translate all information into a standardized format.

5-24. Processing personnel transcribe audio and video recordings from media storage devices into text format. For processing of non-English recordings, transcription is extremely important when the English language skills of the processing personnel are inadequate for authoritative, direct translation into English. The transcriber uses native font or transliteration to represent the spoken language in the recording. The transcript, particularly of video files, includes descriptions of the activity, setting, and conditions that the transcriber hears in the audio and observes in the video.

5-25. During transcription, a linguist provides either an extract or a full translation of the original audio or video recording. The linguist provides an extract of the recording when time and resources are insufficient for a full transcript or the content does not meet reporting criteria. A full transcript requires the linguist to render all information in the recording into a standard transcription report format. The linguist uses online dictionaries, gazetteers, and working aids to improve the transcript. Once completed the linguist stores or forwards the transcript to a quality control linguist.

5-26. Processing personnel translate document content and transcripts into English-language text format. To ensure consistency and quality, the processing team applies a standard, three-phase process to translate spoken and written information into English. During processing, a linguist provides an extract, summary, or a full translation of the original document or transcript. The linguist provides an extract or summary of the document or transcript when time and resources are insufficient for a full translation or the content does not meet reporting criteria. A full translation requires the linguist to translate all information in the document or transcript into a standard translation report format. The linguist uses online dictionaries, gazetteers, and working aids to improve the translation. Once completed the linguist stores or forwards the translation to the quality control linguist.

5-27. Professional level linguists review each transcription and translation to ensure consistency with reporting standards and quality of the translation. With some exceptions, a US Government linguist should review all information that a non-US linguist processes. Exceptions include operations involving long-term multinational or coalition partners of the US and US contractors with the requisite skills and the command's confidence. Each transcript and translation undergoes two levels of review:

- **Quality Control.** During quality control, a qualified linguist ensures that the transcript or translation is accurate and clearly expresses the meaning of the original recording or document. The quality control linguist reviews the transcript or translation to ensure that it is accurate, complete, free of bias, and in accordance with reporting standards. The linguist returns the transcript or translation for correction or personally adds missed content, corrects minor errors, and fixes minor format errors. Upon completion of quality control, the transcript or translation is available for analysis.
- **Quality Assurance.** During quality assurance, a qualified individual reviews the transcript or translation to ensure that it contains all required information and, if a translation, reads naturally in English. Once reviewed, the quality assurance linguist saves the completed transcript or translation to the local database. If authorized, the quality assurance linguist disseminates the transcript or translation to external databases.

REPORT INFORMATION

5-28. Collection and processing personnel report information in accordance with their unit SOPs and reporting guidance. Upon recognition, they report time-sensitive information such as I&W of hostile action against US forces to their C2 element. If authorized, they report time-sensitive information directly to affected units. Collection personnel use LANs to transfer text and audio and video files requiring processing to personnel for transcription, translation, or other processing. Collection and processing personnel use wide area networks (WANs) to disseminate unprocessed and processed information to external databases and organizations.

5-29. Collection and processing personnel use basic reporting procedures to identify, evaluate, and report time-sensitive information and other information that meets reporting criteria. These reports focus primarily on conveying facts but can include comments on the source's reliability and the information's credibility. The following describes the basic procedure for reporting information of intelligence value.

- **Reportable Information.** Collection and processing personnel identify information meeting the reporting criteria in the task or request. As a minimum, they identify the basic facts (who, what, where, and when) in the information. If they have the time, analytic skills, target knowledge, and situational understanding then they use basic analysis techniques and procedures to reach conclusions about the meaning (why) of the information.
- **Report Guidelines.** Report formats include standardized reports such as the SALUTE report, TACREP, information intelligence report, or webbased transcription and translations reports. Personnel should consider the following guideline when preparing reports:
  - **Timely Information.** Upon recognition, report immediately time-sensitive information such as warning of hostile action against US and non-US civilians or US, allied, and coalition forces. Report the information in accordance with reporting guidance including, if authorized, directly to affected units. Do not delay reports for the sole purpose of assuring the correct format.
  - **Relevant Information.** Reports should contain only relevant information. The information should answer or contribute to the answering of the IRs in the task or the request. Limiting reports to relevant information reduces the time and effort spent collecting, organizing, and transmitting reports. Send only lines of the report that contain new information or changes.
  - **Complete Information.** Reports have prescribed formats to ensure completeness of transmitted information. Unit SOPs should outline the format for each report. The SOPs should also explain under what conditions to submit each report.

This page intentionally left blank.

Appendix A

Asian Studies Detachment

A-1. The Asian Studies Detachment serves as a model for the COCOM'S or ASCC's theater level OSINT (Figure A-1). Subordinate to the 441st MI Battalion of the INSCOM's 500th MI Brigade, the Detachment began in 1947, when it stood up as the Research and Analysis Group, Town Plan Group, and Cartographic Unit of the G2 Geographic Section under General MacArthur's General Headquarters in downtown Tokyo. The unit has been located at Camp Zama since 1974 and known as the US Army Asian Studies Detachment since October 1981.

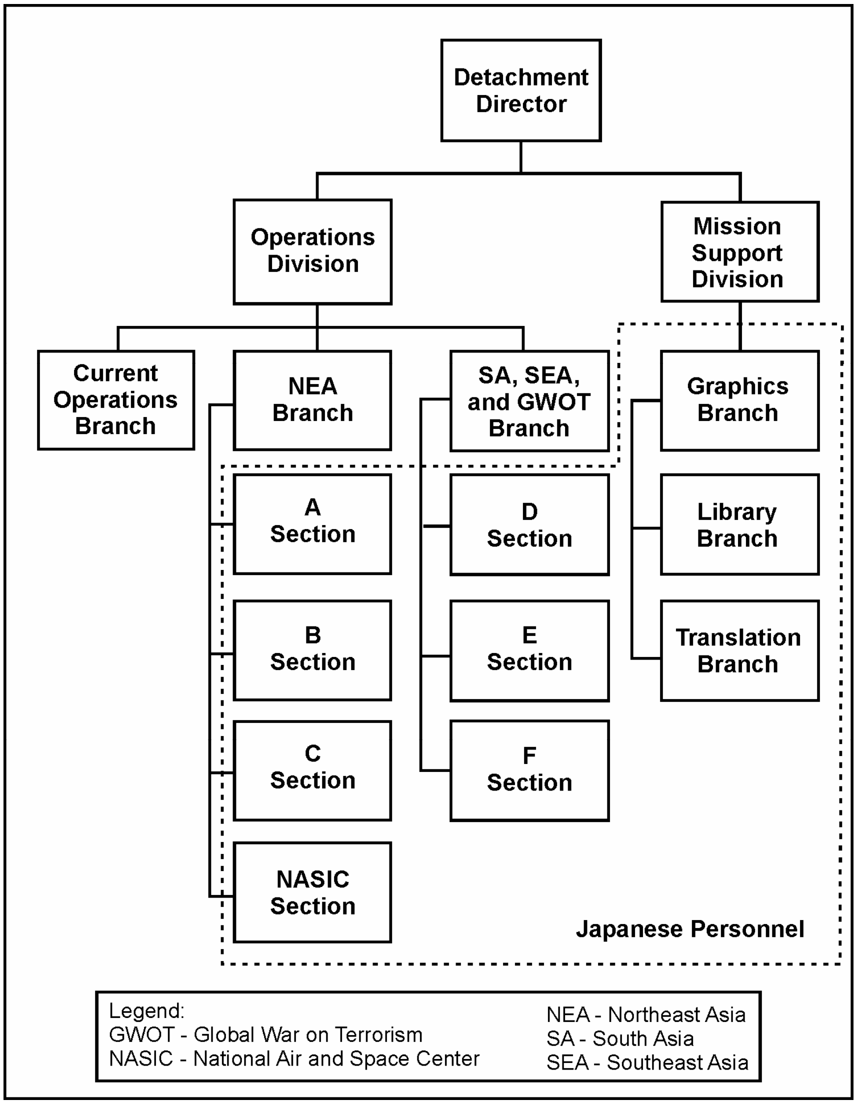


Figure A-1. Asian Studies Detachment

MISSION

A-2. The Asian Studies Detachment's mission is to collect, analyze, and report publicly available information from foreign open sources in response to theater and National level intelligence requirements. The unit exists primarily to support the tactical intelligence needs of US Army Pacific Command (USAPACOM), but its products serve all Services, COCOMs, DOD intelligence agencies; non-DOD customers such as the DNI OSC, the FBI, the Department of State (DOS); and nongovernmental strategic "think tanks." The Asian Studies Detachment strives to set the standard for providing timely and value-added reporting on Asia, derived from the fullest possible exploitation of foreign open sources.

ORGANIZATION

A-3. The Asian Studies Detachment consists of DA civilians (DACs), Japanese Nationals, US contractors, and a varying number of Army Reservists and National Guardsmen. Many of staff bring with them extensive experience from private sector and government organizations in various countries. The DACs are Japanese linguists. The Asian Studies Detachment's Japanese National employees, all funded and contracted to the US Government by the Japanese government, make up the bulk of the operation (Figure A-1). As the unit's analysts, translators, librarians, and administrative support personnel, the Japanese personnel accomplish the Asian Studies Detachment's collection, analysis, and reporting mission. All together, they provide the Asian Studies Detachment with language expertise in Bengali, Burmese, Chinese, Indonesian, Japanese, Khmer, Korean, Hindi, Malaysian, Nepali, Russian, Tagalog, Thai, Uygur, and Vietnamese, as well as a handful of European languages.

OPERATIONS

A-4. The Asian Studies Detachment subscribes to over 400 international publications in hardcopy and digital format. Not all open source materials used by the Asian Studies Detachment, however, are acquirable through subscription. The Asian Studies Detachment obtains other materials through memberships in international research and friendship organizations, and also by direct purchase from foreign bookstores and publishing houses.

A-5. The Asian Studies Detachment is not a translation unit. On the contrary, its analysts within each section research materials, extract information relating to intelligence requirements, and write reports directly into their native language (Japanese) without actually translating the materials into English themselves. The Asian Studies Detachment's Translations Branch then translates the reports into English. The DAC Reports Officers in the Branch check these translations and perform the final editing and formatting before publishing the reports as intelligence information reports, the unit's primary product.

A-6. With the exception of some Defense Attaché reporting, the Asian Studies Detachment is the only unit in the Army that synthesizes and cites a large number of open source references in an intelligence information report format similar to research papers or essays. The Asian Studies Detachment’s intelligence information reports support the USAPACOM and the US Army Pacific as well as the DIA, the NGIC, and the US Air Force's NASIC on topics ranging from North Korean underground facilities to Chinese Peoples Liberation Army Air Force air and space science and technology developments.

A-7. In addition to the intelligence information report, the Current Operations Branch of the Asian Studies Detachment produces a daily Force Protection and Situational Awareness Report, an email product composed of a compilation of news article excerpts from foreign media websites throughout the USAPACOM’s AOR. Unlike the intelligence information report, which is more strategic in nature, the Force Protection and Situational Awareness Report provides US forces stationed or deployed throughout the USAPACOM’s AOR and other travelers with current FP or security-related open source information.

A-8. The intelligence information reports and Force Protection and Situational Awareness Reports are available on the Asian Studies Detachment's unclassified and classified websites. The Force Protection and Situational Awareness Reports are also posted on the OSC’s website, the FBI-Honolulu's Law Enforcement Online website, the FMSO’s WBIL, and the AKO Intelligence Knowledge Collaboration Center.

CHALLENGES

A-9. The explosion of the Internet over the last decade has had a tremendous effect on the Asian Studies Detachment's OSINT techniques and procedures. Approximately half of the Asian Studies Detachment’s cited sources currently consist of Internet-derived information, and the percentage is steadily growing. The Asian Studies Detachment must meet the near-future challenge of increasing its Internet coverage while simultaneously protecting its Internet research from OPSEC threats. To this end, the Asian Studies Detachment has already begun looking at increasing and standardizing its use of the Intelink-SBU for Internet searches since the system supports increased OPSEC while not compromising its ability to conduct overt collection.

A-10. The Asian Studies Detachment plans to install Intelink-SBU on all of its computers. In addition, the Asian Studies Detachment is exploring the feasibility of entering the realm of audio visual media analysis with the possible implementation of tools which enables continuous real-time monitoring, transcription, and machine translation of foreign-language television broadcasts.

This page intentionally left blank.

Appendix B

Intelligence Oversight

B-1. Executive Order 12333 stems from activities that DOD intelligence and CI units conducted against US persons involved in the Civil Rights and anti-Vietnam War movements in the 1960s and 1970s. DOD intelligence personnel used overt and covert means to collect information on the political positions and expressions of US persons then retained the information in a nationwide database and disseminated the information to law enforcement authorities. In response to these abuses, the President issued Executive Order 12333 to provide general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests.

B-2. The purpose of Executive Order 12333 is to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers. Accurate and timely information about the capabilities, intentions, and activities of foreign powers, organizations, or persons and their agents being essential to informed decisionmaking in the areas of national defense and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the US was founded.

B-3. Executive Order 12333 states the goal of the National intelligence effort is to provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense, and economic policy, and the protection of US national interests from foreign security threats. Supporting this goal are the following principles which apply to all intelligence components of the US Intelligence Community:

- All means, consistent with applicable US law and Executive Order 12333 and with full consideration of the rights of US persons, shall be used to develop intelligence information for the President and the National Security Council. A balanced approach between technical collection efforts and other means should be maintained and encouraged.
- Special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence services against the US Government, or US corporations, establishments, or persons.
- To the greatest extent possible consistent with applicable US law and Executive Order 12333, and with full consideration of the rights of US persons, all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the US intelligence effort.

B-4. For more information on Executive Order 12333 and Intelligence Oversight, visit the Assistant to the Secretary of Defense for Intelligence Oversight website at http://www.dod.mil/atsdio/

INTERPRETATION

B-5. AR 381-10 promulgates the instructions of Executive Order 12333 and DOD Directive 5240.1R. The following summary of AR 381-10 does not modify or supersede published regulatory instructions, policy, or legal opinions. A thorough understanding of this regulation is necessary during the planning, preparation for, execution, and assessment of any intelligence operation. AR 381-10 directs intelligence organizations to refer questions concerning the interpretation of the instructions on collection, retention, and dissemination of US person information to the responsible legal office.

B-6. For current policy information on AR 381-10 and Army Intelligence Oversight, visit the Army Deputy Chief of Staff, G2 website at http://www.dami.army.pentagon.mil/offices/dami-ch/io/io_home.html. AR 381-10 is available from the Army Publication Directorate at http://www.army.mil/usapa/epubs/index.html.

ARMY INTELLIGENCE ACTIVITIES

B-7. AR 381-10 enables Army intelligence components performing authorized intelligence functions to carry out those functions in a manner that protects the constitutional rights of US persons. The regulation does not itself authorize intelligence activity. An Army intelligence component must first have the mission and authority to conduct the intelligence activity. The regulation does not apply to Army intelligence components when engaged in civil disturbance or law enforcement activities. Army intelligence components include the following Regular Army, Army National Guard, and Army Reserve activities:

- Office of the Deputy Chief of Staff for Intelligence, G2.
- Senior intelligence officers and staff of MACOMs and other commands and organizations.
- G2 and S2 staffs.
- MI units.
- INSCOM and subordinates units.
- US Army Intelligence Center and other organizations when conducting intelligence training.
- Contractors of any Army entity when conducting intelligence activities as defined in AR 381-10.
- Any other Army entity when conducting intelligence activities as defined in AR 381-10.

Assigned Functions

B-8. Titles 10, 32, and 50 of the US Code of Law are the legal basis for the authorized intelligence and CI functions of Army's Regular Army, Army National Guard, and Army Reserve. A number of Executive Orders, DOD directives, and Army regulations promulgate these sections of the US Code. DOD Directive 5100.1 defines the functions of the DOD. DOD Directive 5100.1 states a common function of Military Departments (for example, DA) is to "provide adequate, timely, and reliable intelligence and counterintelligence for the Military Department and other Agencies as directed by a competent authority." Based on DOD Directive 5100.1 and Executive Order 12333, the assigned intelligence functions of the US Army are to—

- Collect, produce, and disseminate military and military-related foreign intelligence and CI as required for execution of the Secretary of Defense's responsibilities.
- Conduct programs and missions necessary to fulfill departmental and tactical foreign intelligence requirements.
- Conduct CI activities in support of DOD components outside the US in coordination with the CIA, and within the US in coordination with the FBI pursuant to procedures agreed upon by the Secretary of Defense and the Attorney General.
- Protect the security of DOD installations, activities, property, information, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the DOD as are necessary.
- Cooperate with appropriate law enforcement agencies (LEAs) for the purpose of protecting the employees, information, property and facilities of any agency within the Intelligence Community.

- Unless otherwise precluded by law or Executive Order 12333, participate in LEAs to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities.
- Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local LEAs. Provision of assistance by expert personnel shall be approved in each case by the General Counsel of the providing agency.
- Render any other assistance and cooperation to law enforcement authorities not precluded by applicable law.

B-9. DOD Directives 5100.1 and 5240.1 are available online from the Defense Technical Information Center's Directives and Records Division at http://www.dtic.mil/whs/directives. Executive Order 12333 is available online from Assistant to the Secretary of Defense for Intelligence Oversight at http://www.dod.mil/atsdio/. Titles 10, 32, and 50 are available online from the Government Printing Office Access online database at http://www.gpoaccess.gov/uscode/index.html.

DEFINITION OF A US PERSON

B-10. AR 381-10 defines a US person as—

- A US citizen.
- A US permanent resident alien.
- An unincorporated association composed substantially of US citizens or permanent resident aliens.
- A corporation incorporated in the US that is not directed or controlled by a foreign government. (A corporation or subsidiary incorporated abroad is not a US person even if partially or wholly owned by a corporation in the US.)

B-11. Unless specifically provided for in a particular procedure, AR 381-10 does not apply to non-U.S. person information. Such collection is generally authorized pursuant to any lawful function assigned an Army intelligence component. Unless an Army intelligence component obtains specific information to the contrary, the following are presumed not to be a US person—

- A person or organization outside of the US.
- An alien, any person not a citizen or permanent resident alien of the US.

B-12. Once intelligence personnel have substantiated or have reliable information that a person is an alien but not a "green-card" holder, they can presume the individual is not a US person. Personnel should not rely on ethnic stereotypes, activities, or use of a language other than English to determine whether an individual is a US person or an alien.

COLLECTION OF US PERSON INFORMATION

B-13. In intelligence usage, collection means gathering or receiving information by intelligence personnel in the course of official duties with the intent to use or retain the information for intelligence purposes. An employee must take an action that demonstrates intent to use or retain the information, such as producing an intelligence information or incident report or adding the information to an intelligence database. Data acquired by electronic means (for example, SIGINT or measurement and signatures intelligence [MASINT]) is "collected" only when it has been processed from digital electrons into a form intelligible to a human.

B-14. Under AR 381-10, Procedure 2, Army intelligence activities may collect US person information only when it is necessary to fulfill an assigned function and when it falls within one of the following categories:

- Consensual.
- Publicly Available Information.

- Foreign Intelligence.
- Counterintelligence.
- Potential Sources of Assistance.
- Protecting Intelligence Sources and Methods.
- Physical Security.
- Personnel Security.
- Communications Security.
- Narcotics.
- Threats to Safety.
- Overhead Reconnaissance.
- Administrative Purposes.

B-15. The fact that a collection category exists does not convey authorization to collect. There must be a link between the collection of the US person information and the Army intelligence component's assigned mission and function. This link is particularly important in OSINT and data exploitation.

B-16. Army intelligence components may collect US person information by lawful means but must exhaust the least intrusive collection means before requesting a more intrusive collection means. In general, this means—

- Collection is made first from publicly available sources or with the US person's consent.
- If that collection is not feasible or sufficient, Army intelligence components will seek to collect the US person information from cooperating sources.
- If cooperating source information is not feasible or sufficient, Army intelligence components will seek to collect using other lawful means that do not require a warrant or Attorney General approval.
- If none of the above means is feasible, Army intelligence components units may request approval for the use of techniques requiring a warrant or Attorney General approval.

B-17. Within the US, Army intelligence components may only collect foreign intelligence concerning US persons by overt means, unless all the following conditions are met:

- The foreign intelligence sought is significant and does not concern a US person's domestic activities.
- The foreign intelligence cannot be reasonably obtained by overt means.
- Collection has been coordinated with the FBI.
- Other than overt means was approved in writing by the Army Deputy Chief of Staff, G2 or the Commander, INSCOM.

B-18. The following considerations are applicable to the collection of US person information from the Internet:

- Army intelligence components must use government computers to access the Internet for official Government business unless otherwise authorized.
- If OPSEC so requires, such as to protect a government computer from hacker retaliation, a MACOM commander may approve non-attributable Internet access.
- IP addresses, URLs, and email addresses that are not self-evidently associated with a US person may be acquired, retained, and processed by Army intelligence components without making an effort to determine whether they are associated with a US person as long as the component does not engage in analysis focused upon specific addresses. Once such analysis is initiated, the Army intelligence component must make a reasonable and diligent inquiry to determine whether the data are associated with a US person.

B-19. Army intelligence components will interpret nothing in AR 381-10 as authorizing the collection of any information relating to a US person solely because of that person's lawful advocacy of measures opposed to government policy as embodied in the First Amendment to the US Constitution. The First Amendment states:

> *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.*

Retention of US Person Information

B-20. Retention refers only to maintaining information about US persons that the Army intelligence component can retrieve by the person's name or other personal identifying data. AR 381-10, Procedure 3, describes the kinds of US person information that Army intelligence component may knowingly retain without the individual's consent. AR 381-10 authorizes the retention of US person information under the following criteria:

- Information properly collected in accordance with AR 381-10, Procedure 2
- Information acquired incidentally. Army intelligence components acquired the information incidental to an otherwise authorized collection activity, and retained the information if it—
  - Could have been collected intentionally under the provisions of AR 381-10, Procedure 2.
  - Is necessary to understand or assess foreign intelligence or CI.
  - Is foreign intelligence or CI collected from authorized electronic surveillance. Electronic surveillance means the acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.
  - Is incidental to authorized collection and may indicate involvement in activities that may violate Federal, State, local, or foreign law.
- Information relating to functions of other Army activities, DOD components, or non-DOD agencies. The information pertains solely to the functions and responsibilities of other activities, components or agencies, and is retained only as necessary to transmit the information to that agency. The transmittal is filed and destroyed under general correspondence records management. Army intelligence components will not retain the information in intelligence databases or repositories.
- Temporary retention. Army intelligence components may retain information up to 90 days, solely to determine if the information is, in fact, retainable under this regulation. The 90-day period starts upon receipt of the information.
- Other information. Army intelligence components will only retain information not covered in this section to report the collection for oversight purposes and for necessary subsequent proceedings.

B-21. Access to US person information retained in intelligence files, databases, and repositories is limited to those with a need to know the information. US person information in intelligence files, databases, and repositories is retained in accordance with disposition criteria in AR 25-400-2. Intelligence components will review intelligence files and databases annually. Intelligence components will specifically review US person information to ensure its retention is still necessary to an assigned function. This ensures US person information is not held beyond established disposition criteria, is retained for an authorized function, and was not retained in violation of this regulation. This does not apply to the Investigative Records Repository or other authorized long-term records holding areas.

