ATP 2-22.9

Open-Source Intelligence

July 2012

DISTRIBUTION RESTRICTION: Unlimited Distribution

Headquarters, Department of the Army

***ATP 2-22.9**

Army Techniques Publication
No. 2-22.9 (FMI 2-22.9)

Headquarters
Department of the Army
Washington, DC, 10 July 2012

Open-Source Intelligence

Contents

DISTRIBUTION RESTRICTION: Unlimited Distribution

.

*This publication supersedes FMI 2-22.9, 5 December 2006.

Figures

Tables

Preface

ATP 2-22.9 establishes a common understanding, foundational concepts, and methods of use for Army open-source intelligence (OSINT). ATP 2-22.9 highlights the characterization of OSINT as an intelligence discipline, its interrelationship with other intelligence disciplines, and its applicability to unified land operations.

This Army techniques publication—

- Provides fundamental principles and terminology for Army units that conduct OSINT exploitation.
- Discusses tactics, techniques, and procedures (TTP) for Army units that conduct OSINT exploitation.
- Provides a catalyst for renewing and emphasizing Army awareness of the value of publicly available information and open sources.
- Establishes a common understanding of OSINT.
- Develops systematic approaches to plan, prepare, collect, and produce intelligence from publicly available information from open sources.

The target audience for this Army techniques publication is Army units at the division level and below conducting OSINT exploitation.

Defined terms are identified in the text. Definitions for which this publication is the proponent are printed in boldface. 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 publication follows the definition. Terms for which this publication is the proponent are indicated with an asterisk in the glossary.

"OSINT personnel" applies to intelligence and nonintelligence Active Army, Army National Guard/Army National Guard of the United States, and U.S. Army Reserve personnel who engage in missions involving publicly available information and open sources.

AR 381-10 defines a *U.S. person* as—

- A U.S. citizen.
- A U.S. permanent resident alien.
- An unincorporated association substantially composed of U.S. citizens or permanent resident aliens.
- A corporation or subsidiary incorporated in the United States that is not directed or controlled by a foreign government.

The following are presumed to be *non-U.S. persons*:

- A person or organization outside of the United States.
- A person not a citizen or permanent resident alien of the United States.

The use or mention of the name of any commercial or private organization or its associated trademark or services by the Army does not express or imply an endorsement of the sponsor or its products and services by the Army.

This publication applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve unless otherwise stated.

Headquarters, U.S. Army Training and Doctrine Command, is the proponent for this publication. The preparing agency is the U.S. Army Intelligence Center of Excellence (USAICoE), Fort Huachuca, AZ. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to: Commander, USAICoE, ATTN: ATZS-CDI-D (ATP 2-22.9), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017.

Introduction

Since before the advent of the satellite and other advanced technological means of gathering information, military professionals have planned, prepared, collected, and produced intelligence from publicly available information and open sources to gain knowledge and understanding of foreign lands, peoples, potential threats, and armies.

Open sources possess much of the information needed to understand the physical and human factors of the operational environment of unified land operations. Physical and human factors of a given operational environment can be addressed utilizing publicly available information to satisfy information and intelligence requirements and provide increased situational awareness interrelated with the application of technical or classified resources.

The world is being reinvented by open sources. Publicly available information can be used by a variety of individuals to expand a broad spectrum of objectives. The significance and relevance of open-source intelligence (OSINT) serve as an economy of force, provide an additional leverage capability, and cue technical or classified assets to refine and validate both information and intelligence.

As an intelligence discipline, OSINT is judged by its contribution to the intelligence warfighting function in support of other warfighting functions and unified land operations.

Chapter 1

Open-Source Intelligence (OSINT) Fundamentals

Pioneer and reformative directives led to the passing of legislation that affected the U.S. intelligence community and its application of publicly available information. The National Security Act of 1992 began the reformation of the U.S. intelligence community resulting in the establishment of the Open Source Office and subsequently the Director of National Intelligence (DNI) Open Source Center (OSC) in 2005. This chapter describes the fundamentals of open-source intelligence (OSINT).

DEFINITION AND TERMS

1-1. *Open-source intelligence* is the intelligence discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement (FM 2-0). OSINT also applies to the intelligence produced by that discipline.

1-2. OSINT is also intelligence developed from the overt collection and analysis of publicly available and open-source information not under the direct control of the U.S. Government. OSINT is derived from the systematic collection, processing, and analysis of publicly available, relevant information in response to intelligence requirements. Two important related terms are open source and publicly available information:

- **Open source** 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. Open-source information can be publicly available but not all publicly available information is open source. Open sources refer to publicly available information medium and are not limited to physical persons.
- **Publicly available information** 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.

Note. All OSINT operations conducted by intelligence personnel must comply with the legal restrictions as outlined in Executive Order (EO) 12333, DOD 5240.1-R, DODD 3115.12, JP 2-0, and AR 381-10.

1-3. OSINT collection is normally accomplished through monitoring, data-mining, and research. Open-source production supports all-source intelligence and the continuing activities of the intelligence process (generate intelligence knowledge, analyze, assess, and disseminate), as prescribed in FM 2-0. Like other intelligence disciplines, OSINT is developed based on the commander’s intelligence requirements.

CHARACTERISTICS

1-4. The following characteristics address the role of OSINT in unified land operations:

- **Provides the foundation.** Open-source information provides the majority of the necessary background information on any area of operations (AO). This foundation is obtained through open-source media components that provide worldview awareness of international events and perceptions of non-U.S. societies. This foundation is an essential part of the continuing activity of *generate intelligence knowledge*.