Dissemination of US Person Information

B-22. In intelligence usage, dissemination is the delivery of intelligence to users in a suitable form with subsequent application of the intelligence to appropriate missions, tasks, and functions. AR 381-10, Procedure 4, governs the types of information regarding US persons that Army intelligence components may disseminate, without the person's consent, outside the component which collected and retained the information. It does not apply to information collected solely for administrative purposes; disseminated pursuant to law; or disseminated pursuant to a court order that imposes dissemination controls. An Army intelligence component may disseminate non-SIGINT information about a US person without that person's consent under the following conditions:

- The information was collected or retained under AR 381-10, Procedures 2 and 3.
- The recipient is reasonably believed to have a need for the information to fulfill a lawful assigned governmental function and is—
  - A DOD employee or a DOD contractor employee.
  - A Federal, State, or local law enforcement entity when the information is in the recipient's jurisdiction.
  - An agency of the US Intelligence Community so that it can determine if the information is relevant to agency responsibilities.
  - A non-DOD or non-Intelligence Community Federal agency.
  - A foreign government, under the provisions of existing policy, agreements, and other understandings with the US in accordance with AR 380-10.
- Dissemination outside DOD of information about a US citizen or permanent resident alien from a US Army system of records requires disclosure accounting under the provisions of AR 340–21.
- After consultation with the Department of Justice and DOD General Counsel, the legal office responsible for advising the Army intelligence component concerned must approve any dissemination that does not conform to the conditions listed in AR 381-10, Procedure 4.
- The Adjutant General Counsel approves any other dissemination not conforming to Procedure 4 in coordination with the DOD General Counsel and the Department of Justice. These dissemination requests are forwarded through command channels to the Office of the Deputy Chief of Staff, G2.

QUESTIONABLE INTELLIGENCE ACTIVITY

B-23. Questionable intelligence activity is conduct during or related to an intelligence activity that may violate law, Executive Order or Presidential Directive, or applicable DOD or Army policy, including regulations. Intelligence personnel will report questionable intelligence activity upon discovery. Employees are encouraged to report questionable intelligence activity through command or inspector general channels in accordance with AR 381-10. The following are commonly reported questionable intelligence activities on improper collection, retention, or dissemination of US person information:

- Gathering information about US domestic groups not connected with a foreign power or international terrorism.
- Producing and disseminating intelligence threat assessments containing US person information without a clear explanation of the intelligence purpose for which the information was collected (for example, listing area universities with foreign students or US companies with DOD contracts in an assessment without showing a connection to a foreign power or international terrorism). An exception to this would be an Army intelligence component providing direct CI or technology protection support to a DOD contractor.

- Incorporating US person criminal information into an intelligence product without determining if identifying the person is appropriate.
- Collecting US person information for FP purposes without determining if the intelligence function related to it is authorized (for example, collecting information on the domestic activities of US persons).
- Submitting a CI incident report under AR 381-12 that contains information on a US person suspected of committing a crime not related to national security, as opposed to passing the information directly to the responsible law enforcement or commander.
- Storing operations and command traffic about US persons in intelligence files merely because the information was transmitted on a classified system.
- Collecting US person information from open sources without a logical connection to the unit's mission or correlation to a validated collection requirement (for example, a unit in one area collecting information from the Web page of a militia group in another area, then reporting that information as a CI incident report or disseminating it in unit intelligence products).
- Disseminating command FP information on US person domestic activity as an intelligence product (for example, including US person groups in an intelligence annex as enemy forces).
- Becoming directly involved in criminal investigative activities (for example, direct participation in a narcotics suspect interrogation) without prior Army General Counsel concurrence and Secretary of Defense approval.
- Identifying a US person by name in an Intelligence Information Report without a requirement to do so.
- Including the identity of a US person in a contact report when that person is not directly involved with the operation.

This page intentionally left blank.

Appendix C

Open Source Intelligence and Homeland Security

C-1. Open sources are a readily accessible and rich source of publicly available information that CA, CI, engineer, intelligence, law enforcement, logistics, medical, operations, PA, and other personnel can use to enhance planning, preparation, execution, and assessment of Regular Army, Army National Guard, and Army Reserve support to homeland defense and civil support missions. Publicly available information includes published or broadcasted information on weather, terrain, and civil considerations needed to support national, regional, state, and local civil support missions as well as information on foreign threats to homeland defense. Retrieving and analyzing publicly available information as part of staff planning and situational awareness ensures commanders and their subordinates receive timely, relevant, and accurate information about the conditions and variables of the operational environment that affect homeland security operations.

C-2. Operating within the scope of their authorized functions and assigned missions, Army intelligence organizations use open source research and intelligence production techniques to support homeland security operations. Open source research and analysis of domestic operational environments may require the collection, retention, and dissemination of US person information. When such activity is necessary, Executive Order 12333, DOD Directive 5240.1-R, and AR 381-10 provide procedures that enable organizations performing authorized intelligence functions to carry out those functions in a manner that protects the constitutional rights of US persons. In addition, DOD Directive 5200.27 and AR 380-13 provide instructions on the acquisition, reporting, processing, and storage of CI investigative information on persons or organizations not affiliated with DOD.

HOMELAND SECURITY

C-3. The National Strategy for Homeland Security provides a framework for organizing the efforts of federal, state, local, and private organizations whose primary functions are often unrelated to national security. Military application of the National Strategy for Homeland Security calls for preparation, detection, deterrence, prevention, defending, and responding to threats and aggression aimed at the homeland. DOD also provides military assistance to civil authorities, including consequence management activities. The Armed Forces of the United States support the National Strategy for Homeland Security through two distinct but interrelated mission areas: homeland defense operations and civil support missions.

Homeland Defense Operations

C-4. DOD is the lead, supported by other agencies, in defending against traditional external threats or aggression. However, against internal asymmetric, nontraditional threats (for example, terrorism), DOD may be in support of homeland security. When ordered to conduct homeland defense operations within US territory, DOD will coordinate closely with other federal agencies or departments. Consistent with laws and policy, the Services will provide capabilities to support COCOM requirements against a variety of air, land, maritime, space, and cyber incursions that can threaten national security. These include invasion, computer network attack, and air and missile attacks. The purpose of homeland defense is to protect against and mitigate the impact of incursions or attacks on sovereign territory, the domestic population, and defense critical infrastructure.

Civil Support Missions

C-5. Employment of military forces within the US, its territories, and possessions, under the auspices of civil support, typically falls under the broad mission of military assistance to civil authorities. Military assistance to civil authorities consists of three mission subsets:

- **Military Support to Civil Authorities.** Military support to civil authorities refers to support provided by Federal military forces, DOD civilians, contractor personnel, and DOD agencies and components in response to requests for assistance during domestic incidents to include terrorist threats or attacks, major disasters, and other emergencies. Military support to civil authorities missions consist of DOD support to US domestic emergencies and for designated law enforcement, civil disturbances, and other activities.
- **Military Support to Civilian Law Enforcement Agencies.** The use of the military in law enforcement roles is a sensitive topic and restrictions apply to such use. Military forces performing in this role support the lead Federal agency and other supporting agencies and may be armed depending on the Secretary of Defense decision. Military support to civilian law enforcement agencies may include, but is not limited to, national special security events, support for combating terrorism, support to counterdrug operations, maritime security, ISR capabilities, and general support.
- **Military Assistance for Civil Disturbances.** The President is authorized by the Constitution and statutory laws to employ the Armed Forces of the United States to suppress insurrections, rebellions, and riots, and provide federal supplemental assistance to the states to maintain law and order. Responsibility for the management of federal response for civil disturbances rests with the Attorney General.

Homeland Defense and Civil Support Command and Control

C-6. Regardless of whether DOD is conducting homeland defense or civil support, military forces will always remain under the control of the established Title 10, Title 32, or state active duty military chain of command. In certain circumstances, military commanders or responsible officials in other DOD components may face situations that will require them to provide immediate response to civil authorities. Military commanders respond to requests from civil authorities prior to receiving authority from the President or chain of command when immediate support is critical to save lives, prevent human suffering, or to mitigate great property damage. Such requests are situation specific, time-sensitive, and may or may not be associated with a declared disaster.

C-7. The Army National Guard primarily operates under three different command relationships: federal funding and federal control (Title 10 US Code); federal funding and state control (Title 32 US Code); and state status (state funding and state control). Army National Guard adjutants general and commanders are responsible for planning and training for federal and state missions. The Secretary of Defense may provide funds to a governor to employ Army National Guard units or members to conduct homeland defense activities that the Secretary of Defense determines to be necessary and appropriate for participation by the Army National Guard units or members, as the case may be. The Army National Guard, when in state status, responds under the governor’s control for civil support missions in accordance with state laws. When Army National Guard personnel or units are federalized by order of the President under Title 10, they respond under the same legal restrictions and structures (command and control) as Regular Army military forces.

C-8. For more information, Joint Publication 3-26 provides the joint doctrine to guide the Armed Forces in the conduct of homeland security operations. It describes the homeland security framework, mission areas, and missions and related supporting operations and enabling activities. It also discusses legal authorities; joint force, multinational, and interagency relationships; C2; planning and execution; and training and resource considerations.

INTELLIGENCE OPERATIONS

C-9. Intelligence operations have specific applications and legal implications when employed in a homeland security operation. The US military has a limited role in collecting foreign intelligence in domestic operations. Executive Orders and DOD Directives allow and require the collection of CI to protect US Government property and human resources. The Services must turn over any information of possible foreign intelligence value that they may have obtained in a CI or domestic operation to the FBI, which has the primary responsibility for domestic intelligence collection within the United States. The Patriot Act of 2001 eases some of the restrictions on foreign intelligence gathering within the United States, and affords the US Intelligence Community greater access to information gathered during criminal investigations.

C-10. Under AR 381-10, Army intelligence activities may collect publicly available information on US persons only when it is necessary to fulfill an assigned function. There must also be a link between the collection of the US person information and the Army intelligence component's assigned mission and function. Army intelligence components must exhaust the least intrusive collection means before requesting a more intrusive collection means. According to AR 381-10, the least intrusive means of collection is from publicly available sources or with the US person's consent. Within the US, Army intelligence components may only collect foreign intelligence concerning US persons by overt means except when all of the following conditions are present:

- The foreign intelligence sought is significant and does not concern a US person's domestic activities.
- The foreign intelligence cannot be reasonably obtained by overt means.
- Collection has been coordinated with the FBI.
- Other than overt means was approved in writing by the Army Deputy Chief of Staff, G2 or the Commander, INSCOM.

C-11. Under AR 380-13, the Army prohibits acquiring, reporting, processing or storing of investigative information on persons or organizations not affiliated with DOD, except under those circumstances authorized in AR 380-13, paragraphs 6 and 7, when such information is essential to accomplish DA missions. Paragraph 6 addresses operations related to protection of army personnel, functions and property. Paragraph 7 describes operations related to civil disturbances. All information-gathering activities are subject to overall civilian control and general supervision by the Secretary or Under Secretary of the Army.

C-12. Investigative information includes all data developed as a result of CI investigative activities, such as investigations, operations, and services, and through liaison with local, state, and federal agencies. It may also come from unsolicited sources, and from public sources such as newspapers, magazines, books, periodicals, handbills, and radio and television broadcasts. Where acquisition activities are authorized by AR 380-13 to meet an essential requirement for information, maximum reliance is placed on liaison with domestic civilian investigative agencies, federal, state, and local. AR 380-13 is not applicable to—

- Pretrial investigations required by the Uniform Code of Military Justice (UCMJ).
- Activities involving cryptography.
- Use by public information officers of relevant information from published sources solely for the purpose of preparing responses to public inquiries.
- Foreign intelligence information including the acquisition reporting, processing, and storing of such information.

- Authorized criminal investigation and law enforcement information gathering activities (for example, those activities not "CI related") which are the responsibility of military police and the US Army Criminal Investigation Command.

C-13. Nothing in AR 380-13 prohibits the prompt reporting to LEAs, or keeping a record of such a report, of any information indicating the existence of a threat to life or property, or violation of law. The regulation does not prohibit the receipt of information from all agencies in the course of liaison authorized by AR 380-13 provided organizations—

- Promptly screen such information.
- Immediately destroy information not authorized for the retention.

C-14. AR 380-13 prohibits the assignment of Army personnel, military or civilian, to attend public or private meetings, demonstrations, or other similar activities held off post to acquire investigative information authorized by the regulation without specific approval by the Secretary or the Under Secretary of the Army. This prohibition includes any attempt to encourage or request the unofficial attendance of any persons at such events, whether or not such personnel have official CI or investigative responsibilities. An exception to the policy is authorized when, in the judgment of the local commander, the threat is direct and immediate and time precludes obtaining prior approval.

Military Support to Civilian Law Enforcement Agencies

C-15. Military support to civilian LEAs includes support to civilian LEAs. This includes but is not limited to combating terrorism, counterdrug operations, national security special events, and national critical infrastructure and key asset protection. Joint Publication 3-26 describes National critical infrastructure and key assets as the infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. They include telecommunications, electrical power systems, gas and oil distribution and storage, water supply systems, banking and finance, transportation, emergency services, industrial assets, information systems, and continuity of government operations.

C-16. Under AR 380-13, information on persons and organizations not affiliated with the DOD may be acquired, reported, processed, and stored only if there is a reasonable basis to believe that one or more of the following situations exists:

- Theft, destruction or sabotage of weapons, ammunition, equipment, facilities, or records belonging to DOD units or installations.
- Possible compromise of classified defense information by unauthorized disclosure or by espionage.
- Subversion of loyalty, discipline or morale of DA military or DAC personnel by actively encouraging violation of laws, disobedience of lawful orders and regulations, or disruption of military activities.
- Demonstrations on Regular Army, Army National Guard, and Army Reserve installations or demonstrations immediately adjacent to them which are of such a size or character that they are likely to interfere with the conduct of military activities.
- Direct threats to DOD military or civilian personnel regarding their official duties or to other persons authorized protection by DOD resources.
- Activities or demonstrations endangering classified defense contract facilities or key defense facilities.

C-17. Effective liaison with local LEAs will occur regularly to determine if actual or potential situations described above exist. Organizations will conduct CI surveys and inspections for the same purpose.

Military Assistance for Civil Disturbances

C-18. Military assistance for civil disturbances are missions of civil support involving DOD support, normally based on the direction of the President, to suppress insurrections, rebellions, and domestic violence, and provide federal supplemental assistance to the states to maintain law and order. In accordance with AR 380-13, Army resources may only acquire, report, process or store civil disturbance information concerning nonaffiliated persons and organizations upon receipt of specific prior authorization from the Secretary or the Under Secretary of the Army. The Secretary or the Under Secretary of the Army will only grant such authorization when there is a distinct threat of a civil disturbance exceeding the law enforcement capability of state and local authorities. The authorization will set forth the procedures and the limitations on the acquisition, reporting, processing and storing of civil disturbance information.

C-19. As an exception to the above limitation, AR 380-13 authorizes overt acquisition and current maintenance of the following information:

- Listing of local, state, and Federal officials whose duties include direct responsibilities related to the control of civil disturbances.
- Data on vital public and commercial installations or facilities and private facilities believed to be appropriate targets for individuals or organizations engaged in civil disorders.

This page intentionally left blank.

Appendix D

Copyright Basics

D-1. AR 27-60 prescribes policy and procedures for the acquisition, protection, and transfer and use of patents, copyrights, trademarks, and other intellectual property by DA. It is Army policy to recognize the rights of copyright owners consistent with the Army's unique mission and worldwide commitments. When uncertain, intelligence personnel should contact their supporting Judge Advocate General office before publishing information containing copyrighted or similarly protected intellectual property.

FAIR USE

D-2. As a general rule, Army organizations will not reproduce or distribute copyrighted works without the permission of the copyright owner unless such use is within an exception under US Copyright Law or required to meet an immediate, mission-essential need for which noninfringing alternatives are either unavailable or unsatisfactory. According to the US Copyright Office, "fair use" of a copyrighted work for purposes such as criticism, comment, news reporting, teaching, scholarship, or research is not an infringement of copyright. The four factors in determining fair use are –

- **Purpose and character of the use.** In the context of fair use, intelligence operations are similar in purpose and usage to non-profit news reporting and research organizations.
- **Nature of the copyrighted work.** Self-explanatory**.**
- **Amount and substantiality of the portion used in relation to the copyrighted work as a whole.** There is no specific number of words, lines, or notes that may safely be taken without permission. Usually, the amount or portion of copyrighted material is limited to quotations of excerpts and short passages; and summary of a speech or article, with brief quotations.
- **Effect of the use upon the potential market for or value of the copyrighted work.** The effect on the market or value of copyrighted material relates to reproduction and dissemination of products provided by the owner beyond that authorized the owner's "Terms of Use" or described in contracts and licenses with the US Government. Operators of fee-based data services have an economic interest in the scope and dissemination of the data they offer. Improper use or dissemination could be infringement on the copyright law protections of the owner of the database.

D-3. Implicit with fair use is the documentation and citation of the source of the copyrighted information. Upon retrieval or collection, intelligence personnel must document the source's identity and the circumstances "who, what, where, when, and why" of retrieval or collection. When using copyrighted material, intelligence personnel must include a citation or a reference that attributes the information to the source. The format for citations may vary by organization or style manual (for example, Government Style Manual, Modern Language Association, American Psychological Association) but the basic components include the name of the authors, the title of the material; the date of publication, retrieval, or collection; the identify of the source (for example, publisher, organization, website).

NATURE OF COPYRIGHTED WORKS

D-4. The following extracts from US Copyright Office Circular 1 provide basic information on the nature of copyrighted works.

Description

D-5. Copyright is a form of protection provided by the laws of the US (Title 17 US Code) to the authors of “original works of authorship,” including literary, dramatic, musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works. Section 106 of the 1976 Copyright Act generally gives the owner of copyright the exclusive right to do and to authorize others to do the following:

- Reproduce the work in copies or phonorecords.
- Prepare derivative works based upon the work.
- Distribute copies or phonorecords of the work to the public by sale or other transfer of ownership, or by rental, lease, or lending.
- Perform the work publicly, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works.
- Display the copyrighted work publicly, in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work.
- In the case of sound recordings, perform the work publicly by means of a digital audio transmission.

D-6. It is illegal for anyone to violate any of the rights provided by the copyright law to the owner of copyright. These rights, however, are not unlimited in scope. Sections 107 through 121 of the 1976 Copyright Act establish limitations on these rights. In some cases, these limitations are specified exemptions from copyright liability. One major limitation is the doctrine of "fair use," which is given a statutory basis in section 107 of the 1976 Copyright Act. In other instances, the limitation takes the form of a "compulsory license" under which certain limited uses of copyrighted works are permitted upon payment of specified royalties and compliance with statutory conditions.

Protected Works

D-7. Copyright protects "original works of authorship" that are fixed in a tangible form of expression. The fixation need not be directly perceptible so long as it may be communicated with the aid of a machine or device. Copyrightable works include the following categories:

- Literary works.
- Musical works, including any accompanying words.
- Dramatic works, including any accompanying music.
- Pantomimes and choreographic works.
- Pictorial, graphic, and sculptural works.
- Motion pictures and other audiovisual works.
- Sound recordings.
- Architectural works.
- Data or information from fee-based websites.

Works Ineligible for Protection

D-8. Several categories of material are generally not eligible for federal copyright protection. These include among others:

- Works that have not been fixed in a tangible form of expression (for example, choreographic works that have not been notated or recorded, or improvisational speeches or performances that have not been written or recorded).

- Titles, names, short phrases, and slogans; familiar symbols or designs; mere variations of typographic ornamentation, lettering, or coloring; mere listings of ingredients or contents.
- Ideas, procedures, methods, systems, processes, concepts, principles, discoveries, or devices, as distinguished from a description, explanation, or illustration.
- Works consisting entirely of information that is common property and containing no original authorship (for example: standard calendars, height and weight charts, tape measures and rulers, and lists or tables taken from public documents or other common sources).

International Copyright Protection

D-9. There is no such thing as an "international copyright" that will automatically protect an author's writings throughout the entire world. Protection against unauthorized use in a particular country depends, basically, on the national laws of that country. Most countries, however, do offer protection to foreign works under certain conditions, and these conditions have been greatly simplified by international copyright treaties and conventions. For further information and a list of countries that maintain copyright relations with the US is available in US Copyright Office Circular 38a, "International Copyright Relations of the United States" on the US Copyright Office website at http://www.copyright.gov.

This page intentionally left blank.

Appendix E

Director of National Intelligence Open Source Center

E-1. Open source as an intelligence discipline has been practiced to varying degrees throughout the nation's history. In addition over 200 years of military history of utilizing openly available sources, US missions to foreign countries have traditionally dedicated personnel to reviewing local press and later broadcast media to keep up with host nation current events and to understand local perspectives. The work of those "Press Attaches" and their staffs has come to make a significant contribution to the effectiveness of US Embassies abroad.

E-2. In February of 1941, the US Government took the first step in creating an open source mission-specific organization by creating the Foreign Broadcast Monitoring Service, dedicated to "recording, translating, transcribing, and analyzing certain radio broadcast programs" from foreign transmitters, primarily Germany and Japan. Eventually residing in the CIA, that organization, which came be known as the Foreign Broadcast Information Service, developed into a service of common concern that for almost 65 years provided products derived from foreign open sources to consumers across the US military and Government.

E-3. In response to language in the Intelligence Reform and Prevention of Terrorism Act of 2004 and recommendations in the Silberman-Robb Commission calling for more effective use of open sources to support intelligence, the newly established DNI created the DNI OSC at CIA on 1 November 2005. The DNI assigned the Director, CIA as Executive Agent for OSC. The DNI directed that the OSC to—

- Build on the capabilities and expertise of the CIA's Foreign Broadcast Information Service.
- Report directly to the Director, CIA, in response to the Assistant Deputy, DNI, for Open Source's direction and guidance.

MISSION

E-4. The DNI OSC supports the National Open Source Enterprise as directed by the Assistant Deputy DNI for Open Source. The OSC is a center of excellence in the distributed Open Source Enterprise which nurtures distributed expertise and capabilities that exist not only within the Intelligence Community but also across the government and throughout the private sector and academia. The OSC works with COCOMs and the entire DOD down to the small unit level to deconflict strategies and minimize redundancy. As directed by the Assistant Deputy, DNI for Open Source, the OSC provides services of common concern to the National Open Source Enterprise such as training and content procurement.

Open Source Requirements

E-5. The OSC's operations are driven by the standing open source requirements contained in the OSC's collection plans, which are reviewed and approved annually. OSC analysts are urged to familiarize themselves with the collection plans and standing requirements related to their AOIs in order to gain maximum benefit from their participation in the collection management process. The plans reside on Intelink-Top Secret within the Open Source Requirements Management System site on the Intelink-SBU at http://cres.cia.ic.gov/oshome.nsf/welcome.

E-6. Organizations wishing to submit ad hoc requirements to the OSC must contact their organization's designated point of contact for open source requirements. The points of contact are listed on the Open Source Requirements Management System site. Contact the OSC Customer Service Center about a specific requirement or the requirements process.