- **Answers requirements.** The availability, depth, and range of publicly available information enables organizations to satisfy intelligence and information requirements without the use or support of specialized human or technical means of collection.
- **Enhances collection.** Open-source research supports surveillance and reconnaissance activities by answering intelligence and information requirements. It also provides information (such as biographies, cultural information, geospatial information, and technical data) that enhances and uses more technical means of collection.
- **Enhances production.** As part of a multidiscipline intelligence effort, the use and integration of publicly available information and open sources ensure commanders have the benefit of all sources of available information to make informative decisions.

THE INTELLIGENCE WARFIGHTING FUNCTION

1-5. The intelligence warfighting function is composed of four distinct Army tactical tasks (ARTs):

- Intelligence support to force generation (ART 2.1).
- Support to situational understanding (ART 2.2).
- Perform intelligence, surveillance, and reconnaissance (ART 2.3).
- Support to targeting and information superiority (ART 2.4).

1-6. The *intelligence warfighting function* is the related tasks and systems that facilitate understanding of the operational environment, enemy, terrain, weather, and civil considerations (FM 1-02). As a continuous process, the intelligence warfighting function involves analyzing information from all sources and conducting operations to develop the situation. OSINT supports each of these ARTs.

1-7. Publicly available information is used to—

- Support situational understanding of the threat and operational environment.
- Obtain information about threat characteristics, terrain, weather, and civil considerations.
- Generate intelligence knowledge before receipt of mission to provide relevant knowledge of the operational environment.
- Rapidly provide succinct answers to satisfy the commander’s intelligence requirements during intelligence overwatch.
- Develop a baseline of knowledge and understanding concerning potential threat actions or intentions within specific operational environments in support of the commander’s ongoing intelligence requirements.
- Generate intelligence knowledge as the basis for Army integrating functions such as intelligence preparation of the battlefield (IPB). IPB is designed to support the staff estimate and the military decisionmaking process (MDMP). Most intelligence requirements are generated as a result of the IPB process and its interrelation with MDMP.
- Support situation development—a process for analyzing information and producing current intelligence concerning portions of the mission variables of enemy, terrain and weather, and civil considerations within the AO before and during operations (see FM 2-0). Situation development—
  - Assists the G-2/S-2 in determining threat intentions and objectives.
  - Confirms or denies courses of action (COAs).
  - Provides an estimate of threat combat effectiveness.
- Support information collection. Planning requirements and assessing collection analyzes information requirements and intelligence gaps and assists in determining which asset or combination of assets are to be used to satisfy the requirements.

1-8. For more detailed information on the intelligence warfighting function, see FM 2-0. For examples of how OSINT is used to support other intelligence disciplines and operational tasks, see appendix D.

THE INTELLIGENCE PROCESS

1-9. The intelligence process consists of four steps (plan, prepare, collect, and produce) and four continuing activities (analyze, generate intelligence knowledge, assess, and disseminate). Just as the activities of the operations process (plan, prepare, execute, and assess) overlap and recur as the mission demands, so do the steps of the intelligence process. The continuing activities occur continuously throughout the intelligence process and are guided by the commander's input.

1-10. The four continuing activities plus the commander's input drive, shape, and develop the intelligence process. The intelligence process provides a common model for intelligence professionals to use to guide their thoughts, discussions, plans, and assessments. The intelligence process results in knowledge and products about the threat, terrain and weather, and civil considerations.

1-11. OSINT enhances and supports the intelligence process and enables the operations process, as described in FM 2-0. The intelligence process enables the systematic execution of Army OSINT exploitation, as well as the integration with various organizations (such as joint, interagency, intergovernmental, and multinational). Figure 1-1 illustrates the intelligence process. (For more information on the intelligence process, see FM 2-0.)

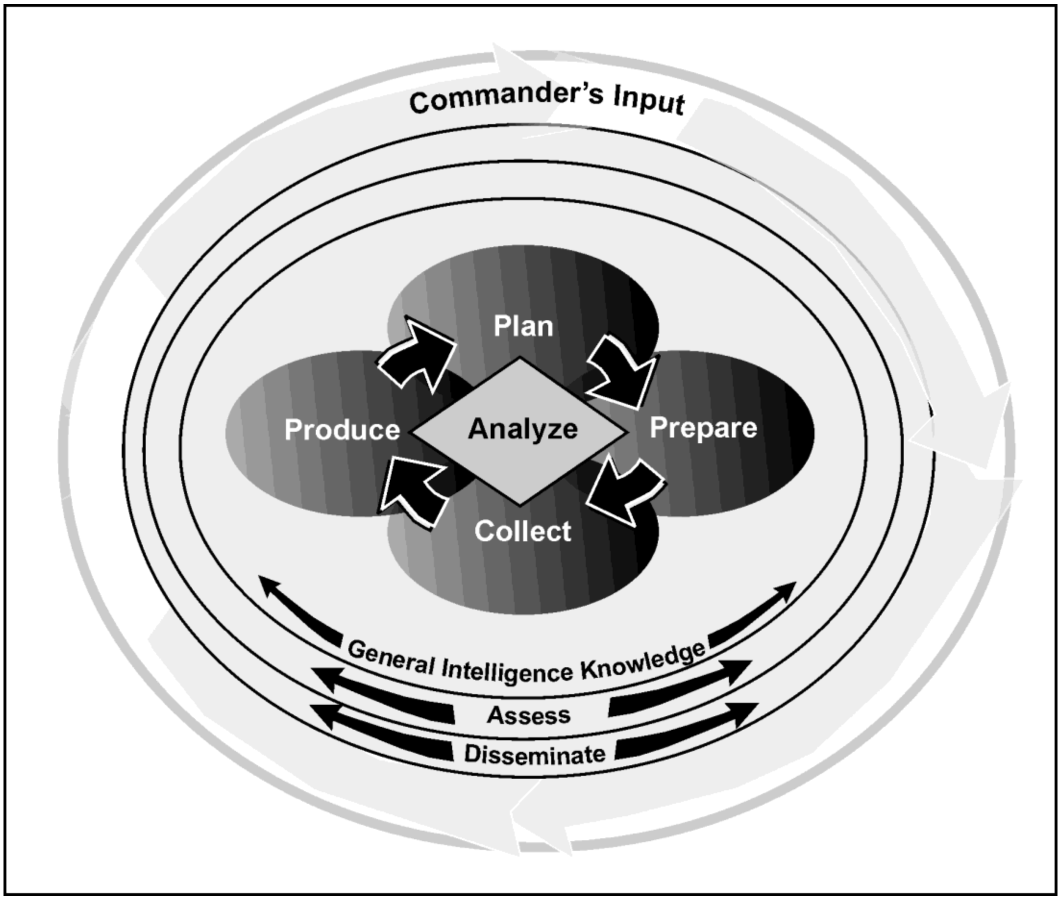

Figure 1-1. The intelligence process

THE PLANNING REQUIREMENTS AND ASSESSING COLLECTION PROCESS

1-12. Information collection informs decisionmaking for the commander and enables the application of combat power and assessment of its effects. *Information collection* is an activity that synchronizes and integrates the planning and operation of sensors, assets, as well as the processing, exploitation, and dissemination of systems in direct support of current and future operations (FM 3-55). This is an integrated intelligence and operations function. For Army forces, this activity is a combined arms operation that focuses on priority intelligence requirements (PIRs) while answering the commander's critical information requirements (CCIRs).

1-13. Information collected from multiple sources and analyzed becomes intelligence that provides answers to commanders' information requirements concerning the enemy and other adversaries, climate, weather, terrain, and population. Developing these requirements is the function of information collection:

- A *commander's critical information requirement* is an information requirement identified by the commander as being critical to facilitating timely decisionmaking. The two key elements are friendly force information requirements and priority intelligence requirements (JP 3-0).
- A *priority intelligence requirement* is an intelligence requirement, stated as a priority for intelligence support, which the commander and staff need to understand the adversary or the operational environment (JP 2-0).
- A *friendly force information requirement* is information the commander and staff need to understand the status of friendly force and supporting capabilities (JP 3-0).

1-14. The *planning requirements and assessing collection* process involves six continuous, nondiscrete activities. These activities and subordinate steps are not necessarily sequential and often overlap. The planning requirements and assessing collection process supports the staff planning and operations processes throughout unified land operations.

THE MILITARY DECISIONMAKING PROCESS

1-15. Upon receipt of the mission, commanders and staffs begin the MDMP. The *military decisionmaking process* is an iterative planning methodology that integrates the activities of the commander, staff, subordinate headquarters, and other partners to understand the situation and mission; develop and compare courses of action; decide on a course of action that best accomplishes the mission; and produce an operation plan or order for execution (FM 5-0).

1-16. During the second step of the of the MDMP, mission analysis, commanders and staffs analyze the relationships among the mission variables—mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC)—seeking to gain a greater understanding of the—

- Operational environment, including enemies and civil considerations.
- Desired end state of the higher headquarters.
- Mission and how it is nested with those of the higher headquarters.
- Forces and resources available to accomplish the mission and associated tasks.

1-17. Within the MDMP, OSINT assists in enabling the planning staff to update estimates and initial assessments by using publicly available information and open sources. Major intelligence contributions to mission analysis occur because of IPB. (For more information on the MDMP, see FM 5-0.)

> ***Note.*** Nonintelligence staff can also research publicly available information to prepare functional area-specific estimates, papers, briefings, plans, and orders in support of the MDMP.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

1-18. *Intelligence preparation of the battlefield* is a systematic process of analyzing and visualizing the portions of the mission variables of threat, terrain, weather, and civil considerations in a specific area of interest and for a specific mission. By applying intelligence preparation of the battlefield, commanders gain the information necessary to selectively apply and maximize operational effectiveness at critical points in time and space (FM 2-01.3).

1-19. IPB was originally designed to support the MDMP and troop leading procedures, but it can also be incorporated into other problem-solving models like design and red teaming. OSINT plays a significant and integral part during IPB in satisfying intelligence and information requirements indicated during the MDMP in support of unified land operations. The indicators that can be satisfied using OSINT during IPB include but are not limited to—

- Population.
- Propaganda.
- Commodities.
- Environment.

1-20. IPB is used primarily by commanders and staffs as a guide to evaluate specific datasets in order to gain an understanding of a defined operational environment. Prior to operations, an examination of national, multination partner, joint, and higher echelon databases is required to determine if the information requested is already available. As operations commence, new intelligence and information requirements are further identified as a result of battlefield changes. Publicly available information and open sources, when produced and properly integrated in support of the all-source intelligence effort, can be used to satisfy intelligence and information requirements. (For more information on IPB and indicators, see FM 2-01.3.)