Operations

E-7. The OSC maintains a worldwide network of multilingual regional experts. They respond to intelligence requirements using open sources including radio, television, newspapers, news agencies, databases, and the Internet. The OSC monitors open sources in more than 160 countries in over 80 languages and acquires open source data worldwide for organizations across the military and government, down to local law enforcement.

E-8. The OSC analyzes the content and behavior of the media and Internet websites of nations and other international actors of significant policy interest to the US Government. These contextual and analytical products, categorized as OSC Analysis and OSC Media Aids, are available on Opensource.gov and the OSC websites hosted on government-sponsored communications systems, including SIPRNET and JWICS.

E-9. OSC products and services include—

- **Analysis.** OSC analyses range from short, time-sensitive products that explain the media treatment of issues on the US Government policy agenda to longer analytic pieces that examine issues or the content and behavior of a set of media over time to detect trends, patterns, and changes related to US national security interests.
- **Media Aids – Media Guide.** Media guides offer a comprehensive characterization of the media of a country or region and provide an overview or characterization of the larger media environment, including what makes up the media of a country, how that media operate, who uses the media and how they use it, and other factors, such as literacy rates, press laws, economic status, and demographics that affect the media and their behavior or use.
- **Media Aids – Commentator Profile.** Commentator profiles provide detailed information on one or more media personalities in a particular country, outlining their influence, background, views, and biases on key topics. The focus is on personalities who speak or write about issues of importance to the United States or who have influence with their government, businesses, or large segments of the general population.
- **Open Source Center Reports.** Through its worldwide access to foreign media and other publicly available material, the OSC provides translations and transcriptions of the latest political, military, economic, and technical information gleaned from foreign open sources. Reports gist from select sources, such as jihadist websites or daily editorials, on topics related to the National Intelligence Priorities.
- **Video Services.** Video Services Division collects, analyzes, and disseminates more than 550 channels of foreign and domestic television and Internet video for 24 hours a day, 7 days a week to military and Intelligence Community customers. Video Services Division can access, via OSC's international collection network, between 16,000 and 34,000 additional channels. Video Services Division archives over 1.6 million hours of video per year and has a library containing 10,000 hours spanning 45 years. The Video Server System provides access to foreign video at the desktop. The capabilities of the system include keyword searching, English closed-captioning, speech-to-text transcripts, thumbnail program scanning, video on demand, unlimited archive capability, still photographs from video, multiple customizable topic profiling, and on-line ordering. The Video Server System hosts a nearly 2-year archive of web-accessible video. Military customers can access the unclassified Video Server System hosted on the Open Source Information Service network or request delivery via videotape, digital video device, or compact disc.
- **Map Services.** OSC geographers are experts on foreign mapping, geographic information, and geospatial technologies. The Maps Services Center provides maps, data, information, analytical products, training and a host of related geographic services to those on the front lines of

intelligence. Map Services Center maintains the community's central repository of hundreds of thousands of foreign maps and geographic data.

Open Source Tools

E-10. The OSC array of tools facilitates the open source efforts of agencies and offices throughout the US Government by enabling the creation, management, and dissemination of unclassified products, including dissemination to classified networks and platforms. The tools' effectiveness and high adaptability stem from these characteristics:

- Highly developed for open source exploitation and product creation through years of testing and use in the OSC.
- Designed to support a distributed workforce, and can accommodate staff or contractor resources.
- Independent of location; most capabilities require only Internet access for full functionality.
- Tailored for a non-technical workforce.
- Consistent with Intelligence Community security, and technical and metadata standards.

E-11. OSC tools include—

- **Analytic Tools and Methodology.** In the Analytic Development Lab, community analysts work alongside open source specialists to discover new open sources and develop research and analytic methods and tools. While working in the Lab, analysts have access to large-scale Internet and data mining tools in addition to the linguistic and substantive resources of OSC. Tours in the lab run from 6- to 12-month details, and there are limitations on the number of spaces available.
- **Internet Exploitation Tools.** OSC's Internet Exploitation Team provides training as well as access to a large data repository; including an Internet cache and other purchased content, and a suite of data mining tools to allow research of web-based and other open sources. As with tours in the Lab, the training and system access are available to the community on a limited basis; use of some services may also incur fees.
- **Video Collection and Product Creation.** The OSC's video repository is an interactive, real-time and archive database for viewing live and recorded television programming, Internet video posts, and OSC video products at the desktop. The repository streams and records over 160 programs from 50 countries in 31 languages daily. Video processing tools, and more video content, will be available mid-2006 through the OSC's Digital Audio Video Enterprise (DAVE) Program. The repository is directly accessible through the OSC's website at www.Opensource.gov.
- **Product Creation Tools and Systems.** OSC product creation tools and systems enable the creation of open source products via the Internet. For complex work processes, particularly those involving a distributed workforce or a multi-step workflow, the OSC's PRINCE system provides the optimal solution, as its web interfaces enable product creation, editing, and dissemination. Users can direct items for translation, editing, and dissemination from any point in the globe, the only requirement being Internet access. PRINCE accommodates value-added products, such as open source analysis, in addition to translations. The OSC's website, Opensource.gov, also has product creation capabilities that are simple to use and can be accessed via the Internet. To ensure the broadest possible dissemination, open source products created in PRINCE or Opensource.gov are distributed to classified networks, including JWICS SIPRNET, as well as customer platforms.
- **Opensource.gov Content Management Services.** To maximize access to open source products, Opensource.gov content management capabilities are available to the community. These capabilities include highlighting individual open source products on the site or even highlighting the open source efforts of other government agencies through the creation of entire "communities," or pages, on the site. These content management capabilities can be granted to

government employees or contractors, and require minimal training. The OSC also offers a fee-for-service capability for managing the content of other government agencies. For more information, contact OSC's Directorate for Information Access at 703-613-5844 or the Open Source Center Help Desk at 1-800-205-8615.

Open Source Center Website

E-12. Opensource.gov, formerly known as fbis.gov, is the OSC's Internet-accessible website. The site is available to the Uniformed Services, any US Government employee, and US Government contractors. Accounts can be set up easily and quickly over the Internet. The site provides ready access to the top OSINT on key issues of the day. OSC has over 200 content managers working around the globe to actively manage the 2,400 to 2,500 reports—translations and analysis—OSC issues each day. Customers can find OSINT on major issues on the Opensource.gov home page, browse the over 100 pages on the site devoted to regional or topical reporting, or search the entire repository if they wish to delve deeper. A single search on Opensource.gov can retrieve reporting and analysis from today or dating back to the mid-1990s.

E-13. The OSC works with other US Government components to host their open source products on Opensource.gov. Many of the National Intelligence Council's unclassified products are now available, and the National Intelligence Council has its own page on the site. In addition, an increasing number of DOS reports are on Opensource.gov, as are selected reports from the US Army's FMSO and other DOD components. By placing their open source products on the website, organizations across the government dramatically increase the availability of the products. On the commercial side, OSC has thus far (as of January 2006) focused its efforts on acquiring analysis of the foreign media. As a result, a number of studies by InterMedia and Media Tenor are available on the site. OSC anticipates branching out to other open source resources in the future.

E-14. One of the drivers behind the development of a "state of the art" website for the OSC was the goal of increasing the amount of multimedia available to customers. This goal includes multimedia content in textual products, usually in the form of attachments or links; multimedia in its "raw" form, such as streaming video or recorded television programs; and video analysis products. OSC's collection units currently monitor and analyze hundreds of thousands of hours of television and radio broadcasts each year. The yield of this enormous collection effort includes live video streams from high-profile channels, such as Al-Jazirah, and thousands of hours of archived video from thousands of television stations around the world. While some of that content is currently available on Opensource.gov via the Video Server link on the home page, the OSC's multiyear, multimillion dollar DAVE project will dramatically increase this amount in the coming years. DAVE deployments begin in early Calendar Year 2006 and will continue through 2008. In addition, DAVE will provide customers outside OSC ready access to tools for manipulating and searching video.

E-15. OSC also combines various media formats to create sophisticated web products that enhance usability of and access to open source material. For example, the "Repository of Kim Jong Il's Public Appearances" catalogs all major appearances by the North Korean leader with pertinent video, images, and media reporting, while the "China Open Source Community" highlights key open source resources on China.

E-16. Opensource.gov serves double-duty in that it operates as both a pull and push technology. On the "push" side, customers have the option of subscribing to the content in the repository via email or file transfer protocol (ftp), depending on their needs. Opensource.gov also provides a system-to-system push and is, for example, used to transfer OSC reporting to classified as well as unclassified networks and systems. Opensource.gov's product delivery options are easily accessed through the "Browse and Search" community on the site.

E-17. Opensource.gov promises the capability for OSC to create a "community of interest" with its customers through greatly increased interaction. The first significant step in this direction came in the form of web logs, or "blogs," which the OSC initiated in October 2005. OSC blogs are run by OSC, academic, and private sector experts on top intelligence issues, and the OSC's initial efforts have been on China, Central Asia, library and geospatial intelligence, and, interestingly, foreign blogs (in the aptly named "Blog on Blogs"). Most recently, new blogs have been launched on terrorist use of the Internet and Kazakhstan. In addition to blogs, Opensource.gov customers can interact with the OSC by providing feedback on the products in Opensource.gov.

E-18. To ensure that customers can access the OSC's products no matter where they are, Opensource.gov is accessible via the Internet at www.opensource.gov. System protection is provided by Secure Sockets Layer, the same system commonly used to protect banking and financial data on the web. Secure Sockets Layer not only provides security from system intrusion but also ensures that customer movement within the site is not subject to hostile tracking.

E-19. To gain access to the OSC's site, a simple account registration process is available on Opensource.gov, and account approval occurs within one business day for government employees using .gov or .mil email accounts in their application. Applications with commercial email addresses are generally validated telephonically, which can take longer. Government contractors can also get accounts, but their contract status must be validated by their government contracting officer.

Customer Center

E-20. The OSC's Customer Center has experts ready to assist in helping customers. The Customer Center is open Monday through Friday from 0800 – 1630 (Eastern Standard Time). The Customer Center can be reached via telephone, facsimile, or email at as follows:

- Toll Free Voice: 1-800-205-8615.
- Commercial Voice: 203-338-6735.
- Commercial Fax: 703-613-5735.
- Defense Switched Network: 695-8761.
- Secure Voice: 65670 or 9365670.
- NIPRNET: oscinfo@rccb.intelink.gov.
- SIPRNET: assist@jdiss.cia.sgov.gov.
- JWICS: assist@jdiss.cia.ic.gov.

Open Source Academy

E-21. OSC's Open Source Academy has been a leading provider of open source tradecraft training since 2003. As intelligence consumers place a greater value on OSINT, open source specialists throughout the Federal Government, including the armed services, are turning to Open Source Academy courses to build their open source skills and keep abreast of evolving technologies. Open Source Academy is building relationships with community leaders and training focal points across the community to develop a comprehensive approach to instilling open source tradecraft skills. The Academy hosts participants from the Air Force, Army, Marine Corps, Navy, DOD's CI Field Activity, Defense Human Intelligence Service, DIA, Department of Treasury, DOS, FBI, National Geospatial Intelligence Agency, National Reconnaissance Office, and National Security Agency and welcomes personnel with OSINT duties from US Government organizations not yet listed.

E-22. The Open Source Academy's core curriculum includes instructor-led courses on an expanding range of topics, from analysis to Internet exploitation to reviewing finished intelligence products. The following Open Source Academy courses are open to military and government employees:

- Assessing Media Environments.
- Bright Planet – Deep Query Manager.

- Creating Multimedia Products.
- George Mason University Seminars on Understanding and Analyzing.
- Global Media (by invitation).
- Hidden Universes of Information on the Internet.
- Introductory Analytic Tradecraft.
- Media Analysis.
- Orientation to the OSC.
- OSINT and the Other Intelligence Disciplines.
- Overview of the OSC Collection Requirements Process.
- Reviewing Analytic Products.
- Security and Privacy Issues for Internet Users.

E-23. Open Source Academy courses focus on real-work issues and provide open source tradecraft knowledge and tools that enhance intelligence collection and analysis practices. There is ample opportunity for shared learning and networking as participants exchange insights, experience, and solutions with colleagues from organizations across the community. Participants also receive valuable reference materials that they can use to reinforce and apply the course content at their regular duty stations.

E-24. The Open Source Academy Course Catalog describes each of the courses and indicates when they are offered. Course objectives are also available upon request. To obtain a copy of the Catalog, register, or request information on Open Source Academy’s other services, contact the Open Source Academy Registrar at 703-613-5090.

Appendix F

INTELINK-SBU System

F-1. The Intelink-SBU is a US Government, Joint-use, remotely accessed, and operationally implemented information service that is used to access and process unclassified, publicly accessible information only. It provides a protected environment to exchange authorized unclassified, unclassified for official use only, and sensitive but unclassified information among personnel of the Defense, the Diplomatic, the Homeland Security, the Intelligence, and the Law Enforcement communities. The Intelink-SBU firewalls protect users and allow customers to access the public Internet; thus giving Intelink-SBU users a single point of access to an unprecedented amount of unclassified open source information.

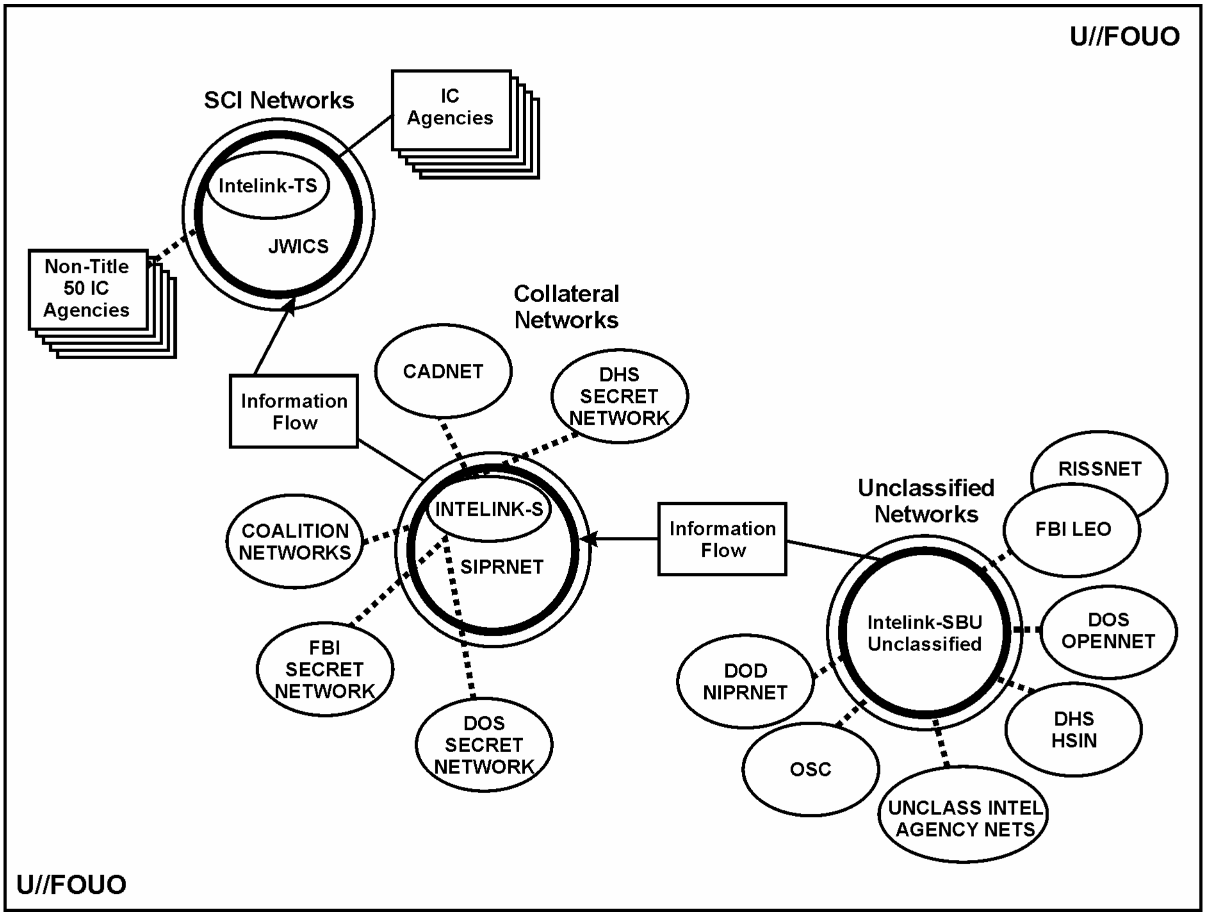


Figure F-1. Intelligence Community Enterprise architecture

Overview

F-2. Intelink-SBU is a private electronic network that provides the information technology infrastructure enabling protected intranet research for the sharing of sensitive and unclassified information within the

Intelligence Community components, its customers, and affiliates. It was developed at Director of Central Intelligence direction under authority contained within the National Security Act of 1947 (as amended) and Executive Order 12333 to support the National Intelligence effort through full and free exchange of information across all agencies and departments of the Federal Government.

F-3. Additionally, Intelink-SBU provides protected and monitored access to the public Internet in order to provide Intelink-SBU users a single point of access to unclassified intelligence information. It provides a central point of access for Regular Army, Army Reserve, and Army National Guard units around the World to share common mission tools and practices. Intelink-SBU provides the one venue that the Army contributes resources to support. Intelink-SBU provides unique OPSEC tools and techniques that, if not available on one network, would cost the DOD and the Army millions of dollars to replicate.

F-4. This Intelink-SBU system is not directly connected to the public Internet. Access to Intelink-SBU services is implemented through multiple virtual private networks. Users gain access to the public Internet through Intelink-SBU provided proxy-based firewalls. The Intelink-SBU boundary devices include firewalls and the virtual private network tunnel boxes, including the desktop-tunnel endpoint devices.

F-5. Intelink-SBU users can view current and historical open source content, shared by Intelink-SBU participants or purchased by a participant from a commercial vendor. This is more of a rear-only view into Intelink-SBU. Participants appear as an Intelink-SBU network (intelink.gov) on the Internet, instead of using their organization’s network name, such as a “.mil” site. Participation in the Intelink-SBU network is via a standalone (dedicated) host or network connected host.

- Standalone (Dedicated) Host. The use of a standalone, dedicated laptop or desktop platform is the preferred option to support the Intelink-SBU environment within an Army organization with the least amount of residual operational risk to the supporting network. The installation firewall will deny all traffic to the Intelink-SBU client and permit by exception only the destination Intelink-SBU IP address inbound or outbound to the Intelink-SBU client. The system will only be used for the Intelink-SBU virtual private network connection. Use of the open Internet for web-surfing, connection to local or web email, or other unapproved applications will not be installed or authorized.
- Network Connected Host. Users are required to access the local host through existing authentication methods, traditionally through input of a user name and password, before they can access the local system; and then shall use a separate user name and password to access the Intelink-SBU account. The local host identified for Intelink-SBU connectivity will have a statically assigned IP address for the desktops to attribute security auditing and reviews. User activity on the Intelink-SBU server is seen as an intranet user on the Intelink-SBU network, and all user activity is logged and accountable to that user. When using desktop virtual private network software, all existing local network devices (for example, printers, network file servers, local email services) become unavailable.

General Requirements

F-6. Intelink-SBU is responsible for providing virtual private network desktop client configuration management, application support, and product updates. This system displays the DOD Warning Banner as a part of the logon process. Access to the Intelink-SBU virtual private network from any system will be restricted to authorized users. No temporary, seasonal, or liaison personnel shall be authorized to use an Intelink-SBU virtual private network client installed on an Army information system. Personnel using a NIPRNET LAN connected and supported Intelink-SBU systems will possess access credentials equivalent to their position and authorizations for use of those NIPRNET systems. This requirement is waiverable only when access to Intelink-SBU is from a standalone (dedicated) system used for Intelink-SBU connectivity only, and the individual is authorized an Intelink-SBU account. Many Intelink-SBU users who do not possess or hold an appropriate clearance are often assigned open source tasks on the Intelink-

SBU network as the best operational use of these personnel and as a training vehicle available to those personnel pending their clearance approvals.

F-7. All users accessing the Intelink-SBU system will receive training on the importance and risks of establishing a virtual private network from internal systems and the procedures for any data transfers that may be conducted as part of their acceptable use of such systems. Users will have unique personal identifiers unless mission requirements dictate the use of pseudonym identifiers (aliases). Internal procedures will record and track these aliases identifiers with actual users in the event Intelink-SBU requires incident attribution.

F-8. Password management for the Intelink-SBU service is centrally managed by the Intelink Management Office through a dedicated Service point of contact trusted agent. Each MACOM should establish a centrally managed Intelink-SBU accounting mechanism for control and approvals of accounts. Normally this would reside in the organization’s intelligence directorate, but is customizable in accordance with local directives. If the MACOM establishes centralized control of the Intelink-SBU approval, notification of such a designation shall be made to the Army Intelink-SBU (for example, INSCOM) point of contact. If a MACOM point of contact is not established, the Army Intelink-SBU point of contact can service and manage Intelink-SBU Access Requests at the Army level.

F-9. DOIM network and information assurance security teams (or designated personnel) will have administrator rights to all Intelink-SBU computers and network components that connect to the garrison NIPRNET, or are supported by the DOIM. The System Administrator or other information assurance person will review audit logs weekly and maintain these logs for at least one year. Intelink-SBU information systems are configured with local security policy to audit, at a minimum, the success and failure of—

- Audit Account Logon Events.
- Audit Account Management.
- Audit Logon Events.
- Audit Policy Change.
- Audit System Events.

F-10. Intelink-SBU account users are not allowed to give out or share user, system, or network information using email, interactive websites, or telephone of any Intelink-SBU accounts or network accesses. They will use these accounts within their official capacity for the authorizations granted to them. No personal use or violations of ethical or professional conduct will be tolerated. Intelink-SBU will monitor acceptable usage of all user accounts and activities.

F-11. DOIM personnel may access and physically inspect this system, conduct scans, or collect information as a part of their role in protecting networks and systems or investigating incidents. The DOIM may monitor and record this system’s activity to ensure system and data availability, confidentiality, and integrity. DOIMs will use automated tools to periodically detect system vulnerabilities and review system security settings. DOIM and the Installation Security Office have the right to disconnect service if the system configuration is not maintained or a breach in security is detected.

F-12. All Intelink-SBU identified workstations will be registered in the Army Asset and Vulnerability Tracking Repository database when approved for installation. The Repository is accessible at https://newia.us.army.mil.

F-13. To request Intelink-SBU access, personnel must contact their organizational Intelink-SBU account manager or send an email to accounts@intelink.gov.

F-14. The Army G6 Information Assurance Office approved the Information Assurance Better Business Practice for connecting the NIPRNET to the Intelink-SBU on 30 November 2005. The Intelink-SBU Better Business Practice is available online from the Army's Information Assurance Office at https://informationassurance.us.army.mil/bbp/ or https://www.us.army.mil/suite/doc/4938453.