Chapter 2

Planning and Preparation of the OSINT Mission

Directly or indirectly, publicly available information and open sources form the foundation for all intelligence when conducting operations. This foundation comes from open-source media components that provide worldview awareness of international events and perceptions of non-U.S. societies. This awareness prompts commanders to visualize a plan. Planning occurs when intelligence and information requirements are identified and means are developed as to how they will be satisfied. Effective OSINT mission planning and preparation are conducted during the Army force generation (ARFORGEN) train/ready force pool to enable the ease of transition to combat operations. (See FM 7-0 for more information on ARFORGEN.)

SECTION I – PLANNING OSINT ACTIVITIES

2-1. The *plan* step of the intelligence process consists of the activities that identify pertinent information requirements and develop the means for satisfying those requirements and meeting the commander's desired end state. As an aspect of intelligence readiness, planning for OSINT exploitation begins before a unit receives an official order or tasking as part of the *generate intelligence knowledge* continuing activity of the intelligence process.

2-2. The focus of OSINT research prior to deployment is determined and directed by the commander's guidance. Sustained and proactive open-source research using basic and advanced Internet search techniques plays a critical role in understanding AOs through foundational knowledge required for unit readiness and effective planning. Research during planning for possible missions provides insight into how nontraditional military forces, foreign military forces, and transnational threats have operated in similar AOs. Prior to deployment, organizations with dedicated OSINT missions can also be resourced to satisfy intelligence and information requirements. (See appendix E.)

2-3. After a unit receives a mission, the focus of OSINT research is further refined based on the AO in which the unit operates. OSINT supports the continuous assessment of unified land operations during planning. Effective research and planning ensure commanders receive timely, relevant, and accurate intelligence and information to accomplish assigned missions and tasks. The MDMP and IPB driven by the intelligence process frame the planning of OSINT exploitation. OSINT is integrated into planning through the four steps of the IPB process:

- Define the operational environment.
- Describe environmental effects on operations.
- Evaluate the threat.
- Determine threat COAs.

DEFINE THE OPERATIONAL ENVIRONMENT

2-4. When assessing the conditions, circumstances, and influences in the AO and area of interest, the intelligence staff examines all characteristics of the operational environment. There are preexisting publicly available inputs that can be used to identify significant variables when analyzing the terrain, weather, threat, and civil considerations. At the end of step one of the IPB process, publicly available information and open sources can be used to support the development of the AO assessment and area of interest assessment.

DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS

2-5. When analyzing the environmental effects on threat and friendly operations, publicly available information and open sources can be used to describe the—

- Physical environment (terrestrial, air, maritime, space, and information domains).
- Weather.
- Civil considerations.
- Threat.

2-6. Combine the evaluation of the effects of terrain, weather, and civil considerations into a product that best suits the commander’s requirements. At the end of the second step of IPB, publicly available information and open sources can be used to better inform the commander of possible threat COAs and products and assessments to support the remainder of the IPB process.

EVALUATE THE THREAT

2-7. Step three of the IPB process is to evaluate each of the significant threats in the AO. If the staff fails to determine all the threat factions involved or their capabilities or equipment, or to understand their doctrine and tactics, techniques, and procedures (TTP), as well as their history, the staff will lack the intelligence needed for planning. At the end of step three of IPB, publicly available information and open sources can provide the majority of the information required to identify threat characteristics, as well as provide possible information needed to update threat models.

DETERMINE THREAT COURSES OF ACTION

2-8. Step four of the IPB process is to identify, develop, and determine likely threat COAs that can influence accomplishment of the friendly mission. The end state of step four is to replicate the set of COAs available to the threat commander and to identify those areas and activities that, when observed, discern which COA the threat commander has chosen. At the end of step four of IPB, publicly available information and open sources can be used to determine indicators adopted by the threat commander.

SECTION II – PREPARATION OF OSINT ACTIVITIES

2-9. The reliance on classified databases has often left Soldiers uninformed and ill-prepared to capitalize on the huge reservoir of unclassified information from publicly available information and open sources, as the following quote describes:

> *OSINT was fairly new to us and once the term was understood we placed a signals intelligence analyst in charge of OSINT. At the tactical level, it seemed to be effective after the fact. There were three successful attacks against coalition forces aircraft in a specific area. We couldn’t figure out the “how” and 5Ws [who, what, when, where, why] but our OSINT analyst found a downed aircraft video on the Internet that helped us identify the ingress and egress routes used during the attack that led to a “no fly” area and successful area denial missions in our area of operation.*
>
> All-Source Intelligence Analyst, Combat Aviation Brigade
> Operation Iraqi Freedom 2008-2009,

OSINT EXPLOITATION

2-10. When preparing to conduct OSINT exploitation, the areas primarily focused on are—

- Public speaking forums.
- Public documents.
- Public broadcasts.
- Internet Web sites.

PUBLIC SPEAKING FORUMS

2-11. Acquiring information at public speaking forums requires close coordination to ensure that any overt acquisition is integrated and synchronized with the information collection plan and does not violate laws prohibiting the unauthorized collecting of information for intelligence purposes. (See appendix A for further information on U.S. persons.)

2-12. Before gathering OSINT information at public speaking forums—

- Coordinate with key staff sections, such as the G-2X/S-2X, G-7/S-7, G-9/S-9, public affairs officer (PAO), and staff judge advocate (SJA), prior to conducting surveillance.
- Identify additional force protection personnel and equipment requirements.
- Identify the procedure for emplacement and recovery of audio and video processing equipment.

2-13. The operation order (OPORD), TTP, or unit standard operating procedures (SOPs) should describe how the unit that is tasked with the public speaking forum mission requests, allocates, and manages funds to purchase digital camera and audio recording equipment along with the computer hardware and software to play and store video-related data.

PUBLIC DOCUMENTS

2-14. Organizations within an AO conduct document collection missions. Once collected, documents are analyzed and the information is disseminated throughout the intelligence community. Before executing any OSINT exploitation related to collecting public documents, it is important to—

- Coordinate document collection, processing, and analysis activities across echelons.
- Identify the procedure to deploy, maintain, recover, and transfer hardcopy, analog, and digital media processing and communications equipment.
- Identify academic and commercial-off-the-shelf (COTS) information services that are already available for open-source acquisition, processing, and production.

2-15. The OPORD, TTP, or unit SOPs should describe how the unit requests, allocates, and manages funds for—

- Document collection and processing services.
- Purchasing books, dictionaries, images, maps, newspapers, periodicals, recorded audio and video items, computer hardware, digital cameras, and scanning equipment.
- The cost of subscribing to newspapers, periodicals, and other readable materials.

2-16. For more detailed information on public documents and document exploitation, see TC 2-91.8.

PUBLIC BROADCASTS

2-17. The DNI OSC collects, processes, and reports international and regional broadcasts. This enables deployed organizations to collect and process information from local broadcasts that are of command interest. Before exploiting OSINT related to public broadcasts, it is important to—

- Coordinate broadcast collection, processing, and production activities with those of the OSC.
- Identify the procedure to deploy, maintain, recover, and transfer radio and television digital media storage devices and content processing and communications systems.

- Identify Internet collection and processing resources to collect on television or radio station-specific Web casts.

2-18. The OPORD, unit SOPs, or TTP should describe how the unit tasked with public broadcast missions requests, allocates, and manages funds to purchase antenna and computer equipment, machine translation services or software, and subscribes to regional and international satellite radio and television broadcast service providers.

INTERNET WEB SITES

2-19. Information collected, processed, and produced from Internet Web sites supports unified land operations. Before exploiting OSINT related to Internet Web sites—

- Coordinate Internet collection, processing, and analysis activities across echelons.
- Identify the procedure to deploy, maintain, recover, and transfer computers and associated communications and data storage systems.
- Coordinate with G-6/S-6 for access to the INTELINK-U network or approved commercial Internet service providers that support open-source acquisition, processing, storage, and dissemination requirements.
- Coordinate with G-6/S-6 to develop a list of authorized U.S. and non-U.S. Internet Web sites for official government use, open-source research, and non-U.S. Internet Web sites restricted to selected authorized personnel engaged in OSINT exploitation.
- Identify academic and COTS information services that are already available for open-source information acquisition, processing, and production.

2-20. The OPORD, unit SOPs, or TTP should describe how the unit tasked with Internet research missions requests, allocates, and manages funds to purchase digitized documents, geospatial information, computer hardware and software applications, as well any subscriptions to academic and commercial online databases, newspapers, periodicals, and references.

PREPARATION CONSIDERATIONS

2-21. Preparing for OSINT exploitation also includes—

- Establishing an OSINT architecture.
- Prioritizing tasks and requests.
- Task-organizing assets.
- Deploying assets.
- Assessing completed operations.

ESTABLISHING AN OSINT ARCHITECTURE

2-22. OSINT contributes to establishing an intelligence architecture, specifically ART 2.2.2, *Establish Intelligence Architecture*. Establishing an intelligence architecture comprises complex and technical issues that include sensors, data flow, hardware, software, communications, communications security materials, network classification, technicians, database access, liaison officers, training, and funding. A well-defined and -designed intelligence architecture can offset or mitigate structural, organizational, or personnel limitations. This architecture provides the best possible understanding of the threat, terrain and weather, and civil considerations. An established OSINT architecture incorporates data flow, hardware, software, communications security components, and databases that include—

- **Conducting intelligence reach.** *Intelligence reach* is a process by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command (FM 2-0).
- **Developing and maintaining automated intelligence networks.** This task entails providing information systems that connect assets, units, echelons, agencies, and multinational partners for

intelligence, collaborative analysis and production, dissemination, and intelligence reach. It uses existing automated information systems, and, when necessary, creates operationally specific networks.

- **Establishing and maintaining access.** This task entails establishing, providing, and maintaining access to classified and unclassified programs, databases, networks, systems, and other Web-based collaborative environments for Army forces, joint forces, national agencies, and multinational organizations.
- **Creating and maintaining databases.** This task entails creating and maintaining unclassified and classified databases. Its purpose is to establish interoperable and collaborative environments for Army forces, joint forces, national agencies, and multinational organizations. This task facilitates intelligence analysis, reporting, production, dissemination, sustainment, and intelligence reach.