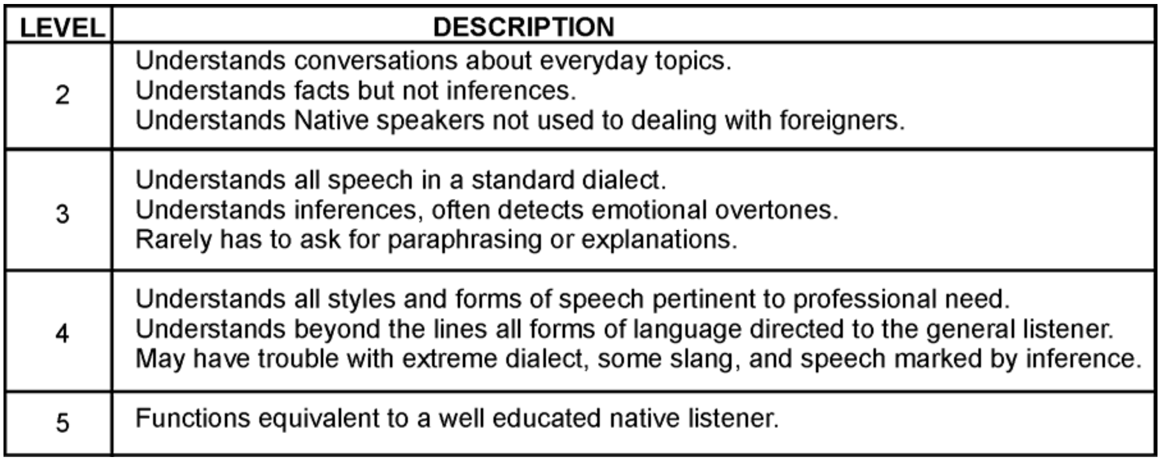
F-15. For more information on Intelink-SBU visit the DA Intelligence Information Services Portal at https://www.us.army.mil/suite/page/132281 or https://akocomm.us.army.mil/dadpm.

Appendix G

Language Proficiency Levels

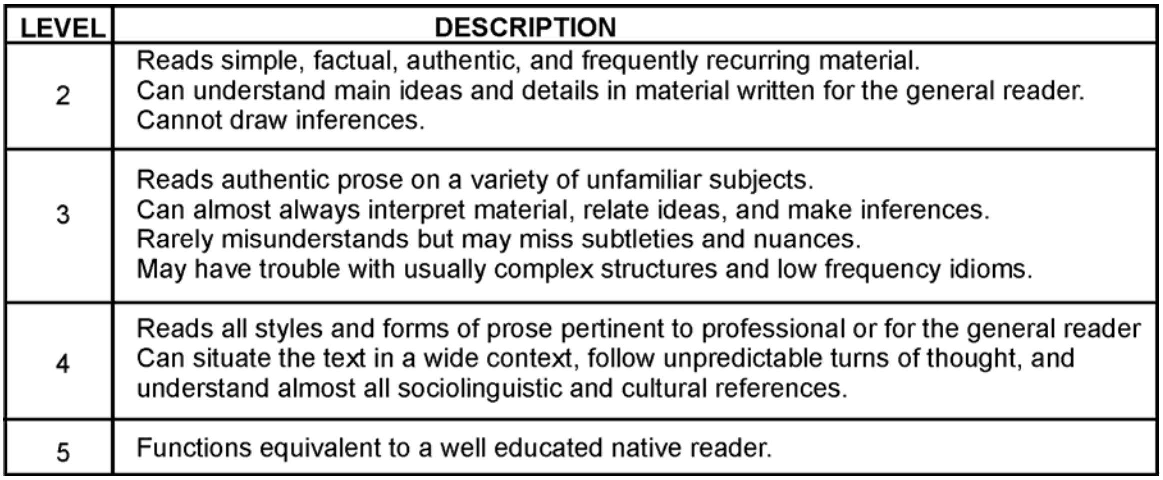
G-1. The Interagency Language Roundtable proficiency level descriptions in this appendix characterize language usage in the areas of listening, reading, speaking, writing, and translation for Levels 2 to 5. Detailed information about language proficiency is available on the Interagency Language Roundtable at http://www.govtilr.org.

Table G-1. Listening proficiency levels 2 to 5



LEVEL	DESCRIPTION
2	Understands conversations about everyday topics. Understands facts but not inferences. Understands Native speakers not used to dealing with foreigners.
3	Understands all speech in a standard dialect. Understands inferences, often detects emotional overtones. Rarely has to ask for paraphrasing or explanations.
4	Understands all styles and forms of speech pertinent to professional need. Understands beyond the lines all forms of language directed to the general listener. May have trouble with extreme dialect, some slang, and speech marked by inference.
5	Functions equivalent to a well educated native listener.

Table G-2. Reading proficiency levels 2 to 5



LEVEL	DESCRIPTION
2	Reads simple, factual, authentic, and frequently recurring material. Can understand main ideas and details in material written for the general reader. Cannot draw inferences.
3	Reads authentic prose on a variety of unfamiliar subjects. Can almost always interpret material, relate ideas, and make inferences. Rarely misunderstands but may miss subtleties and nuances. May have trouble with usually complex structures and low frequency idioms.
4	Reads all styles and forms of prose pertinent to professional or for the general reader Can situate the text in a wide context, follow unpredictable turns of thought, and understand almost all sociolinguistic and cultural references.
5	Functions equivalent to a well educated native reader.

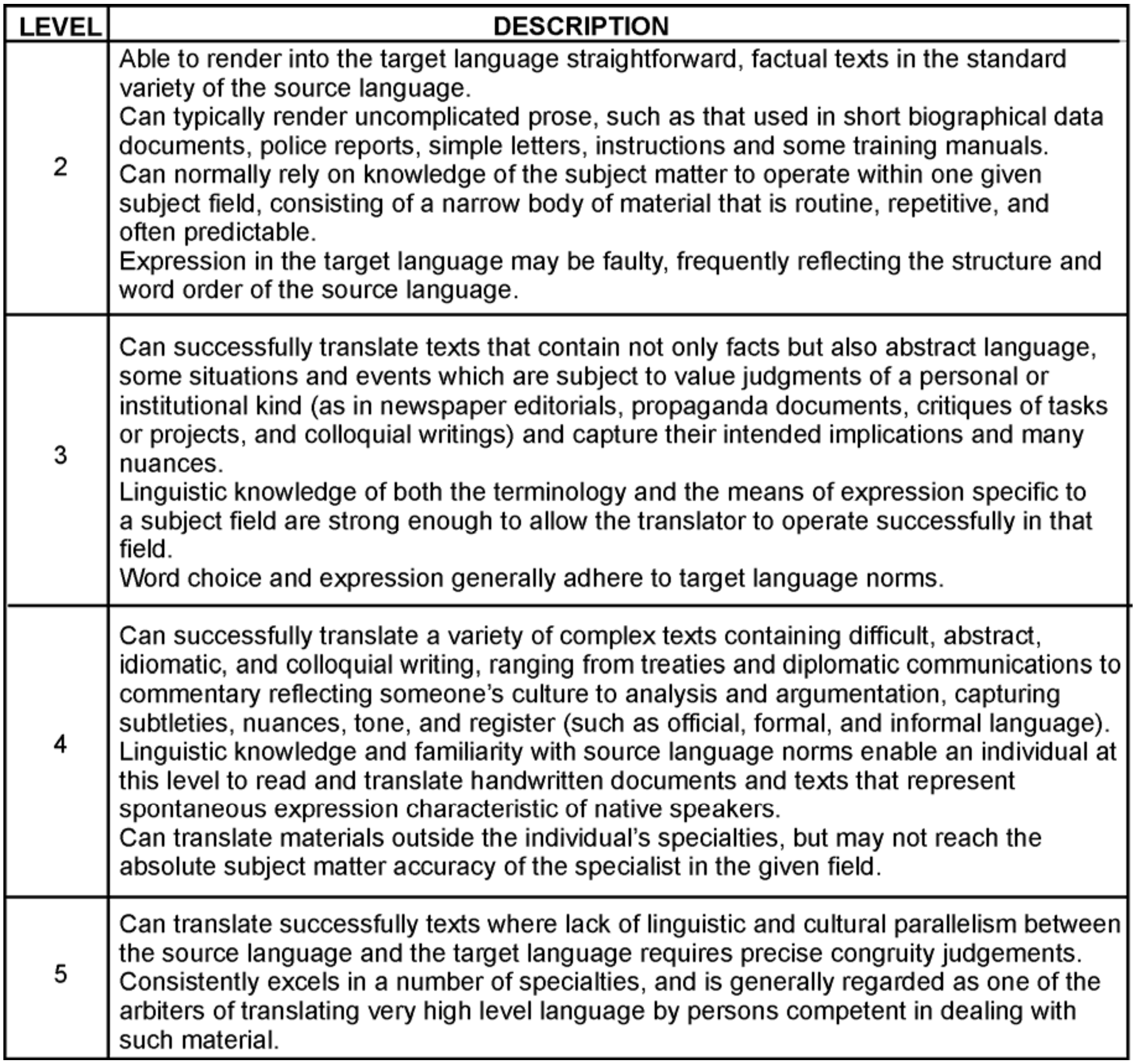
Table G-3. Speaking proficiency levels 2 to 5

LEVEL	DESCRIPTION
2	Fully participates in casual conversations. Can express concrete topics. Understandable to a native speaker not used to dealing with foreigners. Sometimes miscommunicates.
3	Can converse in formal and informal situations. Can discuss practical, social, professional, and abstract topics. Errors never interfere with understanding and rarely disturb the native listener.
4	Tailors language to fit audience. Can discuss all topics normally pertinent to professional needs. Speech is extensive, precise, and appropriate to every occasion with only occasional errors.
5	Functions equivalent to a well educated native speaker.

Table G-4. Writing proficiency levels 2 to 5

LEVEL	DESCRIPTION
2	Meets limited social and work requirements. Can write simple paragraphs about daily situations and events. Writing is comprehensible to a native reader.
3	Writes effectively in most formal and informal exchanges. Writes reports, summaries, and short research papers. Errors never interfere with comprehension and rarely disturb the native reader.
4	Writes in a variety of prose. Writes all topics pertinent to professional or educational needs as well as on social issues of a general nature Errors are rare.
5	Functions equivalent to a well educated native writer.

Table G-5. Translation proficiency levels 2 to 5



LEVEL	DESCRIPTION
2	Able to render into the target language straightforward, factual texts in the standard variety of the source language. Can typically render uncomplicated prose, such as that used in short biographical data documents, police reports, simple letters, instructions and some training manuals. Can normally rely on knowledge of the subject matter to operate within one given subject field, consisting of a narrow body of material that is routine, repetitive, and often predictable. Expression in the target language may be faulty, frequently reflecting the structure and word order of the source language.
3	Can successfully translate texts that contain not only facts but also abstract language, some situations and events which are subject to value judgments of a personal or institutional kind (as in newspaper editorials, propaganda documents, critiques of tasks or projects, and colloquial writings) and capture their intended implications and many nuances. Linguistic knowledge of both the terminology and the means of expression specific to a subject field are strong enough to allow the translator to operate successfully in that field. Word choice and expression generally adhere to target language norms.
4	Can successfully translate a variety of complex texts containing difficult, abstract, idiomatic, and colloquial writing, ranging from treaties and diplomatic communications to commentary reflecting someone's culture to analysis and argumentation, capturing subtleties, nuances, tone, and register (such as official, formal, and informal language). Linguistic knowledge and familiarity with source language norms enable an individual at this level to read and translate handwritten documents and texts that represent spontaneous expression characteristic of native speakers. Can translate materials outside the individual's specialties, but may not reach the absolute subject matter accuracy of the specialist in the given field.
5	Can translate successfully texts where lack of linguistic and cultural parallelism between the source language and the target language requires precise congruity judgements. Consistently excels in a number of specialties, and is generally regarded as one of the arbiters of translating very high level language by persons competent in dealing with such material.

G-2. The Interagency Language Roundtable proficiency level descriptions in this appendix characterize language usage in the areas of listening, reading, speaking, writing, and translating for Levels 2 to 5. Each of the base levels implies control of any previous base level's functions and accuracy. The "plus level" designation is assigned when proficiency substantially exceeds one base skill level and does not fully meet the criteria for the next base level. The plus level descriptions are therefore supplementary to the base level descriptions.

This page intentionally left blank.

Appendix H

Open Source Resources

(The following information is reprinted in whole or part from articles published in the Military Intelligence Professional Bulletin, Volume 31, Issue 2, October-December 2005.)

OPEN SOURCE INTELLIGENCE ON SIPRNET

H-1. Once a decision is made on requirements and means of dissemination, it is time to begin searching for relevant information. Surprisingly, the first place to begin the search for publicly available information is not on the Internet or the DNI's Intelink-SBU, but on the classified networks. The SIPRNET and, to a lesser extent, JWICS, contains numerous links to open source resources.

H-2. The Army open source Portal could be the best place to start your search on the SIPRNET. It has an open source Products section and an Army open source Sites section. These sections will lead you to numerous finished products, and to sites where individual units host their own products. Ideally, one of the command's sites will match your open source requirements, and this will save a lot of time and effort by not having to duplicate the work that others have already done. Also, by reviewing the other units' sites, you can see how other organizations approach open source and gain insight on what may work best for your organization.

H-3. The DA Intelligence Information System (IIS) is another site on the SIPRNET that should be looked at. This site also provides links to numerous open source products and units hosting open source pages. Additionally, DA IIS also has a companion page with links to hundreds of indexed websites available through Intelink-SBU.

A RUNNING START ON THE WORLD WIDE WEB

H-4. Once the search of the Internet finally begins, a common mistake is to think that fee-for-service sites are required, but in the majority of circumstances this is not the case. It will quickly become apparent there are more than enough free or already-paid-for sites available, and the purchase of information by individual units is not required. Of course, there are exceptions for access to unique services or databases, and it is up to the individual unit to determine if they want to spend resources on these services.

H-5. A good first site at which to begin your search for open source content is the Intelink-SBU homepage. Intelink-SBU is a virtual private network managed by the Intelink Management Office which provides authorized users access to unclassified and for official use only information from both the US Government and commercial sources. If your unit does not already have access to the Intelink-SBU network, contact them at info@center.intelink.gov, and they can assist you in gaining access. For OPSEC reasons, the site is not accessible directly from the Internet and requires password authentication for access.

H-6. The Intelink-SBU homepage provides links to unique government sites that are accessible only through the Intelink-SBU network, such as WBIL, which contains basic and background information on 140 countries, the Marine Corps Intelligence Activity, and the NASIC. The US Intelligence Community also provides authorized users free access through Intelink-SBU to premium content providers such as Jane's Electronic Library, Oxford Analytica, Elton B. Stephens Company (EBSCO) Host, Economist Intelligence Unit, and other services that would be cost prohibitive for organizations if they had to pay for the content individually. The site also allows you to customize live feeds from numerous worldwide news services directly to your desktop and, in addition to the links, contains handbooks and reference materials on how to best exploit open source material. Furthermore, in an effort to enhance the user's OPSEC posture, Intelink-SBU also provides "protected access" to the public Internet to allow open source research without divulging personal or organizational identities.

H-7. The AKO Library Program site provides users another Internet tool with a wealth of information. By now, all Army soldiers are aware of AKO, but the fact that the library site exists, and what it contains, is not commonly known. Unlike Intelink-SBU, this site acts more as a gateway to informational type services that one would normally associate with that of a library, and is accessible directly from the Internet. AKO is not limited only to soldiers; non-Army government users and government contractors can also gain access to the site when sponsored by an Army user.

H-8. A separate article would be required to describe all of the products available at this site, but representative examples are Country Watch, which provides up-to-date political, economic, cultural, business and environmental information on 192 countries; and the Student Resource Center link, which provides access to the Worldmark Encyclopedias (worldwide coverage of geographic and cultural issues.) EBSCO Host is available on the AKO site, as well as on Intelink-SBU, providing access to thousands of journals which could contribute to more long-term intelligence issues.

H-9. One unique feature of the AKO library site is the "Ask a Librarian" link. If you experience difficulty trying to find a source or a specific piece of information, you can call on a professional research librarian for help. Simply type in your question, and you will normally receive a response within 48 hours. Regardless of where you are in the world at that moment, you will be able to receive assistance on whatever you are researching.

H-10. Other government library services are available beyond the AKO site. National agency libraries (for example, Library of Congress, National Library of Medicine) and the libraries of military colleges and universities (Combined Arms Research Library, Naval War College) provide searchable sites and content. If the product you require is not available via the Web, many of them will loan the document directly to your command library.

H-11. Neither AKO nor Intelink-SBU are all-encompassing sites that will satisfy all requirements, but these sites need to be fully researched and exploited before any consideration is made to purchase content. While many premium content providers produce original content, the majority repackage much of the information that is already available from these two sites.

H-12. Beyond Intelink-SBU and AKO, the Internet provides a seemingly limitless amount of information that can support your mission. Once the search of the remainder of the Web begins, it is important to ensure that only quality sites are used. Reading Untangling the Web, available on the Intelink-SBU homepage, is recommended prior to searching in order to learn the best techniques to utilize the Web and to understand the potential pitfalls as well. There are numerous sites that look and feel like authoritative websites, but are factually incorrect or biased towards a certain viewpoint that an unsuspecting analyst may not realize.

BEYOND THE WORLD WIDE WEB

H-13. It could be a mistake to overlook the traditional brick-and-mortar library as an source for publicly available information. The quality and quantity of material will vary from location to location, but most libraries have access to inter-library loan programs, providing access to more resources than are available at your local branch as mentioned earlier.

H-14. Depending on your location and budget, private organizations and universities can provide another source for information, and these institutions are also rich in subject matter experts in their respective fields. The Joint Analysis Center (JAC) has unique access to some world-renowned organizations, such as the Chatham House and the Royal United Services Institute, which frequently conduct seminars on topics of direct interest to US European Command (USEUCOM). Our analysts have the opportunity to attend these lectures and hear directly from world leaders and experts. Membership to these types of organizations is relatively expensive; our participation in these seminars is facilitated by our geographical proximity to London. If budget constraints or distance do not allow direct participation, many of these organizations provide e-memberships, at a much-reduced cost compared to full memberships, which may meet your needs.

TAILORED OPEN SOURCES

H-15. Table H-1 contains some of the open source resources specifically tailored for MI research. For more information, visit the MI Library homepage at http://www.universityofmilitaryintelligence.us/mi_library/ default.asp.

Table H-1. Open source research resources

Information Need	Information Source	Location
Regional Information	Department of Army Intelligence Information System (DA IIS)	AKO Password needed: https://www.us.army.mil/suite/page/132281 or https://akocomm.us.army.mil/dadpm
Terrorism and Insurgency	TRADOC Deputy Chief of Staff for Intelligence (DCSINT) Contemporary Operational Environment and Threat Integration Directorate (CTID)	AKO Password needed: https://dcsint-threats.leavenworth.army.mil/Terrorism/default.aspx
	Jane's World Insurgency and Terrorism	Hard and soft copy. Purchase from Jane's or other book vendor. For the online version, access it via Intelink-SBU for free at http://www.intelink.gov//Reference/janes/
	Periscope: Terrorism Database	Access via AKO Library Reference Center.
Cultural Awareness	*Arab Cultural Awareness Handbook*, TRADOC DCSINT CTID	AKO Password needed: https://dcsint-threats.leavenworth.army.mil/Handbooks/default.aspx
	UMI Culture, Foreign Language Integration Center	Public Internet at: http://www.universityofmilitaryintelligence.us/main.asp
Operational Environment Assessments, Country Studies, Regional Security, and Defense Information	TRADOC DCSINT CTID	Access via AKO at: https://dcsint-threats.leavenworth.army.mil/default.aspx.
	Marine Corps Intelligence Activity	Access via Intelink-SBU at: http://www.mcia.intelink.gov/
	TRADOC DCSINT FMSO	Public version available at http://fmso.leavenworth.army.mil/index.htm Access FOUO site via Intelink-SBU: http://www.fmso.intelink.gov/
	Jane's Sentinel Security Assessment	Hard and soft copy. Purchase from Jane's or other book vendor. For the online version, access Jane's Online via Intelink-SBU for free at http://www.intelink.gov//Reference/janes/

Table H-1. Open source research resources (continued)

	Jane's World Armies	For hard copies, contact INSCOM. For online access via Intelink-SBU http://www.mcia.intelink.gov
	Library of Congress Country Studies	Public Internet: http://lcweb2.loc.gov/frd/cs/cshome.html
	Library of Congress Portals to the World	Public Internet: http://www.loc.gov/rr/international/portals.html
	Library of Congress USSR/Eastern Europe Foreign Press Survey	Access via Intelink-SBU: http://www.intelink.gov/loc/eedbrief
	National Ground Intelligence Center	Access via Intelink-SBU: http://dadpm.inscom.intelink.gov/ngic/list.htm
	DA-IIS	AKO Password needed: https://www.us.army.mil/suite/page/132281 or https://akocomm.us.army.mil/dadpm
	Military Policy Awareness Links in the Military Education Research Library Network of the National Defense University	Public Internet: http://merln.ndu.edu/index.cfm?type=page&pageID=3
Daily Intelligence Briefs and Reports	Terrorism Literature Report	Access via Intelink-SBU: http://www.intelink.gov
	Terrorism OSINT Report	
	Swedish Morgen Report	
	Warning Intelligence on the Internet Review	
	Oxford Analytica	Access via Intelink-SBU: http://www.intelink.gov/cgi-bin/rd?http://www.oxan.com/oxweb/
	Jane's Terrorism and Research Center	Access Jane's Online via Intelink-SBU: http://www.intelink.gov//Reference/janes/
Medical Intelligence	Armed Forces Medical Intelligence Center	Access via Intelink-SBU: http://www.afmic.intelink.gov/
Military Equipment	*Worldwide Equipment Guide*, TRADOC DCSINT CTID	AKO Password needed: https://dcsint-threats.leavenworth.army.mil/COE/default.aspx and click on Worldwide Equipment Guide (WEG).
Research Studies: Military, Defense Focus, and Student Papers	Air University Research Web	Public Internet: https://research.maxwell.af.mil/index.aspx

Table H-1. Open source research resources (continued)

Intelligence: Studies, Research, and Journal Articles	Central Intelligence Agency: Studies in Intelligence	Public Internet: http://www.cia.gov/csi/studies.html
	MIPB	Public Internet: http://www.universityofmilitaryintelligence.us/mipb/default.asp
Imagery and Maps	Google Earth: World imagery and other geographic information	Download free software from http://earth.google.com/
	National Geospatial Intelligence Agency	Access via Intelink-SBU: http://intelink.nga.mil
	CIA Map Library	Access via Intelink-SBU: http://www-maps.intelink.gov/
	The Perry-Castañeda Library Map Collection	Public Internet: http://www.lib.utexas.edu/Libs/PCL/Map_collection/Map_collection.html
Scientific and Technical Sources and Research from Foreign Countries	Spires High-Energy Physics Database Indexes over 500,000 articles, papers, preprints, and technical reports	Public Internet: http://www.slac.stanford.edu/spires/hep/
	H-Print Network Search for foreign research in energy, science, and technology	Public Internet: http://www.osti.gov/eprints/
Strategy, Foreign Policy, and Defense	Strategic Studies Institute	Public Internet: http://www.strategicstudiesinstitute.army.mil
	Oxford Analytica	Access via Intelink-SBU: http://www.intelink.gov/cgi-bin/rd?http://www.oxan.com/oxweb/
	Combat Studies Institute	Public Internet: http://cgsc.leavenworth.army.mil/carl/resources/csi/csi.asp
	US Air Force Counterproliferation Center	Public Internet: http://www.au.af.mil/au/awc/awcgate/awc-cps.htm
	Digital National Security Archive; Searchable database with access to once classified documents regarding US Foreign Policy.	Public Internet access at: http://www.gwu.edu/~nsarchiv/

Table H-1. Open source research resources (continued)

Intelligence: Warfighter Systems, Electronic Warfare, and unmanned aerial vehicles	Jane's C4 Jane's Radar & Electronic Warfare Jane's Electronic Mission Aircraft Jane's Unmanned Aerial Vehicles	Purchase from Jane's. For the online version, access it via Intelink-SBU for free at http://www.intelink.gov//Reference/janes/
	Periscope	Access via AKO. Reference→Army Libraries→Library Reference Center
	Global Security	Public Internet: http://www.globalsecurity.org/
Foreign Language: Foreign Media, Translation Tools, and Language Training	Open Source Center	Access via Intelink-SBU: http://www.intelink.gov/cgi-in/rd?https://www.fbis.gov/ Public Internet: http://www.Opensource.gov
	Cultural, Foreign Language Integration Center	Public Internet: http://www.universityofmilitaryintelligence.us
	Language Survival Kits, Defense Language Institute-Foreign Language Center	Public Internet: http://oef.monterey.army.mil/downloadlsk.html
	Google Translation	Public Internet: http://www.google.com/language_tools Access via Intelink-SBU: http://www.intelink.gov/about/machine_translation.htlm
	Foreign Language Resource Center	Access via Intelink-SBU: http://flrc.interlink.gov/

Appendix I

Basic Internet Search Techniques

I-1. The ability to search the Internet is an essential skill for open source research and collection personnel. The Internet provides access to webpages and databases that hold a wide range of information on current, planned, and potential operational environments. *Untangling The Web*: *An Introduction to Internet Research*, a DOD product, provides detailed information on the Internet and Internet search techniques. *Untangling The Web* and similar works are available on the Intelink-SBU homepage at http://www.intelink.gov. In addition, all search engines, commercial databases, and most other Internet resources provide Help pages, overview pages, tours, or tip sheets on how to search the Internet or a specific site. This appendix and the summary in Table I-1 provide basic techniques and procedures for searching the Internet.

CYBER SECURITY

I-2. The Internet is not a benign environment. There are operations and computer security risks to searching the Internet and interacting with Internet sites. Searching the Internet can compromise OPSEC by leaving "footprints" on visited sites. Visiting Internet sites can compromise computer security by exposing vulnerability or providing information that exposing the computer and the network to malicious software or unauthorized access. Users must be vigilant to potential threats; use only authorized hardware and software; and comply with OPSEC measures.

I-3. Awareness of what information the user's computer provides to each server and site on the Internet is the beginning of effective cyber security. Just by visiting a site, the computer transmits machine specifications such as operating system and type and version of each enabled software program, security levels, a history of sites visited during that session, cookie information, user preferences, communication protocol information such as an IP address (for the user and hosting or proxy server), enabled languages, and other computer profile information such as date and time (and time zone), referring URLs (the previous site visited), and more. Available on unprotected computers could be the email address of the user, login information, their certifications. In addition to computer vulnerabilities, just knowing where the research comes from may affect the page accessed. Sites frequently redirect visitors to alternate web pages (or totally block access) based on what user is searching for, where the user is located, what language the user is searching in, and what time of day the user accessed the site.

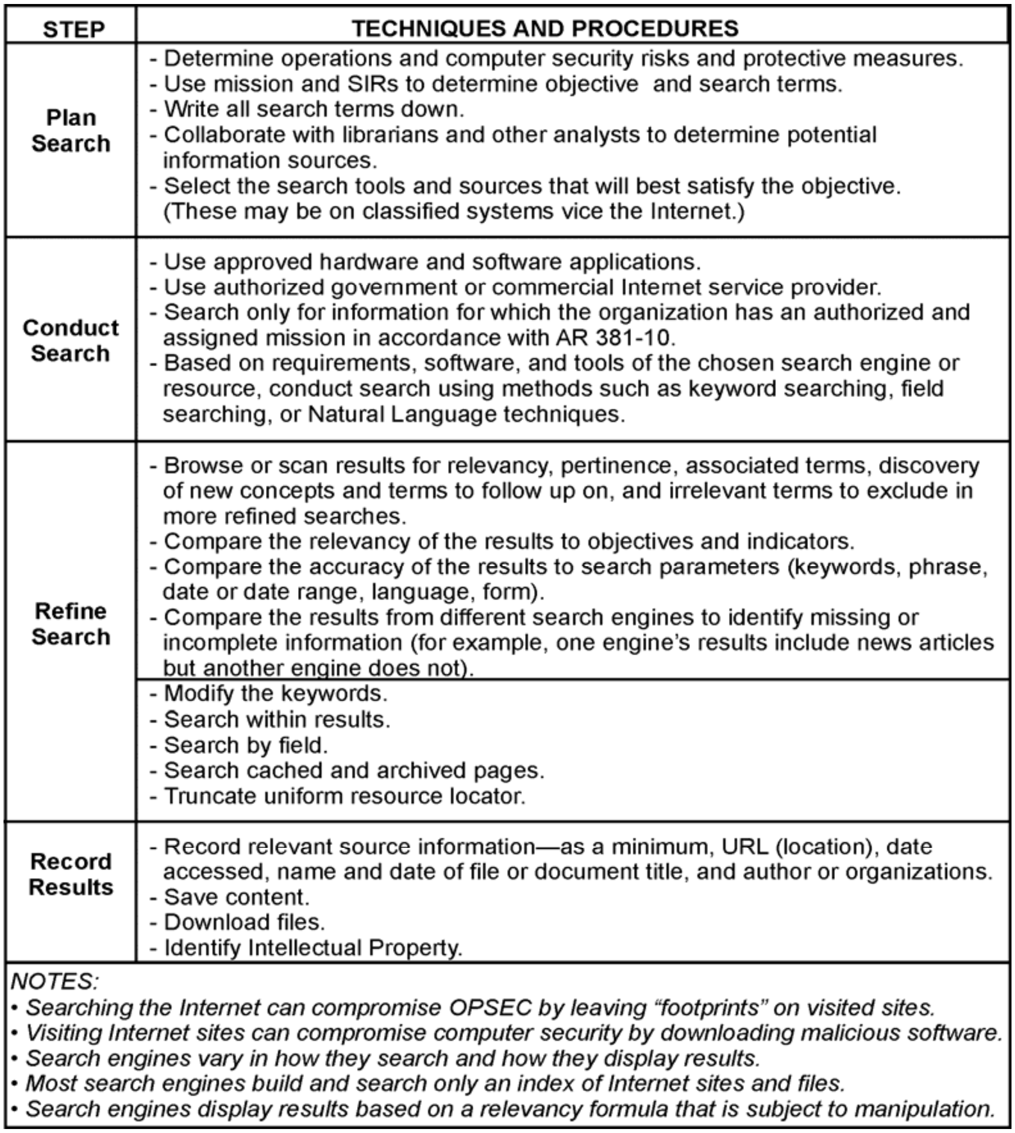
I-4. Uniform resource locator information from the previous sited visited (referring URL) is frequently an OPSEC issue. It identifies some characteristics and interests of the user to the visited site, server, and country. While necessary for an effective search, the use of specific, focused, search terms such as locations, names, and equipment have obvious OPSEC implications.

Example: If the user enters the search terms [bradley us army], the referring URL from the Google hit list would be: http://www.google.com/search?hl=en&q=bradley+us+army. This tells the visited site that the user is searching in English (hl=en) for information on US Army General of the Army Omar N. Bradley or the US Army's Bradley infantry fighting vehicle (IFV).

I-5. All actions taken on a website are logged and saved by the site (and linked to the user with cookie data). User actions include not merely words typed in the search field but also choices in drop-down menus, check boxes, and movement patterns. On many sites, information that the user provides or fills in becomes part of the site and searchable, such as in sites for groups, mailing list archives, forums, weblogs, and wikis. Some of the key information to avoid sharing is not only specific intelligence or research interests and gaps but also military plans, operations, and exercises; maps, charts, locations, and schedules; equipment, operational, and personal vulnerabilities, capabilities, and shortfalls; and lists of names and related numbers such as telephone numbers, birth dates, and identification numbers.

I-6. Information about current threats and tips on cyber security are available online from the US Computer Security Readiness Team at http://www.us-cert.gov.

Table I-1. Internet search techniques and procedures



STEP	TECHNIQUES AND PROCEDURES
Plan Search	- Determine operations and computer security risks and protective measures. - Use mission and SIRs to determine objective and search terms. - Write all search terms down. - Collaborate with librarians and other analysts to determine potential information sources. - Select the search tools and sources that will best satisfy the objective. (These may be on classified systems vice the Internet.)
Conduct Search	- Use approved hardware and software applications. - Use authorized government or commercial Internet service provider. - Search only for information for which the organization has an authorized and assigned mission in accordance with AR 381-10. - Based on requirements, software, and tools of the chosen search engine or resource, conduct search using methods such as keyword searching, field searching, or Natural Language techniques.
Refine Search	- Browse or scan results for relevancy, pertinence, associated terms, discovery of new concepts and terms to follow up on, and irrelevant terms to exclude in more refined searches. - Compare the relevancy of the results to objectives and indicators. - Compare the accuracy of the results to search parameters (keywords, phrase, date or date range, language, form). - Compare the results from different search engines to identify missing or incomplete information (for example, one engine's results include news articles but another engine does not).
	- Modify the keywords. - Search within results. - Search by field. - Search cached and archived pages. - Truncate uniform resource locator.
Record Results	- Record relevant source information—as a minimum, URL (location), date accessed, name and date of file or document title, and author or organizations. - Save content. - Download files. - Identify Intellectual Property.
NOTES: • *Searching the Internet can compromise OPSEC by leaving "footprints" on visited sites.* • *Visiting Internet sites can compromise computer security by downloading malicious software.* • *Search engines vary in how they search and how they display results.* • *Most search engines build and search only an index of Internet sites and files.* • *Search engines display results based on a relevancy formula that is subject to manipulation.*	

PLAN SEARCH

I-7. Intelligence personnel use their understanding of the supported unit's mission, the SIRs, indicators, and the Internet to plan, prepare, and execute their search. The SIR helps to determine what information to search for and where to look. The SIR provides the focus and initial keywords that intelligence personnel use to search for information. Once identified, the analyst or collector records these search terms and uses them to locate information within the Internet.

> ***Example:*** If a unit is planning a humanitarian assistance operation in the Sudan, the specific IR may be "Where are refugee concentrations in the Sudan?" The task for the analyst could be, "Locate the humanitarian relief organizations operating food distribution centers in the Sudan," "Locate population centers in the Sudan," "Locate concentrations of militia forces in the Sudan," and "Identify areas of militia operations in the Sudan that occurred in the last 30 days." The location of NGO aid centers, food, water, and hostile paramilitary forces are possible indicators of where refugees may or may not concentrate. Based on the SIRs and indicators, the search objective is to locate refugee concentrations based on the position of food and militia forces in the Sudan. The indicators that may be useful search terms include: Sudan, refugee, humanitarian relief, food distribution, militia, and water sources.

I-8. After determining the focus and keywords, the intelligence personnel use an Internet browser to connect to a previously identified Internet site. If there are no previously identified sources, the analyst or collector can connect to a communications or service site to collaborate with other analysts or use a search engine to identify Internet sites, respectively. Since search engines do not index the entire Internet, the communications capabilities of the Internet are important means of collaboration with authors, experts, points of contact, and other people who know the information or have the information stored in off-line databases or hardcopy.

CONDUCT SEARCH

I-9. Intelligence personnel should avoid the temptation of using one favorite search engine to the exclusion of others. Each search engine has its strengths and weaknesses. Organizational standards, research experience, and peer recommendations guide the selection of which search engine to use in any particular situation. Generally, a thorough search often requires the use more than one search engine and even then, the information may not be complete. As a rule, if a trained analyst or collector cannot find the information using multiple search engines and common search techniques within 30 minutes, it is possible that the information is not on the Internet, not indexed, or not in a retrievable format. At that point, the analyst or collector should seek assistance from other personnel, digital but non-Internet resources such as commercial and in-house databases, and non-digital resources available at government or university libraries.

Search Engines

I-10. Intelligence personnel use search engines and search terms to locate Internet sites and find information within the Internet site. Search engines allow the user to search for text and images in millions of web pages. The different commercial and government search engines vary in what they search, how they search, and how they display results. Most search engines use programs called webcrawlers to build indexed databases. A webcrawler searches Internet sites and files and saves the results in a database. The search engine, therefore, is actually searching an indexed database not the content of the site or an online database. The search results also vary between search engines because each engine uses different webcrawlers and searches different sites. Most engines display search results in order of relevancy with a brief description and a hyperlink to the referenced Internet file or site.

- **Webcrawler.** Search engines have an index database built by a webcrawler. The webcrawler or spider is a different application than the search engine. The crawler is like some voracious monster with an insatiable appetite, it roams the Internet 24 hours a day, 7 days a week, searching for information. Once it finds a Website, it then indexes and saves it in a database relevant to the search engine. Some search engines have their own spiders while others use commercial contracted spider programs to develop their databases. In addition, each spider may use a different approach to acquiring data. One spider may be programmed to research only the titles of webpages and the first few lines of text. Other spiders research virtually the entire website with the exception of graphics or video files. Because search engines may use different webcrawler software with different ways to index and save data, each separate search engine may yield different results. Also, the search engine provider can supplement or alter the spider software's index to ensure the website of specific customers appears in the index.

- **Relevancy Formulas.** The relevancy formula evaluates how well the query results match the request. For webpages that are commercially oriented, designing the page to achieve the highest ranking has become an art form. For some search engines, the process is simple, the higher the bid, the higher the site's ranking. Search engines are continually changing their relevancy formulas in order to try to stay ahead of web developers. Some web designers, however, load their sites with words like "free," "money" or "sex" in an attempt to influence the search engine's relevancy formula. Other web designers engage in practices called "spamdexing" or "spoofing" in an attempt to trick the search engine. The significance of the relevancy formulas to the user is the importance of understanding that the keyword in the search does not necessarily yield the same results with every search engine. This becomes obvious when the user considers that relevancy formulas vary from search engine to search engine and are in a constant state of evolution. In some formulas, the placement of the keywords yields different results if rearranged because the search engine's relevancy formula places more emphasis on the first words in the search string. Relevancy formulas may also assume importance depending on the type of search being done. For instance, a field-search, which is limited to the webpage itself (for example, title, URL, and date) may be more critical than a full-text search.

I-11. As search engines evolve, some engines have become adept at finding specific types of information such as statistical, financial, and news more effectively than other engines. To overcome this specialization, software engineers developed the metasearch engine. The metasearch engine allows the user to query more than one search engine at a time. On the surface this would seem to be the final answer to the search question; just query all search engines at one time. Unfortunately, it is not quite that easy. Since it must be designed to work with all search engines that it queries, the metasearch engine must strip out each search parameter to the lowest common denominator of each search engine. For example, if a particular search engine cannot accommodate phrases in quotation marks or a type of Boolean function then the metasearch engine will eliminate that function from the search. The resulting search, in many instances, then becomes too broad and less useful than a well-formatted search using a search engine that the user is familiar with and that is known to be good at locating the type of information required.

I-12. With an understanding how search engines work, intelligence personnel—

- Conduct an initial search using unique key words or key word combinations and, if possible, multiple search engines. Avoid using one search engine to the exclusion of others.
- Evaluate the relevance and accuracy of the search results to research objectives, indicators, and search parameters. Do not rely on the relevancy formula of the search engine, particularly commercial search engines, to list the most relevant information source at the top of the list.
- Conduct follow-on searches using refined terms and methods. Refining terms includes inverting the word order, changing the case, searching common misspellings, correcting spelling, and adjusting search terms. Refining search methods includes searching within results that are similar to the desired information.

Search by Keyword

I-13. In keyword-based searches, the intelligence personnel should consider what keywords are unique to the information being sought. The analyst or collector needs to determine enough keywords to yield relevant results but not so many as to overwhelm them with a mixture of relevant and irrelevant information. They should also avoid common words such as “a,” “an,” “and,” and “the” unless these words are part of the title of a book or article. Most search engines ignore common words. For example, if looking for information about Russian and Chinese tank sales to Iraq, the analyst or collector should not use tank as the only keyword in the search. Instead, they should use additional defining words such as “**Russian Chinese tank sales Iraq.**”

I-14. In some search engines, Boolean and Math logic operators help the analyst or collector establish relationships between keywords that improve the search. Using the operators listed in Table I-2, the search engine searches for Russian and tank together when the analyst or collector places the words within parenthesis; (for example, **Russian tank).** If they want to exclude Chinese tank sales from the search result then he uses **(Russian tank) NOT (Chinese tank) sale Iraq** in the search. The analyst or collector can also use a “NEAR” search when the relationship and the distance between the terms are well established. For example, if the analyst or collector is looking for incidents of earthquakes in Pakistan and news articles normally place the placename of the location of an attack within five words of “earthquake” in the title of body of the article then they use earthquake NEAR/5 Pakistan in the search.

Table I-2. Boolean and math logic operators

FUNCTION	BOOLEAN	EXAMPLE
Must be present*	AND	Chemical AND weapon chemical +weapon
Must not be present	NOT	Africa NOT Sudan Africa -Sudan
May be present	OR	chemical OR biological
Complete phrase	“ “	“Chinese tank sales to Iraq”
Nested	( )	(Shining Path)
Near**	NEAR	“White House” NEAR “airspace incursion”
Wildcards	word* or *word	gun* (gunpowder, gunsight)
Stopwords***	“” “”	“”OR”” (do not ignore OR)

NOTES:

*In some search engines, the default is AND. In this case you will have to use the OR operator or the equivalent option on pull down menu.

**Some engines use ten words as the distance between NEAR words. A forward slash and a number indicates the distance between the terms.

***Stopwords are words that search engines ignore because they are too common or are reserved for a special operation. There is no uniform list, but they include words such as an, any, to, with, from. They also include the standard Boolean operators AND, NOT, NEAR, and OR.

Search in Natural-Language

I-15. An alternative to using a keyword search is the natural language question format. Most of the major search engines allow this capability. The analyst or collector obtains the best results when the question contains good keywords. One of the major downsides to this technique is the large number of results. If the needed information is not found in the first few pages then they should initiate a new search using different parameters.

REFINE SEARCH

I-16. Normally, the first few pages of search results are the most relevant. Based on these pages, the analyst or collector evaluates the initial and follow-on search to determine if the results satisfied the objective or requires additional searches. During evaluation, they compare—

- Relevancy of the results to the objective and indicators.
- Accuracy of the results to search parameters (keywords, phrase, date or date range, language, format).
- Results from different search engines to identify missing or incomplete information (for example, one engine's results include news articles but another engine does not).

Modify the Keyword

I-17. If initial search attempts are unsatisfactory, the analyst or collector can refine the search by changing the following:

- **Order.** Search engines may place a higher value or more weight on the first word or words in a multiple word or phrase search string. Changing the word order from "insurgents Iraq" to "Iraq insurgents" may yield different search results.
- **Spelling/Grammar.** Search engines attempt to match the exact spelling of the words in the search string. There are search engines that do recognize alternate spellings or prompt the user to correct common misspellings. Changing the spelling of a word from the American-English "**center**" to the British-English "**centre**" may yield different results. Changing the spelling of a transliterated name from "**Al-Qaeda**" to "**al-Qaida**," "**al-Qa'ida**," "**el-Qaida**," or "**al Qaeda**" generates different results that may be useful depending upon the objective of the search. Some search engines provide this capability for a "sounds like-type" search that eliminates or reduces the manual entry of each variation. Looking for common misspellings or common, grammatically incorrect, short phrases may be useful in yielding results from a source for which English is a second language or the language of the webpage is in a second language for the web designer or web contributor.
- **Case**. Search engines may or may not support case sensitive searches. Like spelling, some engines attempt to match the word exactly as entered in the search. The intelligence personnel should use all lowercase letters for most searches. When looking for a person's name, a geographical location, a title, or other normally capitalized words then the intelligence personnel should use a case sensitive search engine. Changing the case of a word from "**java**" to "**JAVA**" changes the search result from sites about coffee to sites about a software program.
- **Variants.** Intelligence personnel use terms that are common to their language, culture, or geographic area. Using variants of the keyword such as changing "policeman" to "**cop**," "**bobby**," "**gendarme**," "**carabiniere**," "**policía**," "**politzei**," or other form may improve search results.

Search Within Results

I-18. If the initial or follow-on search produces good but still unsatisfactory results, the analyst or collector can search within these results to drill down to the webpages that have a higher probability of matching the search string and containing the desired information. Most of the popular search engines make this easy by displaying an option such as "search within these results" or "similar pages" that the user can select. Selecting the option takes the analyst or collector to webpages with additional, related information.

Search by Field

I-19. In a field search, the analyst or collector looks for the keywords within the URL as opposed to searching the entire Internet. The best time to use a field search is when the search engine returned a large number of webpages. While capabilities vary by search engine, some of the common field search operators are—

- Anchor: Searches for webpages with a specified hyperlink.
- Domain: Searches for specific domains (see Table I-3 or visit http://www.iana.org).
- Like: Searches for webpages similar or related in some way to specified URL.
- Link: Searches for specific hyperlink embedded in a webpage.
- Text: Searches for specific text in the body of the webpage.
- URL: Searches for specific text in complete Web addresses.

I-20. With the millions of URLs on the web, the analyst or collector is faced with a myriad of sites that may or may not actually be produced and maintained by the type of organization represented by the majority of web pages in that domain (see Table I-3). Certain domains, such as ".mil," ".edu," and ".gov" are consistently reliable as being administered and authored by those organizations. Several domains have, over the years of ever-increasing numbers of Internet participants, become highly suspect as to the validity of the organization using such a domain extension. In particular, the open source information gatherer must not take ".org," ".info," or ".net" extensions as necessarily produced by a bona fide organization for that domain. Each country has a two-digit digraph and registers domains with Internet Assigned Number Authority (http://www.iana.org). The country digraph is important because it indicates the site in another country. For example, .uk (United Kingdom) has more than a billion sites indexed; .cn (China) has 700 million sites; .fr (France) has more than 600 million sites, while the domains you listed have fewer than a million sites each (for instance, .aero, .jobs, .museum, .pro).

Search in Cache and Archive

I-21. Sometimes a search or an attempt to search with results returns a URL that matches exactly the search objective but when the analyst or collector tries to link to the site, the link or the site is no longer active. If the search engine captures data as well as the URL locator, they can select "cached" link to access the original data. Another technique is search in an Internet archive site such as www.archive.org for the content. The analyst or collector needs to be aware that this information is historical and not subject to update by the original creators.