Operational and Technical Open-Source Databases

2-23. OSINT exploitation requires access to databases and Internet capabilities to facilitate processing, storage, retrieval, and exchange of publicly available information. These databases are resident on local area networks (LANs), the World Wide Web (WWW), and the Deep Web (see appendix C for additional information). To support unified land operations, OSINT personnel use evaluated and analyzed publicly available information and open sources to populate information databases such as—

- **Operational information databases**, which support the correlation of orders, requests, collection statuses, processing resources, and graphics.
- **Technical information databases**, which support collection operations and consist of unprocessed text, audio files, video files, translations, and transcripts.

Open-Source Collection Acquisition Requirement–Management System

2-24. The primary open-source requirements management operational information and technical information database is the Open-source Collection Acquisition Requirement-Management System (OSCAR-MS). OSCAR-MS is a Web-based service sponsored by the Office of the Assistant Deputy Director of National Intelligence for Open Source (ADDNI/OS) to provide the National Open Source Enterprise (NOSE) with an application for managing open-source collection requirements. OSCAR-MS links OSINT providers and consumers within the intelligence community down to the brigade combat team (BCT) level. Personnel at the BCT level access OSCAR-MS via the SECRET Internet Protocol Router Network (SIPRNET) in order to submit requests for information to the Department of the Army Intelligence Information Services (DA IIS) request for information portal. The goal of the OSCAR-MS is to automate and streamline ad hoc open-source collection requirements by—

- Providing useful metrics to understand OSINT requirements.
- Allowing the digital indexing and tagging of submitted and completed open-source products to be searchable in the Library of National Intelligence.
- Providing for local control of administrative data such as unit account management, local data tables, and local formats.
- Allowing simple and flexible formats that employ database auto-population.
- Using complete English instead of acronyms, computer codes, and other nonintuitive shortcuts.
- Allowing linkages between requirements, products, and evaluations.
- Enabling integration of open-source users for collaboration between agencies.
- Reducing requirement duplication through customers directly contributing to existing requirements.

2-25. For more detailed information on OSCAR-MS or to submit OSINT requirements, contact the U.S. Army Intelligence and Security Command (INSCOM) DA IIS at https://www.intelink.gov/sharepoint/default.aspx.

PRIORITIZING TASKS AND REQUESTS

2-26. The G-2/S-2 and G-3/S-3 staffs use commander guidance and primary intelligence requirements to complete the information collection plan. The plan is used to assign tasks to subordinate units or submit requests to supporting intelligence organizations to achieve the desired information collection objectives. Embodied in the information collection plan, these tasks describe how the unit—

- Requests collection and production support from joint, interagency, intergovernmental, and multinational organizations.
- Task-organizes and deploys organic, attached, and contracted collection, processing, and production assets.
- Conducts remote, split-based, or distributed collection, processing, and production.
- Requests and manages U.S. and non-U.S. linguists based on priority for support, mission-specific skills, knowledge requirements (such as language, dialect, and skill level), clearance level, and category.

2-27. When developing information collection tasks for subordinate units, the G-2/S-2 and G-3/S-3 staffs use the task and purpose construct for developing task statements to account for—

- *Who* is to execute the task?
- *What* is the task?
- *When* will the task begin?
- *Where* will the task occur?

TASK-ORGANIZING ASSETS

2-28. With the exception of the Asian Studies Detachment (ASD) that maintains an organic table of distribution and allowances (TDA) with the government of Japan in support of U.S. Pacific Command (USPACOM), the Army does not have a TDA or base table of organization and equipment for OSINT personnel or units when preparing to conduct OSINT exploitation.

DEPLOYING ASSETS

2-29. Deployment of publicly available assets—

- Supports the scheme of maneuver.
- Supports the commander’s intent.
- Complies with unit SOPs.

2-30. The deployment of assets generally requires a secure position, with network connectivity to the Internet, in proximity to supporting sustainment, protection, and communications resources.

ASSESSING COMPLETED OPERATIONS

2-31. Typical guidelines used to assess operations are—

- Monitoring operations.
- Correlating and screening reports.
- Disseminating and providing a feedback mechanism.
- Cueing.

2-32. See paragraph 2-67 for an explanation of these guidelines.

SECTION III – PLANNING AND PREPARATION CONSIDERATIONS

2-33. Planning and preparation considerations when planning for OSINT exploitation include—

- Open-source reliability.
- Open-source information content credibility.
- Compliance.
- Operations security (OPSEC).
- Classification.
- Coordination.
- Deception and bias.
- Copyright and intellectual property.
- Linguist requirements.
- Machine foreign language translation (MFLT) systems.

OPEN-SOURCE RELIABILITY

2-34. The types of sources used to evaluate information are—

- Primary sources.
- Secondary sources.

2-35. A *primary source* refers to a document or physical object that was written or created during the time under study. These sources are present during an experience or time period and offer an inside view of a particular event. Primary sources—

- Are generally categorized by content.
- Is either public or private.
- Is also referred to as an original source or evidence.
- In fact, are usually fragmentary, ambiguous, and difficult to analyze. The information contained in primary sources is also subject to obsolete meanings of familiar words.

2-36. Some types of primary sources include—

- Original documents (excerpts or translations) such as diaries, constitutions, research journals, speeches, manuscripts, letters, oral interviews, news film footage, autobiographies, and official records.
- Creative works such as poetry, drama, novels, music, and art.
- Relics or artifacts such as pottery, furniture, clothing, artifacts, and buildings.
- Personal narratives and memoirs.
- Person of direct knowledge.