Truncate the Uniform Resource Locator

I-22. In addition to using the search engine to search within results, the analyst or collector can also manually search within the results by truncating the URL to a webpage. The analyst or collector works backward from the original search result to the webpage or homepage containing the desired information or database by deleting the end segments of the URL at the "/" forward slash. This technique requires a basic understanding of how webpage designers structure their webpage.

Table I-3. Top-level domains

DOMAIN	DESCRIPTION	OPERATOR/SPONSOR
.Aero	Reserved for members of the air-trasport industry	Société Internationale de Télécommunications Aéronautiques
.biz	Restricted to business	NeuLevel, Incorporated
.com	Unrestricted top-level domain intended for commercial content	VeriSign Global Registry Services
.coop	Reserved for cooperative associations	Dot Cooperation limited Liability Company
.edu	Reserved for postsecondary institutions accredited by an agency on the US Department of Education's list of Nationally Recognized Accrediting Agencies	Educause
.gov	Reserved exclusively for the US Government	US General Services Administration
.info	Unrestricted top-level domain	Afilias Limited
.int	Used only for registering organizations established by international treaties between governments	Internet Assigned Number Authority
.jobs	Reserved for human resource managers	Dot Cooperational Limited Liability Company
.mil	Reserved exclusively for the US military	US Department of Defense Network Information Center
.museum	Reserved for museums	Museum Domain Management Association
.name	Reserved for individuals	Global Name Registry
.net		VeriSign Global Registry Services
.org	Intended for noncommercial use but open to all communities	Public Interest Registry
.pro	Restricted to credentialed professionals and related entities	RegistryPro

Note: *Country code domain digraphs are available at http://www.iana.org*
Source: *Internet Assigned Number Authority at http://www.iana.org*

RECORD RESULTS

I-23. Intelligence personnel must save the search results that satisfy the research objective. Saving the results enables the analyst or collector to locate the information later as well as to properly cite the source of the information in intelligence reports and databases. While printing a hardcopy is an option, a softcopy (electronic) record of the search results provides a more portable and versatile record. Also, some intelligence organizations have software tools specifically designed for creating a complete record of the webpage content and metadata. The following are some basic techniques for saving an electronic record of the search results.

- **Bookmark.** Bookmark the link to the webpage using the "bookmarks" or "favorites" option on the Internet browser.
- **Save Content.** Save all or a portion of the webpage content by copying and pasting the information in text document or other electronic format such as a field within a database form. The naming convention for the softcopy record should be consistent with unit electronic file management standards. As a minimum, the record should include the URL and retrieval date within the file.
- **Download Files.** Download audio, image, text, video, and other files to the workstation. The naming convention for the softcopy record should be consistent with unit electronic file management standards.
- **Save Webpage.** Save the webpage as .mht, .pdf, .doc, .html—or other specified format—that creates a complete, stable record of the webpage content. It may be necessary to include the date and time in the file name in order to ensure a complete citation for the information.
- **Record Source.** As a minimum, record the author or organization, title, publication or posting date, retrieval date, and URL locator of the information in a citation format that is consistent with the American Psychological Association and Modern Language Association style manuals. The following is an example of a American Psychological Association citation for an Internet document:

  > BBC News (2005). Sudan: A Nation Divided. Retrieved 16 May 2005 from http://news.bbc.co.uk/1/hi/in_depth/africa/2004/sudan/default.stm

- **Identify Intellectual Property.** Identify intellectual property that an author or an organization has copyrighted, licensed, patented, trademarked, or otherwise taken to preserve their rights to the material. Some webpages list the points of contact and terms of use information at the bottom of the site's homepage. When uncertain, intelligence personnel should contact their supporting Judge Advocate General office before publishing information containing copyrighted or similarly protected intellectual property.

This page intentionally left blank.

Appendix J

Operational Environment Assessment

J-1. Open source research, coupled with an understanding of the COE, is the basis for an operational environment assessment. An operational environment assessment is a technique designed to apply the COE variables to a specific region, nation states, or non-state actors. It encompasses all the conditions, circumstances, and influences that affect the employment of military forces and the decisions of the unit commander. The operational environment assessment consists of a detailed examination and analysis of the eleven critical variables of the COE, their interaction and reciprocal relationships. Based on this analysis, the operational environment assessment identifies trends and issues with which units may have to grapple during their planning, preparation for, and execution of operations. As an unclassified document (in whole or part), the operational environment assessment also serves as a useful tool for individual and collective training during preparation for operations in a specific area.

J-2. Every operational environment is complex, dynamic, and multi-dimensional. An operational environment assessment provides a detailed look at a specific operational environment in terms of the eleven critical variables and their impacts. It identifies the critical relationships between the variables in the operational environment, how they affect one another, and how this affects military operations. Some variables are dependent variables, whose value is determined by that of one or more other variables. For each dependent variable, the assessment identifies the most significant independent variables that are linked to it and shows their impact on the dependent variable under investigation.

J-3. To understand any operational environment, one needs to study and understand the synergy and interaction of variables and their reciprocal influence on one another. Within the analysis by variables, the operational environment assessment identifies key actors (nation-state and non-state) and assesses their impact on the operational environment. This analysis of variables and actors helps to identify relevant trends and issues in the operational environment over time. Given the dynamic and fluid nature of the operational environment under investigation, an operational environment assessment requires continuous updates and additions in order to remain current and relevant.

CRITICAL VARIABLES

J-4. Open source research must address the eleven critical variables that describe the conditions in the potential operational environment. Collectively, these variables provide a complete framework for thoroughly assessing and understanding the complex and ever-changing combination of conditions, circumstances, and influences that affect military operations in any given real-world operational environment. While these variables can be useful in describing the overall (strategic) environment, they are most useful in defining the nature of specific operational environments. The variables do not exist in isolation from one another. The linkages of the variables cause the complex and often simultaneous dilemmas that a military force might face. Only by studying and understanding these variables—and their dynamic and complex combinations and interactions—will the US Army operational and tactical forces be able to keep adversaries from using them against them or to find ways to use them to its own advantage.

J-5. The eleven critical variables shown in Figure J-1 are discussed below.

- **Physical Environment.** The physical environment defines the physical circumstances and conditions surrounding and influencing military forces and the execution of operations. The defining factors include urban settings and other complex terrain, all relevant infrastructures, weather, topography, hydrology, and environmental concerns.

- **Nature and Stability of the State (or Other Critical Actors).** It is important to understand the nature and stability of the state or states with which or in which military operations take place. This variable, however, refers to the internal cohesiveness of the various political actors (nation-states as well as non-state actors) with respect to the population, economic infrastructures, political processes, military and/or paramilitary forces, authority, goals, and agendas.

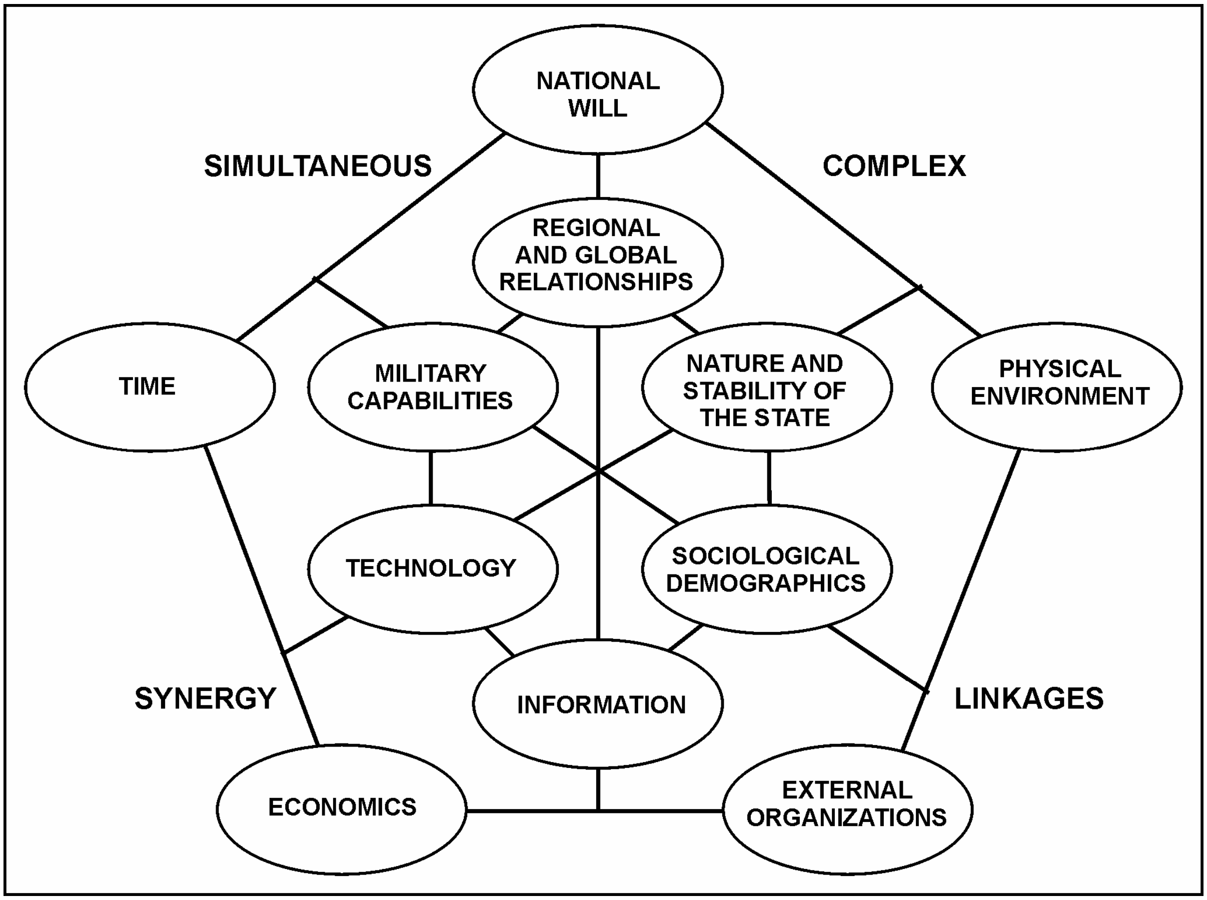


Figure J-1. Critical variables of the operational environment

- **Sociological Demographics.** Sociological demographics refer to the traits and trends that have an impact on the human population of a particular group, area, country, or region. This includes its cultural, religious, and ethnic makeup.
- **Regional and Global Relationships.** Regional and global relationships include political, economic, military, or cultural mergers and partnerships. An actor's membership in or allegiance to such a relationship can determine its actions in terms of support, motivation, and alliance construct.
- **Military (or Paramilitary) Capabilities.** The military or paramilitary capabilities of various actors in the operational environment are a key concern. This variable includes such factors as equipment, manpower, training levels, resource constraints, and leadership issues. The military variable interacts with the other variables, and all the other variables can affect military and paramilitary capabilities.

- **Technology.** Technology represents the level or sophistication of technologies an actor could bring to the operational environment. Their level of integration and exploitation, and any niche technologies are important.
- **Information.** Information involves the access, use, manipulation, distribution, and reliance on information technology systems, both civilian and military, by a nation-state or non-state entity. Information technology is the systems or mechanisms for preserving or transmitting information.
- **External Organizations.** External organizations refer to those entities found in an operational environment, which come from outside the confines of that specific operational environment but could impact the battlefield and related battlespace. Such impact could be both positive and negative in nature—at the strategic, operational, and tactical levels and across the entire spectrum of conflict. An understanding of each group's varying and dynamic agendas, media philosophies, and international connections can be critical to the success of any military endeavor.
- **National Will (or Actors' Will).** Will encompasses a unification of values, morals, and effort between the population, the leadership or government, and the military or paramilitary forces. Through this unity, all parties are willing to sacrifice individually for the achievement of the unified goal. The interaction of military actions and political judgments, conditioned by national will, further defines and limits the achievable objectives of a conflict, thereby determining its duration and conditions of termination. It is imperative to study not just the national will of the state actors but also the will of the non-state actors (such as ethnic groups, political groups, insurgents, terrorist groups, and criminal organizations) involved in the operational environment. The will of non-state actors often affects the environment more significantly.
- **Time.** The time available for commanders to accomplish missions is determined by the goals and associated milestones established by the national political leadership. It is within this "timeframe" that all the elements of power—diplomatic, informational, military, and economic—must operate to achieve national objectives. How much time is available and how long events might take will affect every aspect of military planning, to include force package development, force flow rate, quality of intelligence preparation of the AO, and the need for forward-deployed forces and logistics. Time is often in favor of actors other than the US and its friends and multinational or coalition partners. Such actors often can afford to prolong the conflict and try to outlast the US will to continue operations in a particular operational environment.
- **Economics.** There may be significant differences among nation-states, organizations, or groups, regarding how they produce, distribute, and consume goods and services. Being able to affect another actor, positively or negatively, through economic rather than military means may become the key to regional hegemonic status or dominance. Economic deprivation is also a major cause of conflict. One actor may have economic superiority over another for many reasons, including access to natural resources or energy. Control of and access to natural or strategic resources can cause conflict. Military personnel operating in this complex environment may need to look beyond political rhetoric to discover a fundamental economic disparity among groups.

J-6. Variables are fluctuating factors or elements that make up an operational environment. When operationalized, they define the conditions, circumstances, and influences that affect the employment of military forces and influence the options and decisions of the commander. The starting point for understanding the operational environment are those critical variables that reside in all operational environments and have the greatest impact on the military. See FM 7-100 for detailed information on the critical variables and operational environments.

ASSESSMENT METHODOLOGY

J-7. An operational environment assessment provides a methodology for examining and understanding any potential operational environment. In effect, this assessment is an application of the COE concept to the specific operational environment under investigation. The methodology involves the following steps:

- **Define Variables.** Defining a variable simply means describing the nature and composition of each of the eleven variables in a specific operational environment.
    - To help focus and facilitate the research effort, it is necessary for analysts to break down each variable into its subcategories of information (main topics and subtopics). This topic outline defines the scope and focus of the variable and serves as a guide for research on the variable in question.
    - All eleven variables are present in all operational environments, but different operational environments typically will require different outlines within the variables. For example, a landlocked operational environment will not require discussion of coastlines or ports under the Physical Environment variable or of naval forces under Military Capabilities. As analysts begin to populate the outline with information gleaned from their research, further refinements and additions to the headings and subheadings may be necessary.
    - Because of the interrelated and sometimes overlapping nature of the individual variables, some subsets of available information may have a place under more than one variable. For instance, information technology might be addressed under both Information and Technology and could have an impact on several other variables.
    - Analysts may determine links between the subcategories of one variable and the same, similar, or related subcategories that may exist under other variables. Thus, it may be necessary for one variable description to repeat some information contained under another variable or to cross-reference or provide an electronic link to it. Such linkages may be obvious when constructing the original topic outlines for the variables, or may become evident later—when analysts are populating the outlines with information.
- **Populate the Variable Outlines.** Analysts then conduct extensive research to populate the outline for each variable.
    - This can be done with relevant information gleaned from all available open sources. The various sources can include official government documents, think-tank products, academic journals, open source periodicals, foreign press, websites, and interviews or discussions with various subject matter experts. Each variable is described as it applies to the specific operational environment in question. This step is an ongoing process, involving continuous updates as new or better information becomes available or when conditions change.
    - Much of the most useful information about the potential operational environment may be available from open sources. An operational environment assessment can reveal key areas where information gaps exist. These gaps may become PIRs during the planning and the execution of operations—to be targeted by further open source research or perhaps by scarcer, more sensitive intelligence means. The operational environment assessment and underlying data form the basis of the GMI database and continuation of the operational environment assessment process when the unit deploys to the AO—possibly layered with additional information from classified sources.
- **Analyze Relationships, Linkages, and Trends**. The next step highlights the key cause-and-effect relationships and linkages among the variables (Figure J-2).
    - In any operational environment assessment, the key to understanding the significance of the variables is to understand the relationships among the variables and how these affect military operations in the selected operational environment. Therefore, analysts can develop a matrix for each dependent variable that shows its critical relationships to other

variables. This makes it possible to analyze each dependent variable from the perspective of its relationship or connectivity to other, independent variables. From this relational analysis, critical trends and issues become more evident.

- Clearly it is impossible to show every potential linkage and trend. Analysts should, however, identify and examine the most significant independent variables (linked to the dependent variable) to show their specific relationships to and impacts on the dependent variable under investigation. For instance, the variable of military capabilities is dependent on or influenced by virtually all the other variables.

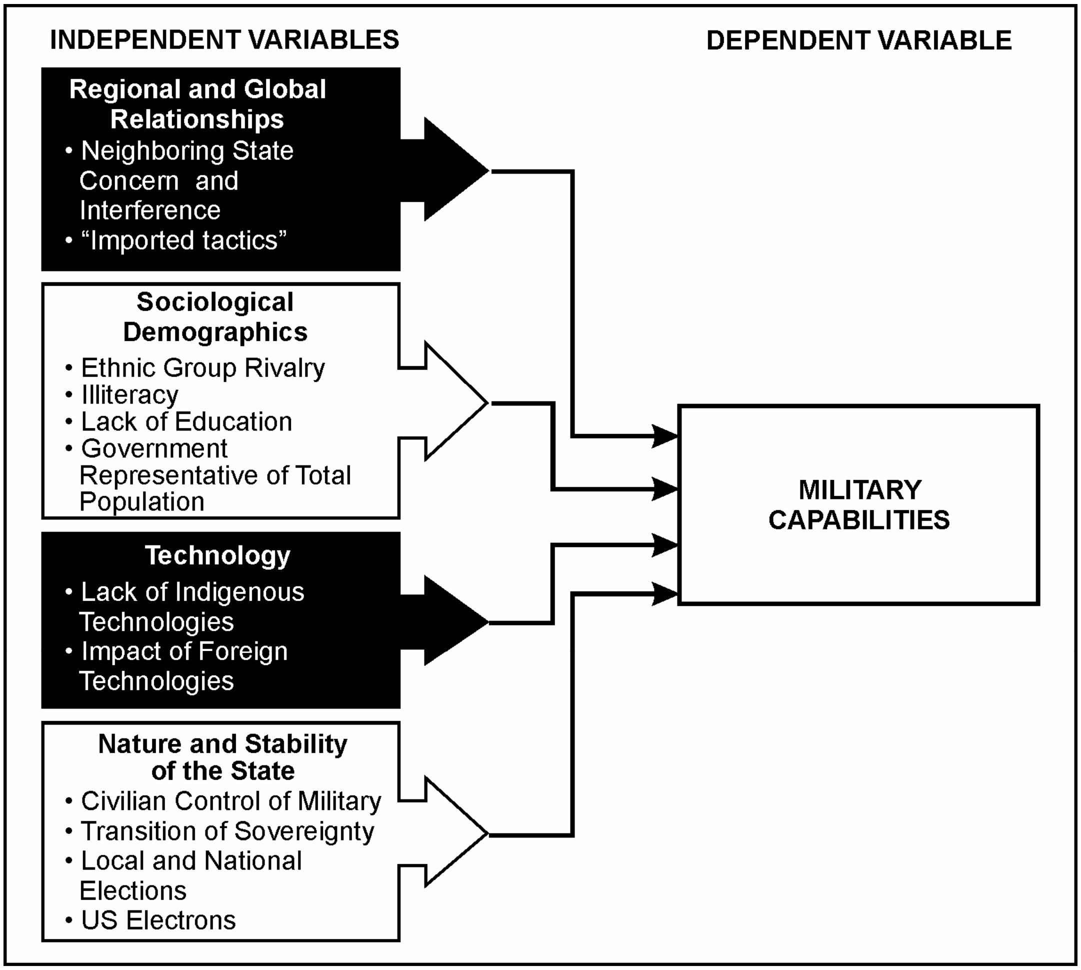

INDEPENDENT VARIABLES
DEPENDENT VARIABLE
Regional and Global Relationships
• Neighboring State Concern and Interference
• "Imported tactics"
Sociological Demographics
• Ethnic Group Rivalry
• Illiteracy
• Lack of Education
• Government Representative of Total Population
Technology
• Lack of Indigenous Technologies
• Impact of Foreign Technologies
Nature and Stability of the State
• Civilian Control of Military
• Transition of Sovereignty
• Local and National Elections
• US Electrons
MILITARY CAPABILITIES

Figure J-2. Example of possible links between dependent and independent variables

- Identify Key Facts and Impacts. Finally, analysts identify and highlight key facts and potential operational impacts for each variable.
  - From the definition of variables and relationship analysis, analysts can attempt to identify trends over time. This trends analysis can provide an understanding of the dynamics of the variables and their impacts in a selected operational environment.
  - Analysis can also identify possible trigger events in the operational environment based on relationships of variables across time.

J-8. As previously mentioned, the results of open source research such as the operational environment assessment contributes to the body of knowledge about the operational environment that enables commanders and their subordinates to better understand the many variables on the affect the military operations. This improved understanding gained through continuous research and analysis of the critical variables assists commanders in defining better intelligence requirements that will drive the intelligence warfighting function throughout planning, preparation for, and execution of military operations.

J-9. Examples of operational environment assessments are available from the TRADOC Deputy Chief of Staff for Intelligence on the Contemporary Operational Environment and Threat Integration Directorate's website at https://dcsint-threats.leavenworth.army.mil/default.aspx.

Appendix K

Media Analysis

K-1. The following OSC's media analysis technique is a systematic examination over time of the content and behavior of a set of media in a country or several countries or on one issue to detect trends, patterns, and changes in the media and to explain them within the context of the media environment. These techniques are based on methods and experience gained during OSINT operations focused on highly authoritarian political systems during World War II, the Cold War, where media control was tightly centralized within the regime. Analysts have adapted these media analysis techniques to other media environments and political systems.

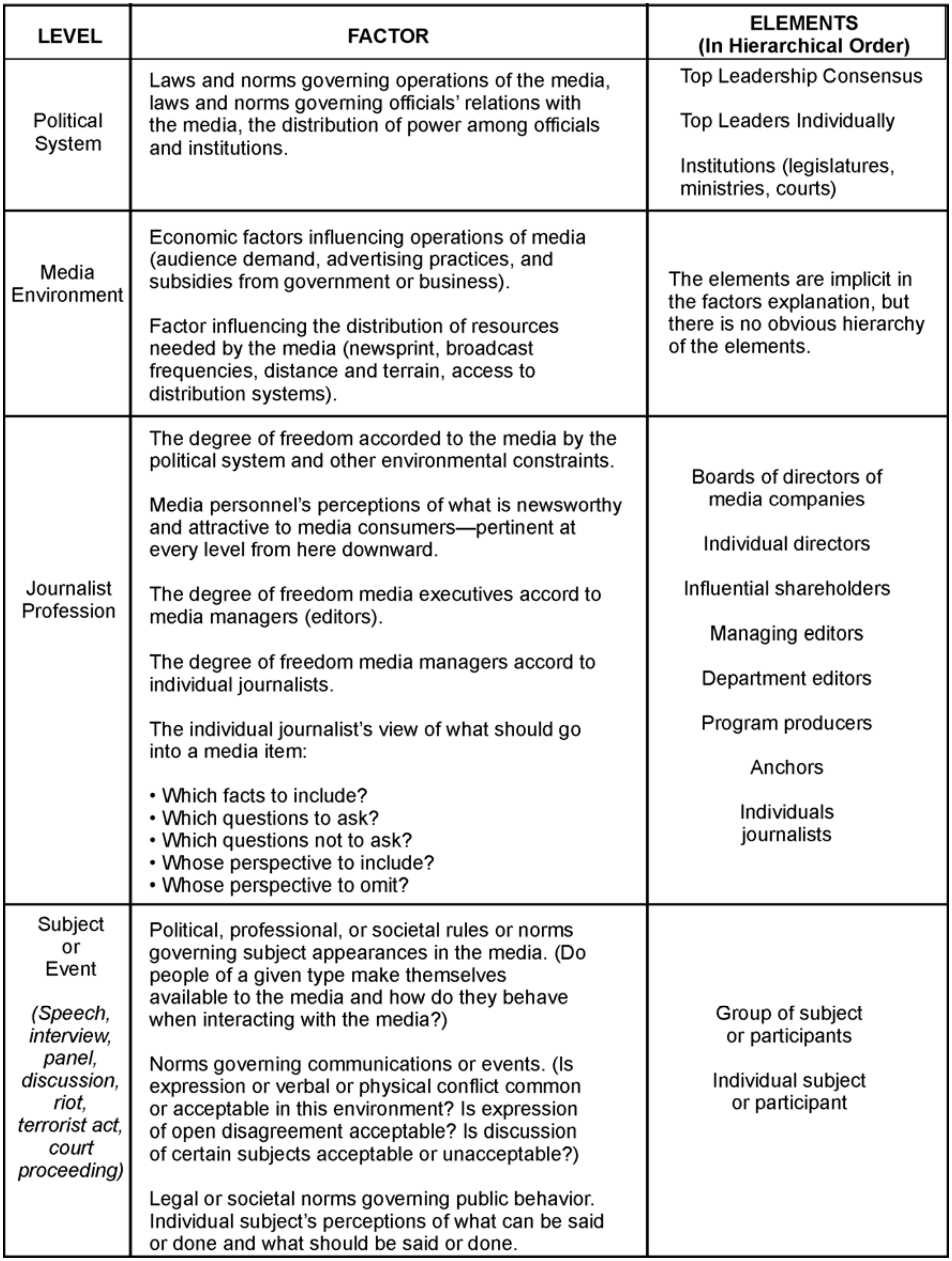
MEDIA CONTROL

K-2. Applying media analysis to different media environments, the analyst must be aware of how the different elements of media control act within the media environment, how much weight attends each element, and which elements of control are of interest to us and our customers. Media environments fall into the following types based on the degree control.

- **Government-Controlled.** Control over the media is tightly centralized within the authoritarian regimes. The dominant element of control is the top political leadership. These regimes use censorship mechanisms to exercise control over media content prior to its dissemination.
- **Semi-Controlled**. Less authoritarian regimes and even some democratic regimes exercise partial control over media in some media environments. The government does not exercise *a priori* censorship exercises but promotes self-censorship by pressuring media managers and journalists who publish items that displease the authorities.
- **Independent.** Control over media is more diffuse in media environments governed by non-authoritarian political systems that exercise only minimal control over media. Governments may regulate allocation of broadcast frequencies, morality in content, ownership in media markets, and occasionally apply political pressure against media or journalists who displease. In these environments, economic factors, norms of the journalist profession, the preferences of people who manage media, and the qualities of individual journalists who report or comment on the news all influence or control media content. Some of these other factors and elements—it depends on the particular country or issue—are of interest to our customers, but others are not.

K-3. All media are controlled. The issue for analysts is what factors and elements (elites, institutions, individuals) exercise control, how much relative power or weight does each factor or element possess, and which factors or elements are of interest to analysts and their customers. Table K-1 describes each level of control, its factors, and its elements.

Table K-1. Factors and elements of media control



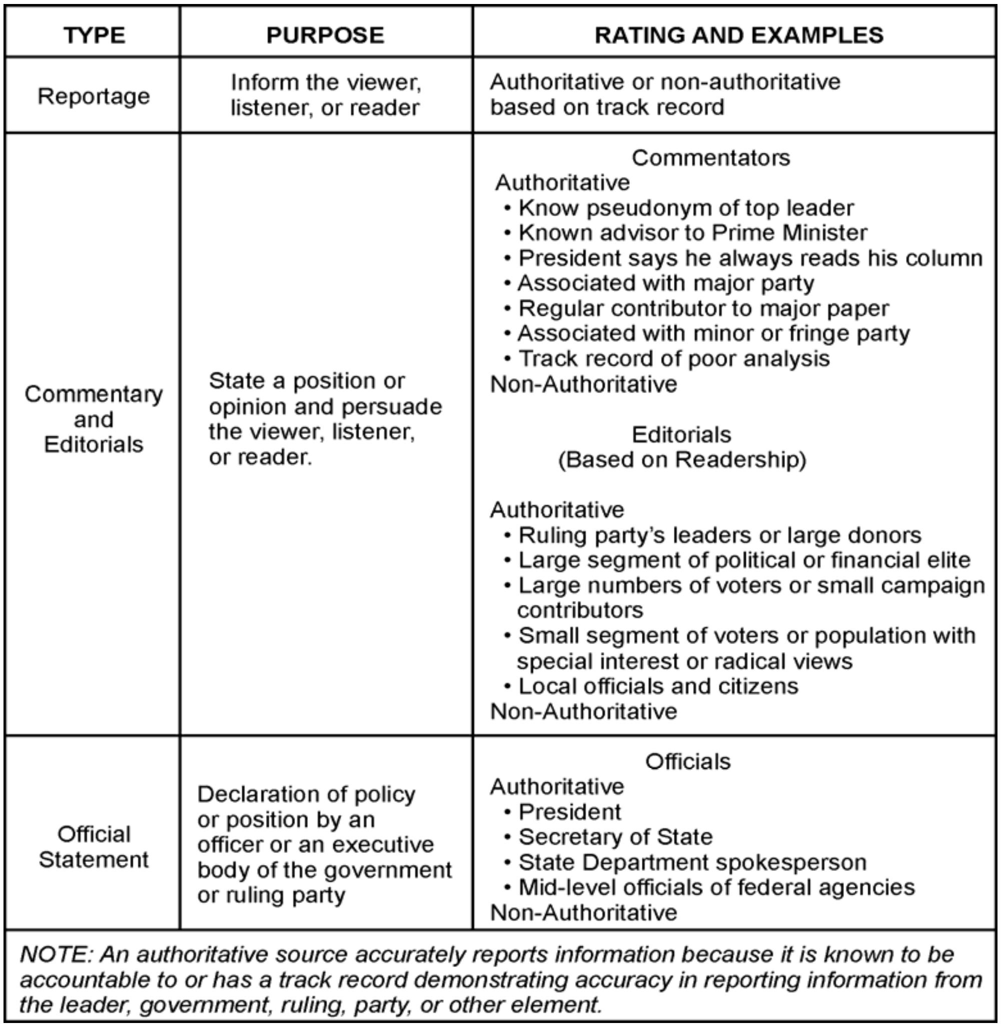
LEVEL	FACTOR	ELEMENTS (In Hierarchical Order)
Political System	Laws and norms governing operations of the media, laws and norms governing officials' relations with the media, the distribution of power among officials and institutions.	Top Leadership Consensus Top Leaders Individually Institutions (legislatures, ministries, courts)
Media Environment	Economic factors influencing operations of media (audience demand, advertising practices, and subsidies from government or business). Factor influencing the distribution of resources needed by the media (newsprint, broadcast frequencies, distance and terrain, access to distribution systems).	The elements are implicit in the factors explanation, but there is no obvious hierarchy of the elements.
Journalist Profession	The degree of freedom accorded to the media by the political system and other environmental constraints. Media personnel's perceptions of what is newsworthy and attractive to media consumers—pertinent at every level from here downward. The degree of freedom media executives accord to media managers (editors). The degree of freedom media managers accord to individual journalists. The individual journalist's view of what should go into a media item: • Which facts to include? • Which questions to ask? • Which questions not to ask? • Whose perspective to include? • Whose perspective to omit?	Boards of directors of media companies Individual directors Influential shareholders Managing editors Department editors Program producers Anchors Individuals journalists
Subject or Event *(Speech, interview, panel, discussion, riot, terrorist act, court proceeding)*	Political, professional, or societal rules or norms governing subject appearances in the media. (Do people of a given type make themselves available to the media and how do they behave when interacting with the media?) Norms governing communications or events. (Is expression or verbal or physical conflict common or acceptable in this environment? Is expression of open disagreement acceptable? Is discussion of certain subjects acceptable or unacceptable?) Legal or societal norms governing public behavior. Individual subject's perceptions of what can be said or done and what should be said or done.	Group of subject or participants Individual subject or participant

MEDIA STRUCTURE

K-4. Media structure encompasses attributes of media material other than its manifest content. Structural elements include the format or type of material, the media source, placement of the media item, intended audience, and the frequency and timing of its appearance. These elements affect the meaning and significance of the content of the item and are often as important as the content itself. Analysts use systematic analysis of these elements to uncover insights into the points of view of agents who control media, including the top political elites in media environments where control is highly centralized, and to establish the editorial slant or bias of foreign media.

- **Selection, Omission, and Slant.** Selection of news items is a fundamental editorial decision at the core of news reporting. Selection includes media managers' decisions about which stories are covered and which are not as well as reporters' and editors' decisions about which viewpoints, images, and information should be included or emphasized in a news item and which should be omitted or deemphasized. Selection decisions can contribute to an implied judgment, or slant, in a news item. The nature of decisions made about omission.

Table K-2. Hierarchy of power



TYPE	PURPOSE	RATING AND EXAMPLES
Reportage	Inform the viewer, listener, or reader	Authoritative or non-authoritative based on track record
Commentary and Editorials	State a position or opinion and persuade the viewer, listener, or reader.	Commentators Authoritative • Know pseudonym of top leader • Known advisor to Prime Minister • President says he always reads his column • Associated with major party • Regular contributor to major paper • Associated with minor or fringe party • Track record of poor analysis Non-Authoritative Editorials (Based on Readership) Authoritative • Ruling party's leaders or large donors • Large segment of political or financial elite • Large numbers of voters or small campaign contributors • Small segment of voters or population with special interest or radical views • Local officials and citizens Non-Authoritative
Official Statement	Declaration of policy or position by an officer or an executive body of the government or ruling party	Officials Authoritative • President • Secretary of State • State Department spokesperson • Mid-level officials of federal agencies Non-Authoritative

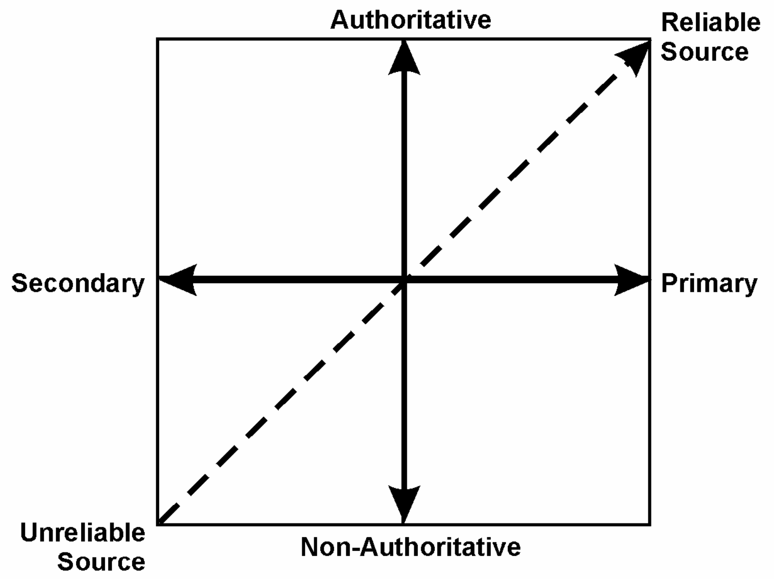
NOTE: An authoritative source accurately reports information because it is known to be accountable to or has a track record demonstrating accuracy in reporting information from the leader, government, ruling, party, or other element.

- **Hierarchy of Power.** All political systems involve hierarchy of power (Table K-2); therefore, it logically follows that official statements issued from different elements in that power hierarchy will have a corresponding hierarchy of authoritativeness. Authoritativeness can be thought of as the likelihood that the views expressed in the statement represent the dominant viewpoint within the political system. The hierarchy will be obvious in many political systems—a statement by the prime minister trumps a statement by a minister. In other cases, the hierarchy may not be so obvious and unique to the political system—a speech by the party chairman trumps a speech by the head of state.
- **Format.** Format can also mean the difference between a live news report or interview and one that is prerecorded, which gives higher level controllers more opportunity to influence the context of the item.
- **Type of Media.** Television is the medium with the largest potential audience in many media environments. It presumably has a significant impact in shaping the impressions of the general viewing public. Television has replaced radio as the population's main source of news except in media environments where poverty or distance prohibits mass access to television. Fewer people may get their information from newspapers and Internet news sites, but these people may be richer, better educated, and more influential than the general television audience. Specialized print publications and Internet sites reach a still smaller audience, but their audience will likely include officials and experts who can be expected to have influence on policy debates and outcomes. Analysts who carefully examine differences in how a media story is handled in different types of media in highly centrally controlled media environments can gain insight into a government's strategies for influencing public and elite opinion among its citizens.
- **Prominence.** Does the story appear on the front page of newspapers or on the homepage of Internet news sties; how much space is the story given; in what order does the story appear in the news broadcast; is it featured in the opening previews of the newscast; how frequently is the story rebroadcast on subsequent newscasts or bulletins; and how much air time does it get? Clustering is another concept applicable here. It involves analysis of the type and content of ideas that appear before or after or alongside the story.
- **Dissemination.** Attention to patterns of dissemination of leaders' statements is important in media environments where control is highly centralized. Leaders communicate publicly in a variety of ways, with formal policy statements, with less formal interviews, and with extemporaneous remarks. By comparing the volume of media attention given to a statement, analysts can determine whether it was intended to be taken as a pronouncement of established policy or merely as an ad hoc, uncoordinated expression, perhaps prompted by narrow contextual or temporal conditions.
- **Timing.** Analysts have traditionally paid close attention to the timing of the appearance of material in the media and that is still relevant today. The appearance of information corresponds to the news cycle. A news cycle is the process and timing by which different types of media sources obtain their material, incorporate or turn it into a product, and make it available to the public. Differences between earlier and later versions of a news item attributable to the actions of a controller can reveal latent information about the controller's views.

MEDIA SOURCE

K-5. Analysts can also learn more about media content by carefully comparing the different characteristics of different media sources (Table K-3). Source analysis is the systematic comparison and analysis of the content and behavior of different media sources over time. It is fundamental to media analysis. Systematic efforts to identify patterns in differences among media have traditionally yielded rich insights into basic policy and leadership disputes. Comparison of trends in the content of individual media with shifts in official policy has suggested that some media, at least more than others, will continue to mirror the dominant policy line. By establishing a track record for different media that suggests which are vulnerable to pressure to follow the central policy line, analysts will still have a powerful tool for identifying policy and recognizing policy shifts.

Table K-3. Types of sources



Type	Description	Factors
Primary Source	Has direct access to the information and conveys the information directly and completely.	**Access.** Did the source have direct access to the event or information? **Mediation:** Does the source provide a direct and complete view of the event or information? **Responsibility:** The more immediately, continuously, and directly a controller controls a source, the more responsible the source is to its controller and the more authoritative it is in presenting the controller's views. **Track Record:** Analysis of the source based on source's past behavior.
Secondary Source	Conveys information through various types of filters: • Uses intermediary sources. • Summarizes, paraphrases, or excerpts. • Translates from the vernacular.	
Authoritative Source	Accurately reports information because it is known to be accountable to or has a track record demonstrating accuracy in reporting information from the leader, government, ruling party, or other element.	

K-6. The concept of source analysis remains valid in media environments where control over media is less highly centralized, but has to be applied more cautiously and over a wider range of actors. In media environments where both official and nonofficial media are present, official media, at least, may be vulnerable to pressure to follow the central policy line. Analyzing less-tightly centralized controlled media, the analyst must expand the concept of source analysis to the journalist and commentator level. It is important to establish the track record of such individuals to discover if they have access to insider information from parts of the government or if they are used by officials to float policy "trial balloons." Differences in content between media outlets controlled by different official elites can reveal policy and leadership disputes. For example, a report on the president's speech by media controlled by the defense ministry may reveal differences from reports in other media or the full text of the speech published on the president's website.

MEDIA CONTENT

K-7. Analysts can enhance the value of that information through the analysis of its content, both latent and manifest. Analyzing the latent content involves determining and explaining the media context in which the information was conveyed and deciphering esoteric communication hidden in the manifest content. During media content analysis, analysts consider two forms of messages or content in the media material are manifest and latent content.

MANIFEST CONTENT

K-8. Manifest content is the actual words, images, and sounds conveyed by open sources. One of the most important forms of media analysis has involved the careful comparison of the content of authoritative official statements to identify the policies or intentions they represent. The practice of all governments and political entities and actors in general use statements and information released to the media to strengthen their support and promote their policies. The importance of words in the political process make analysis of authoritative public statements an enduring and insightful tool for discerning leadership intentions and attitudes regardless of the overall nature of control in a given media environment. Comparison of what is said and what is not said against the background of what others are saying and what has been said before is the core of open source analysis.

- **Esoteric Communications.** Analysts have also developed techniques for interpreting what are known as "esoteric communications"—public statements whose surface meaning (manifest content) does not reveal their real meaning or significance (latent content) or the author's chief purpose in making them. Esoteric communication is particularly evident in political systems with strong taboos against public contention or in cases where especially sensitive issues are at stake, but a strong case can be made that such indirect communications of one form or another are common to all political systems. Esoteric communication may be more formalized in some media environments than in others, but it is a common characteristic of all political communication, known in other contexts as "reading between the lines."
- **Multimedia Content.** Analysts analyzing multimedia can consider elements of content beyond the words used. Facial expression and voice inflection of leaders giving speeches, persons being interviewed, or the anchor reading a script often provide additional information about the views of the subject. They may, for example, provide clues as to whether a statement was seriously considered, intended to be humorous, or simply off-the-cuff. Images accompanying text are also important indicators.
- **Past Behavior.** Information conveyed by open sources must be considered against the record of the source's (media outlet, journalist, or news maker) behavior. Factors beyond immediate control such as time pressures, deadlines, or technical malfunctions, may affect the content or context of public information. Analysts' judgments about a source's behavior must be made with careful consideration of previous behavior.

LATENT CONTENT

K-9. In the latent content, analysts can derive intelligence about the views and actions of the controllers of public information over and above what might be apparent in the information's manifest content. This involves the systematic examination and comparison of content and context. The analyst can uncover patterns and rules governing the structure and content of media. These patterns and rules come from the unstated context or "frame" that provides the underlying meaning of media content and behavior. When a pattern is broken, some element changes or is omitted, or conventional language is replaced by polemics; for example, the analyst can infer that there has been a change in the context from which the communication emerged—a change in the viewpoint of the controller or a change in the balance of power among different controlling elements.

K-10. Analysts are not always able to draw conclusions from media content because there is—

- Insufficient material to do so.
- Conflicting information on the same issue from multiple sources.
- No observable trend in the material available.

K-11. In these situations, an analyst takes care not to imply that they know what is the actual position or policy of the foreign government or other entity by using formula phrases like—

- "Country A is projecting position B on issue C."
- "Country A's statement suggests hopes to achieve result B."

K-12. These phrases give readers of the report an idea of what the analyst thinks Country A wants the US reader to think. Analysts often combine conclusions like these examples with material from other sources to give readers an idea of the political context in which Country A's government is operating. This is a useful reporting technique for assessments of issues concerning countries where television and radio are government controlled and contain only selected information, but where the relatively free press provides much more detailed information that is available to the literate public.

This page intentionally left blank.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

ACE	analysis and control element
AJP	Allied Joint Publication
AKO	Army Knowledge Online
AO	area of operations
AOI	area of interest
AOIR	area of intelligence responsibility
AOR	area of responsibility
AR	Army Regulation
ARNG	Army National Guard
ASCC	Army Service Component Command
ASI	additional skill identifier
BCT	brigade combat team
BDA	battle damage assessment
C2	command and control
C3	command, control, and communications
CA	Civil Affairs
CADNET	Collaboration and Data-Sharing Network
CGS	common ground station
CI	counterintelligence
CIA	Central Intelligence Agency
COA	course of action
COCOM	combatant command
COE	contemporary operational environment
COIN	counterinsurgency
COP	common operational picture
CTID	Contemporary Operational Environment and Threat Integration Directorate
DA	Department of the Army
DA IIS	Department of Army Intelligence Information System
DAC	Department of Army Civilian
DAVE	Digital Audio Video Enterprise
DCSINT	Deputy Chief of Staff for Intelligence
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DOCEX	document exploitation
DOD	Department of Defense

DODD	Department of Defense Directive
DOIM	Director of Information Management
DOS	Department of State
DTG	date-time group
EBSCO	Elton B. Stephens Company
FBI	Federal Bureau of Investigation
FM	field manual
FMI	field manual-interim
FMSO	Foreign Military Studies Office
FOB	forward operating base
FP	force protection
FS	fire support
.ftp	file transfer protocol
G2	Assistant Chief of Staff, Intelligence
G3	Assistant Chief of Staff, Operations
G7	Assistant Chief of Staff, Information Operations
G9	Assistant Chief of Staff, Civil Affairs
GMI	general military intelligence
GWOT	globar war on terrorism
HUMINT	human intelligence
HVT	high value target
I&W	indications and warnings
IC	Intelligence Community
IED	improvised explosive device
IFV	infantry fighting vehicle
IIR	intelligence information report
IIS	Intelligence Information System
IMINT	imagery intelligence
INSCOM	US Army Intelligence and Security Command
INTELINK-SBU	Intelligence Link-sensitive but unclassified
IO	information operations
IP	Internet Protocol
IPB	intelligence preparation of the battlefield
IR	information requirement
ISM	intelligence synchronization matrix
ISP	Internet service provider
ISR	intelligence, surveillance, and reconnaissance

JAC	Joint Analysis Center
JIOC	Joint Intelligence Operations Center
JP	joint publication
JWICS	Joint Worldwide Intelligence Communications System
LAN	local area network
LEA	law enforcement agency
LEO	Law enforcement only
MACOM	major Army command
MASINT	measurement and signatures intelligence
MDCI	multidiscipline counterintelligence
MDMP	military decisionmaking process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MI	military intelligence
MOS	military occupational specialty
MSC	major subordinate command
MP	Military Police
NAI	named area of interest
NASIC	National Air and Space Intelligence Center
NCOIC	noncommissioned officer in charge
NEA	Northeast Asia
NGIC	National Ground Intelligence Center
NGO	nongovernmental organization
NIPRNET	Nonsecure Internet Protocol Router Network
OB	order of battle
OPORD	operations order
OPSEC	operations security
OSC	Open Source Center
OSINT	open source intelligence
PA	Public Affairs
PAO	public affairs officer
PIR	priority intelligence requirement
PRINCE	Processing in a Collaborative Environment
PSYOP	psychological operations
RFI	request for information
RISSNET	Regional Information Sharing System Network
S&T	science and technology
S&TI	scientific and technical intelligence
S1	personnel staff officer

S2	intelligence staff officer
S3	operations staff officer
S4	logistics staff officer
S5	plans staff officer
S6	command, control, communications and computer operations officer
S7	information operations officer
S8	financial management officer
S9	civil-military operations officer
SA	South Asia
SALUTE	size, activity, location, unit, time, and equipment
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SEA	Southwest Asia
SIGINT	signals intelligence
SIPRNET	Secure Internet Protocol Router Network
SIR	specific information requirement
SITMAP	situation map
SJA	Staff Judge Advocate
SOP	standing operating procedure
SQI	Special qualification identifier
TACREP	tactical report
TDN	TROJAN Data Network
TECHINT	technical intelligence
TLP	troop-leading procedure
TOE	table of organization and equipment
TRADOC	US Army Training and Doctrine Command
TTP	tactics, techniques, and procedures
URL	uniform resource locator
US	United States
USAPACOM	US Army Pacific Command
USEUCOM	US European Company
USMC	United States Marine Corps
UCMJ	Uniform Code of Military Justice
WAN	wide area network
WARNO	warning order
WBIL	World Basic Information Library
WEG	Worldwide Equipment Guide

WFF	warfighting function
WMD	weapon of mass destruction
XO	executive officer

SECTION II – TERMS

Acquisition (Collection)

Obtaining of information in any manner, including direct observation, liaison with official agencies, or solicitation from official, unofficial, or public sources. (JP 1-02)

All-Source Intelligence

Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. (JP 1-02)

Analysis

Determination of the significance of the information, relative to information and intelligence already known, and drawing deductions about the probable meaning of the evaluated information. (FM 2-0)

Assessment

The continuous monitoring and evaluation of the current situation and progress of an operation. (FMI 5-0.1)

***Authoritative Source**

A source that reports information accurately because it is known to be accountable to or has a track record demonstrating accuracy in reporting information from the leader, government, ruling party, or other element.