2-37. A *secondary source* interprets, analyzes, cites, and builds upon primary sources. Secondary sources may contain pictures, quotes, or graphics from primary sources. Some types of secondary sources include publications such as—

- Journals that interpret findings.
- Textbooks.
- Magazine articles.
- Commentaries.
- Histories.
- Criticisms.
- Encyclopedias.

Note. Primary and secondary sources are oftentimes difficult to distinguish as both are subjective in nature. Primary sources are not necessarily more of an authority or better than secondary sources. For any source, primary or secondary, it is important for OSINT personnel to evaluate the report for deception and bias.

2-38. Open-source reliability ratings range from **A** (reliable) to **F** (cannot be judged) as shown in table 2-1. A first-time source used in the creation of OSINT is given a source rating of **F**. An **F** rating does not mean the source is unreliable, but OSINT personnel have no previous experience with the source upon which to base a determination.

Table 2-1. Open-source reliability ratings

A	***Reliable***	**No doubt** of authenticity, trustworthiness, or competency; has a history of complete reliability.
B	***Usually reliable***	**Minor doubt** about authenticity, trustworthiness, or competency; has a history of valid information most of the time.
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** authenticity, trustworthiness, and competency; history of invalid information.
F	***Cannot be judged***	**No basis** exists for evaluating the reliability of the source.

OPEN-SOURCE INFORMATION CONTENT CREDIBILITY

2-39. Similar to open-source reliability, credibility ratings range from **one** (confirmed) to **eight** (cannot be judged) as shown in table 2-2. If the information is received from a first-time source, it is given a rating of **eight** and, like the reliability ratings scale, does not mean the information is not credible but that OSINT personnel have no means to verify the information.

Table 2-2. Open-source content credibility ratings

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.

COMPLIANCE

2-40. In accordance with EO 12333, DOD 5240.1-R, and AR 381-10, procedure 2, Army intelligence activities may collect publicly available information on U.S. persons only when it is necessary to fulfill an assigned function. (For more information on intelligence oversight, see appendix A.)

OPERATIONS SECURITY

2-41. OSINT could unintentionally provide present and future indicators of U.S. military operations. Information generally available to the public can reveal the existence of, and sometimes details about classified or sensitive information that can be used to neutralize or exploit military operations. Intelligence organizations must determine the level of contact with open sources and the collection or acquisition technique that could affect Army operations.

CLASSIFICATION

2-42. 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 consumers.” This is an appropriate warning for OSINT personnel where concern for OPSEC can undermine the ability to disseminate inherently unclassified information. Examples of unclassified information being over-classified are—

- Reported information found in a foreign newspaper.
- Message from a foreign official attending an international conference.

2-43. AR 380-5 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. Final analysis of OSINT may require additional restrictions and be deemed *controlled unclassified information* or *sensitive but unclassified information*.

COORDINATION

2-44. During planning, the G-2/S-2 and G-3/S-3 staff must ensure that OSINT missions and tasks are synchronized with the scheme of maneuver. Acquiring open-source information may compromise the operations of other intelligence disciplines or tactical units. Open-source acquisition that is not synchronized may also result in the tasking of multiple assets and the improper utilization of forces and equipment, adversely affecting the ability of nonintelligence organizations, such as civil affairs, military police, and public affairs, to accomplish assigned missions and tasks. Conversely, overt contact with an open source by nonintelligence organizations can compromise OSINT missions and tasks and lead to the loss of intelligence.

DECEPTION AND BIAS

2-45. Deception and bias is a concern in OSINT exploitation. OSINT exploitation does not normally acquire information by direct observation of activities and conditions within the AO. OSINT exploitation relies mainly on secondary sources to acquire and disseminate information. Secondary sources, such as government press offices, commercial news organizations, and nongovernmental organizations spokespersons, can intentionally or unintentionally add, delete, modify, or otherwise filter the information made to the general public. These sources may also convey one message in English with the intent to sway U.S. or international perspectives and a different non-English message for local populace consumption. It is important to know the background of open sources and the purpose of the public information in order to distinguish objectives, factual information, identify bias, or highlight deception efforts against the reader and the overall operation.

COPYRIGHT AND INTELLECTUAL PROPERTY

2-46. *Copyright* is a form of protection, for published and unpublished works, provided by Title 17, United States Code (USC), to authors of “original works of authorship,” including literary, dramatic, musical, and artistic works. Intellectual property is considered any creation of the mind and includes, but is not limited to—

- Musical works and compositions.
- Artistic displays.
- Discoveries.
- Inventions.
- Words or phrases.
- Symbols and designs.

2-47. It is illegal to violate the rights provided by the copyright law to the owner of copyright. One major limitation is the doctrine of fair use, which is given a statutory basis in Section 107 of the 1976 Copyright Act. According to the U.S. 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 the—

- Purpose and character of the use.
- Nature of the copyrighted work.
- Amount and substantiality of the portion used in relation to the copyrighted work as a whole.
- Effect of the use upon the potential market for or value of the copyrighted work.

2-48. AR 27-60 prescribes policies and procedures for the acquisition, protection, transfer, patent usage, copyrights, and trademarks of intellectual property. Army policy recognizes the rights of copyright owners consistent with Army missions and worldwide commitments. OSINT personnel will not produce or distribute copyrighted works without the permission of the copyright owner unless such use is authorized under U.S. copyright law. There is also a requirement for OSINT personnel to forward to the Service SJA for approval and waiver of notice to the copyright holder, if necessary, for OPSEC. (For more information on copyright laws and applicability, see the International Copyright Relations of the United States at http://www.copyright.gov or the local SJA office.)