Chatham House Rule

According to the Chatham House, "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

Civil Authorities

Those elected and appointed officers and employees who constitute the government of the United States, of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, United States possessions and territories, and political subdivisions thereof. (JP 3-26)

Civil Considerations

The influence of manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within an AO on the conduct of military operations. (FM 6-0)

Civil Support

DOD support to US civil authorities for domestic emergencies, and for designated law enforcement and other activities. (JP 3-26)

Clandestine Operation

An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities. See also covert operation; overt operation. (JP 1-02)

Classified Information

Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated. (JP 1-02)

Collect

An activity of information management: the continuous acquisition of relevant information by any means, including direct observation, other organic resources, or other official, unofficial, or public sources from the information environment. (FM 1-02)

Collection

In intelligence usage, the acquisition of information and the provision of this information to processing elements. (JP 1-02)

Collection Agency

Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. (JP 1-02)

Collection Asset

A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (JP 1-02)

Collection Management

In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (JP 1-02)

Collection Plan

A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (JP 1-02)

Collection Resource

A collection system, platform, or capability that is not assigned or attached to a specific unit or echelon which must be requested and coordinated through the chain of command. (JP 1-02)

Command and Control

The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of a mission. Commanders exercise command and control through a command and control system. (FM 6-0)

Commander’s Intent

A clear, concise statement of what the force must do and the conditions the force must meet to succeed with respect to the enemy, terrain, and civil considerations that represent the operation’s desired end state. (FMI 5-0.1)

Communications Intelligence

Technical information and intelligence derived from foreign communications by other than the intended recipients. (JP 1-02)

Confidential Source

Any person, group, or system that provides information with the expectation that the information, relationship, or both, are protected against public disclosure. (AR 380-5)

Control

The regulation of forces and warfighting functions to accomplish the mission in accordance with the commander's intent. (FMI 5-0.1)

Controlled Unclassified Information

Information that requires application of controls and protective measures not to include those that qualify for formal classification. (AR 380-5)

Covert Operation

An operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. A covert operation differs from a clandestine operation in that emphasis is placed on concealment of identity of sponsor rather than on concealment of the operation. (JP 1-02)

Dissemination (and Integration)

In intelligence usage, the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. (JP 1-02)

Document

Any recorded information regardless of its physical form or characteristics including, but not limited to, all written material, whether handwritten, printed or typed; painted, drawn or engraved material; sound or voice recordings; imagery; punched cards, punched paper tape, printed output and associated material to include computer storage media such as floppy, compact and hard disks and magnetic tape; and reproductions of the foregoing, by whatever process. Engraved material such as manufacturers' plates and the like, permanently fastened to captured equipment is not considered a document. (AJP-2.5)

Doctrine

Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. (JP 1-02)

Essential Task

A specified or implied task that must be executed to accomplish the mission. Essential tasks are always included in the unit's mission statement. (FM 5-0)

Evaluate

In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. (FM 2-0)

Execute

To put a plan into action by applying combat power to accomplish the mission and using situational understanding to assess progress and make execution and adjustment decisions. (FM 6-0)

Foreign Intelligence

Information relating to the capabilities, intentions, and activities of foreign powers, organizations, and persons, but not including counterintelligence except for information on international terrorist activities. (JP 1-02)

Homeland Defense

The protection of US sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President. (JP 3-26)

Homeland Security

A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (JP 3-26)

Information

Facts, data, or instructions in any medium or form. (JP 1-02)

Infrastructure

In intelligence usage, the basic underlying framework or feature of a thing; in economics, basic resources, communications, industries, and so forth, upon which others depend; in insurgency, the organization (usually hidden) of insurgent leadership. (FM 2-0)

Intelligence

The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. (JP 1-02)

Intelligence Discipline

A well-defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. (JP 1-02)

Intelligence Process

The process by which information is converted into intelligence and made available to users. (JP 1-02)

Intelligence Report

A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. (JP 1-02)

Intelligence Requirements

1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (JP 1-02) 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the battlespace or threat forces. (JP 1-02)

Intelligence Source

The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. An intelligence source can be people, documents, equipment, or technical sensors. (JP 1-02)

Intelligence Warfighting Function

The related tasks and systems that facilitate understanding of the enemy, terrain, weather, and civil considerations. (FMI 5-0.1)

***Internet**

Publicly accessible communications network that connects computers, computer networks, and organizational computer facilities around the world.

Investigative Information

All data developed as a result of counterintelligence investigative activities, such as investigations, operations, and services, and through liaison with local, State, and Federal agencies. It may also come from unsolicited sources, and from public sources, such as newspapers, magazines, books, periodicals, handbills, and radio and television broadcasts. (Source: AR 380-13)

Metadata

Information about information; more specifically, information about the meaning of other data. (JP 1-02)

Military Intelligence

Intelligence on any foreign military or military-related situation or activity which is significant to military policymaking or the planning and conduct of military operations and activities. (JP 1-02)

***Open Source**

Any person or group that provides information without the expectation of privacy—the information, the relationship, or both are protected not against public disclosure.

Open Source Intelligence

1. Information of potential intelligence value that is available to the general public. (JP 1-02) 2. Relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to intelligence requirement (Army).

Operational Environment

A composite of the conditions, circumstances, and influences that affect the employment of military forces and bear on the decisions of the unit commander. (JP 1-02)

Operations Process

The major command and control activities performed during operations: planning, preparation, execution, and continuous assessment. These activities occur continuously throughout an operation, overlapping and recurring as required. (FMI 5-0.1)

Operations Security

A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

Overt Operation

An operation conducted openly, without concealment. See also clandestine operation; covert operation. (JP 1-02)

Planning

The process by which commanders (and staff if available) translate the commander’s visualization into a specific course of action for preparation and execution, focusing on the expected results. (FMI 5-0.1)

Preparation

Activities by the unit before execution to improve its ability to conduct the operation including, but not limited to, the following: plan refinement, rehearsals, reconnaissance, coordination, inspections, and movement. (FM 3-0)

***Primary Source**

A source that has direct access to the information and conveys the information directly and completely.

***Private Information**

Data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization.

Priority Intelligence Requirements

Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision making. (JP 1-02)

Procedures

Standard, detailed steps that prescribe how to perform specific tasks. (JP 1-02)

Process (Processing)

A function of the intelligence process that involves converting collected data, which is not already in a comprehensible form when it is reported, into a form that is understandable and suitable for analysis and production of intelligence. (FM 2-0)

Production

The integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence. (JP 1-02)

Propaganda

Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. (JP 1-02)

Public Affairs Assessment

An analysis of the news media and public environments to evaluate the degree of understanding about strategic and operations objectives and military activities and to identify levels of public support. Includes judgments about the public affairs impact of pending decisions and recommendations about the structure of public affairs support for the assigned mission. (FM 3-61.1)

***Publicly Available Information**

Data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

***Public Broadcasts**

Simultaneous transmission of data or information for general public consumption to all receivers or terminals within a computer, radio, or television network.

Public Information

A general term describing processes used to provide information to external audiences through public media. (FM 3-61.1)

***Public Speaking**

Distribution of information to audiences during events that are open to the public or occur in public areas.

Regional Information Sharing System Network (RISSNET)

The Regional Information Sharing Systems (RISS) Program is a federally funded program consisting of six regional projects dedicated to the support of local, state and federal law enforcement and criminal justice agencies.

Reconnaissance

A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (JP 1-02)

***Secondary Source**

A source that conveys information through various types of filters; uses intermediary sources; summarizes, paraphrases, or excerpts information; or translates from the vernacular.

Signals Intelligence

A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. (JP 1-02)

Source

A person, thing, or activity from which information is obtained. (JP 1-02)

Surveillance

The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (JP 1-02)

Tactics

The employment and ordered arrangement of forces in relation to each other. (JP 1-02)

Target

In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. (JP 1-02)

Target Analysis

An examination of potential targets to determine military importance, priority of attack, and weapons required to obtain a desired level of damage or casualties. (JP 1-02)

Target Folder

A folder, hardcopy or electronic, containing target intelligence and related materials prepared for planning and executing action against a specific target. (JP 1-02)

Target System

All the targets situated in a particular geographic area and functionally related. (JP 1-02)

Target System Component

A set of targets belonging to one or more groups of industries and basic utilities required to produce component parts of an end product such as periscopes, or one type of a series of interrelated commodities, such as aviation gasoline. (JP 1-02)

Techniques

Nonprescriptive ways or methods used to perform missions, functions, or tasks. (JP 1-02)

***Transcription**

The process of creating a verbatim written record of spoken information.

***Translation**

1. The process of transferring written information from one language into another. 2. A written document in a second language having the same meaning as the written document in a first language.

***Unclassified Information**

Information that does not require protection in the interest of national security.

Warfighting Function

A group of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions and training objectives. (FMI 5-0.1)

This page intentionally left blank.

References

SOURCES USED

These are the sources quoted or paraphrased in this publication.

US Marine Corps. *Operation IRAQI FREEDOM: Lessons Learned*. 26 July 2003. Retrieved from Center for Army Lessons Learned at http://call.army.mil.

White, Louise G. *Political Analysis: Technique and Practice. 4th edition*. Belmont, California: Wadsworth, 1999.

Winder, Robyn. *Untangling The Web: An Introduction to Internet Research. 2005*. Available online at http://www.interlink.gov.

World Bank. **World Development Indicators 2005**. Available online at http://www.worldbank.org/data/wdi2005/

101st Airborne Division. *Lessons Learned Report (Part 1). Division and Brigade Intelligence, Surveillance, and Reconnaissance Operations*. 30 May 2003. Retrieved from Center for Army Lessons Learned at http://call.army.mil.

173d Airborne Brigade. *Lessons Learned Briefing*. 24 January 2004. Retrieved from Center for Army Lessons Learned at http://call.army.mil.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*. Available online from the Army Publishing Directorate at http://www.army.mil/usapa.

DD Form 2745. *Enemy Prisoner of War (EPW) Capture Tag*. 1 May 1996. Available online from the Army Publishing Directorate at http://www.army.mil/usapa.

“Untangling The Web: An Introduction to Internet Research DOD Pamphlet.”

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication.

AR 27-60. *Intellectual Property,* 1 June 1993.

AR 380-13. *Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations*. 13 September 1974.

AR 381-10. *US Intelligence Activities*. 22 November 2005. Available online from Army Publishing Directorate at http://www.army.mil/usapa/epubs/index.html.

FM 2-0. *Intelligence*. 17 May 2004. Available online from Army Publishing Directorate at http://www.army.mil/usapa/doctrine/index.html

FM 3-0. *Operations*. 14 June 2001. Available online from Army Publishing Directorate at http://www.army.mil/usapa/doctrine/index.html

READINGS RECOMMENDED

These sources contain relevant supplemental information.

ARMY PUBLICATIONS

AR 25-400-2. *The Army Records Information Management System (ARIMS).* 15 November 2004.

AR 27-60. *Intellectual Property*. 1 June 1993. Available online from Army Publishing Directorate at http://www.army.mil/usapa/epubs/index.html.

AR 115-11. *Geospatial Information and Services*. 10 December 2001. Available online from Army Publishing Directorate at http://www.army.mil/usapa/epubs/index.html.

AR 340-21. *The Army Privacy Program*. 5 July 1985.

AR 380-5. *Department of the Army Information Security Program*. 9 September 2000. Available online from Army Publishing Directorate at http://www.army.mil/usapa/epubs/index.html.

AR 381-11. *Productions Requirements and Threat Intelligence Support to the US Army*. 28 June 2000. Available online from Army Publishing Directorate at http://www.army.mil/usapa/epubs/index.html.

FM 3-61.1. *Public Affairs Tactics, Techniques, and Procedures*. 1 October 2000. Available online from Army Publishing Directorate at http://www.army.mil/usapa/doctrine/index.html

FM 5-0. *Army Planning and Orders Production*. 20 January 2005. Available online from Army Publishing Directorate at http://www.army.mil/usapa/doctrine/index.html

FM 5-0.1. *The Operations Process*. 31 March 2006. Available online from Army Publishing Directorate at http://www.army.mil/usapa/doctrine/index.html

FM 7-100. *Opposing Force Doctrinal Framework and Strategy*. 1 May 2003.

FM 34-3. *Intelligence Analysis*. 15 March 1990.

FM 34-130. *Intelligence Preparation of the Battlefield*. 8 July 1994.

FM 34-3-61.1. *Public Affairs Tactics, Techniques, and Procedures*. 1 October 2000. Available online from Army Publishing Directorate at http://www.army.mil/usapa/doctrine/index.html

JOINT PUBLICATIONS

JP 1-02. *DOD Dictionary of Military and Associated Terms*. 31 August 2005. Available online from the Joint Staff, J7, Joint Doctrine Division Support Group’s Joint Electronic Library at http://www.dtic.mil/doctrine.

JP 2-0. *Doctrine for Intelligence Support to Joint Operations*. 9 March 2000.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 7 October 2004. Available online from the Joint Staff, J7, Joint Doctrine Division Support Group’s Joint Electronic Library at http://www.dtic.mil/doctrine.

JP 3-26. *Homeland Security*. 2 August 2005. Available online from the Joint Staff, J7, Joint Doctrine Division Support Group’s Joint Electronic Library at http://www.dtic.mil/doctrine.

JP 3-54. *Joint Doctrine for Operations Security*. 24 January 1997. Available online from the Joint Staff, J7, Joint Doctrine Division Support Group’s Joint Electronic Library at http://www.dtic.mil/doctrine

PUBLIC LAWS AND OTHER PUBLICATIONS

US Public Law 109-163. *The National Defense Authorization Act for Fiscal Year 2006*. 6 January 2006.

US Public Law 108-458. *Intelligence Reform and Terrorism Prevention Act of 2004*. 17 December 2004. Available online from the National Counterterrorism Center at http://www.nctc.gov/docs/pl108_458.pdf.

US Public Law 109-163. *National Defense Authorization Act for Fiscal Year 2006*. 6 December 2005. Available online from the US Congress at http://www.nctc.gov/docs.

Aaron, Jane E. *The Little Brown Compact Handbook. 4th edition*. Boston: Addison Wesley Educational Publishers, Inc., 2001.

CALL Initial Impressions Report. *Stability Operations and Support Operations, Operation IRAQI FREEDOM*. January 2004. Retrieved from Center for Army Lessons Learned at http://call.army.mil.

CALL Initial Impressions Report. *Operation Enduring Freedom*. December 2003. Retrieved from Center for Army Lessons Learned at http://call.army.mil.

CALL Initial Impressions Report Number 04-28. *Combined/Joint Task Force Horn of Africa*. October 2004

CALL Newsletter Number 99-2. *Task Force Eagle Information Operations Tactics, Techniques, and Procedures*. January 1999. Retrieved from Center for Army Lessons Learned at http://call.army.mil.

CALL Newsletter Number 03-23. *Targeting For Victory: Winning the Civil Military Operations*. September 2003. Retrieved from Center for Army Lessons Learned at http://call.army.mil.

Chairman of the Joint Chiefs of Staff Instruction 3126.01. *Language and Regional Expertise Planning*. 23 January 2006. Available online from the Chairman of the Joint Chiefs of Staff Directives Electronic Library at http://www.dtic.mil/cjcs_directives/index.htm

Chatham House. *The Chatham House Rule*. Accessed 18 April 2006. Retrieved from Chatham House at http://www.riia.org.

Circular 1. *Copyright Basics*. September 2000. Available online from the United States Copyright Office at http://www.copyright.gov.

Circular 92. *Copyright Law of the United States of America and Related Laws Contained in Tıtle 17 of the United States Code*. June 2003. Available online from the United States Copyright Office at http://www.copyright.gov.

Code of Federal Regulations. *Title 6 - Homeland Security*. 1 January 2005. Available online from Government Printing Office Access online database at http://www.gpoaccess.gov/cfr/index.html.

Code of Federal Regulations. *Title 32 – National Defense*. 1 July 2004. Available online from Government Printing Office Access online database at http://www.gpoaccess.gov/cfr/index.html.

Code of Laws of the US of America. *Title 10 – Armed Forces*. 8 January 2004. Available online from Government Printing Office Access online database at http://www.gpoaccess.gov/uscode/index.html.

Code of Laws of the US of America. *Title 32 – National Guard*. 8 May 2002. Available online from Government Printing Office Access online database at http://www.gpoaccess.gov/uscode/index.html.

Department of the Army. *Army Open Source Information Plan*. 31 May 1995. Washington, DC: Office of the Deputy Chief of Staff For Intelligence.

Department of Defense. *Open Source Information System User Security Guide*. 27 September 2004. Available online at http://www.Interlink.gov.

DOD Directive 5100.1. *Functions of the Department of Defense and its Components*. 1 August 2002. Available online from the Defense Technical Information Center's Directives and Records Division at http://www.dtic.mil/whs/directives.

DOD Directive 5100.20. *The National Security Agency and the Central Security Service* (with Change 4), 24 June 1991. Available online from the Defense Technical Information Center's Directives and Records Division at http://www.dtic.mil/whs/directives.

DOD Directive 5200.27. *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense.* 7 January 1980. Available online from the Defense Technical Information Center's Directives and Records Division at http://www.dtic.mil/whs/directives.

DOD Directive 5200.41. *DOD Centers for Regional Security Studies.* 30 July 2004. Available online from the Defense Technical Information Center's Directives and Records Division at http://www.dtic.mil/whs/directives.

DOD Directive 5240.1. *DOD Intelligence Activities.* 25 April 1998 and DODD 5240.1-R (Procedure 2). Available online from the Defense Technical Information Center's Directives and Records Division at http://www.dtic.mil/whs/directives.

Executive Order 12333. *United States Intelligence Activities*. Available online from Assistant to the Secretary of Defense for Intelligence Oversight at http://www.dod.mil/atsdio/.

Herrington, Vee, Ph.D. *Open Source Information and the Military Intelligence Library*. Military Intelligence Professional Bulletin, Volume 31, Issue 2. October-December 2005.

Jeffson, Joel J. *Creating an Open Source Intelligence Capability. Military Intelligence Professional Bulletin*, Volume 31, Issue 2. October-December 2005.

Les Grau, *National Perceptions and Warfighting: How Potential Foes and Other Nations View United States Strengths and Weaknesses.* (Accessed 15 December 2005). Available online from the Foreign Military Studies Office at http://www.fmso.osis.gov/products.htm.

Ives, John M., CPT. *Brigade Intelligence Team: Fused and Focused*. 2003. The Vanguard, Volume 11, Number 1, Winter 2006. Available online from the Military Intelligence Corps Association website at www.micorps.org.

Madill, Donald L., PhD. *Producing Intelligence From Open Sources*. Military Intelligence Professional Bulletin, Volume 31, Issue 2. October-December 2005.

National Security Decision Directive 298. *National Operations Security Program*, 15 July 2003. Available online from the Interagency Operations Security Support Staff at http://www.ioss.gov/nsdd298.html.

North Atlantic Treaty Organization. *NATO Open Source Intelligence Handbook*. November 2001.

Peavie, Barrett K., MAJ. *Information Sharing in Bosnia*. School of Advanced Military Studies, U.S. Army Command and General Staff College, Fort Leavenworth, Kansas.

RAND Arroyo Center. *Street Smarts: Intelligence Preparation of the Battlefield for Urban Operations*. 2002

Reese, David A. *50 Years of Excellence: ASD Forges Ahead as the Army's Premier OSINT Unit in the Pacific*. Military Intelligence Professional Bulletin, Volume 31, Issue 2. October-December 2005.

Taylor, Michael C. *Open Source Intelligence Doctrine*. Military Intelligence Professional Bulletin, Volume 31, Issue 2. October-December 2005.

Tulak, Arthur N., MAJ. (1999) *The Application of Information Operations Doctrine in Support of Peace Operations*. U.S. Army Command and General Staff College, Fort Leavenworth, Kansas.

US Army Intelligence and Security Command. *INSCOM Open Source Intelligence Operations Handbook*. May 2003. Fort Belvoir, VA: Office of the Assistant Chief of Staff, G3.

US Army Office of Information Assurance and Compliance. Information Assurance Better Business Practice 05-EC-M-0006. *Open Source Information System Services*, Version 1.0. 23 November 2005. Available online from the Army Information Assurance Directorate at https://informationassurance.us.army.mil/bbp.

US Army Special Operations Command. *Civil-Military Operations (4th Infantry Division).* Undated presentation received 9 February 2006.

TRADOC Regulation 25-36. *The TRADOC Doctrinal Literature Program*. 1 October 2004.

US Code. *Title 50 – War and National Defense*. 17 March 2005. Available online from Government Printing Office Access online database at http://www.gpoaccess.gov/uscode/index.html.

National Security Act of 1947. July 1947, as amended on 10 August 1949.

Patriot Act of 2001. October 2001.

Intelligence Reform and Prevention of Terrorism Act of 2004. 7 December 2004.

US Copyright Office Circular 38a. “International Copyright Relations of the United States at US Copyright office website at http://www.copyright.gov.

1976 Copyright Act as amended *(Title 17 of the United States Code).* 1 January 1978.

This page intentionally left blank.

Index

Entries are by paragraph numbers.

This page intentionally left blank.

FMI 2-22.9
5 December 2006
Expires 5 December 2008

By order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

Joyce E. Morrow

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
0631801

DISTRIBUTION:

Regular Army, Army National Guard, and Army Reserve: Not to be distributed. Electronic media only.