LINGUIST REQUIREMENTS

2-49. The ability to gather and analyze foreign materials is critical in OSINT exploitation. The effective use and employment of linguists, both civilian and military, facilitates this activity. The areas of the highest criticality of required foreign language skills and knowledge proficiency are—

- **Transcription.** Both listening and writing proficiency in the source language are essential for an accurate transcript. A transcript is extremely important when English language skills of the OSINT personnel are inadequate for authoritative or direct translation from audio or video into English text.
- **Translation.** Bilingual competence is a prerequisite for translations. Linguists must be able to—
  - Read and comprehend the source language.
  - Write comprehensibly in English.
  - Choose the equivalent expression in English that fully conveys and best matches the meaning intended in the source language.
- **Interpretation.** Bilingual competence is a prerequisite for interpretation. Linguists must be able to—
  - Hear and comprehend the source language.
  - Speak comprehensibly in English.
  - Choose the equivalent expression in English that fully conveys and best matches the meaning intended in the source language.

Note. Interpretation is a specific skill in which not all linguists are trained.

2-50. To effectively plan and employ linguists, commanders and staffs must understand the Army linguist proficiency evaluation system. Evaluation and reevalution of linguist proficiency is covered in detail in AR 11-6, chapter 5. Language testing is required for all Army personnel, in a language-dependent military occupational specialty (MOS) or Army occupational code (AOC), who have received foreign language training. Other Army personnel who have knowledge of a foreign language are encouraged to take the proficiency test and may work as linguists.

2-51. The Army uses the Defense Language Proficiency Test (DLPT) to measure the proficiency level in a specific language. The DLPT is an indication of foreign language capability, but it is not the definitive evaluation of an individual's ability to perform linguist support.

2-52. The Army uses Interagency Language Roundtable (ILR) descriptions of the proficiency levels for the skills of speaking, listening, reading, and writing a foreign language. Detailed descriptions of these levels are available at http://www.govtilr.org. The plus-level designators, shown as a "+" symbol, are used to designate when a linguist is above a base level, but not yet to the capability of the next level. The six base levels of proficiency as established by the DLPT are—

- **Level 0 (no proficiency).** The Soldier has no functional foreign language ability. Level 0+ is the minimum standard for special-forces personnel and indicates a memorized proficiency only.
- **Level 1 (elementary proficiency).** The Soldier has limited control of the foreign language skill area to meet limited practical needs and elementary foreign language requirements.
- **Level 2 (limited working proficiency).** The linguist is sufficiently skilled to be able to satisfy routine foreign language demands and limited work requirements.
- **Level 3 (general professional proficiency).** The linguist is capable of performing most general, technical, formal, and informal foreign language tasks on a practical, social, and professional level.
- **Level 4 (advanced professional proficiency).** The linguist is capable of performing advanced professional foreign language tasks fluently and accurately on all levels.
- **Level 5 (functionally native proficiency).** The linguist is functionally equivalent to an articulate and well-educated native in all foreign language skills; the linguist reflects the cultural standards of the country where the foreign language is natively spoken.

2-53. The above proficiency base levels designate proficiency in any of the four language skills—listening, reading, speaking, and writing. The DLPT only evaluates reading and listening skills (for example, 2+/3, or 3/1+). Currently, these tests do not evaluate linguists above the 3-proficiency level. The current Army standard to be considered a qualified linguist is a level 2. Oral proficiency interviews evaluate speaking proficiency and may be used to provide a listening score. These interviews may provide an evaluation all the way up to the 5-proficiency level.

2-54. Along with proficiency and fluency, OSINT personnel must consider the biases and cultural backgrounds of civilian interpreters when analyzing non-English open-source information. When planning to utilize linguists, commanders must identify requirements by category. Linguist screening categories are—

- **Category I.** Linguists must at least have advanced professional proficiency in the target language, a level 4 as measured by the ILR and general working proficiency (ILR 2+) in English. They may be locally hired or from a region outside the AO. They do not require a security clearance.
- **Category II.** Linguists are U.S. citizens granted access to a Secret clearance by the designated U.S. Government personnel security authority. They must at least have advanced professional proficiency in the target language (ILR 4) and general working proficiency (ILR 2+) in English.
- **Category III.** Linguists are U.S. citizens granted Top Secret (TS)/Sensitive Compartmented Information (SCI) or an interim TS/SCI clearance by the designated U.S. Government personnel security authority. They must meet a minimum of ILR 3 in both the target language and English.

MACHINE FOREIGN LANGUAGE TRANSLATION SYSTEMS

2-55. Developing a reliable and proficient linguist requires a great deal of time, both for training and gaining experience. This extended timeline often results in shortages of linguist personnel. To fill personnel vacancies throughout Army units and to meet language requirements and demands, MFLT systems are used. When employed properly, MFLT systems can provide an increased capability for translation in support of unified land operations.

2-56. Reliable MFLT capability exists to translate media broadcasts into English and there is readily available software to translate Internet sources into English as well. There are limited speech-to-speech (S2S) capabilities in use.

FOREIGN MEDIA MONITORING

2-57. Media monitoring systems like the BBN Broadcast Monitoring System™ (BMS™) create a continuous searchable archive of international television broadcasts. These systems automatically transcribe the real-time audio stream and translate it into English. Both the transcript and translation are searchable and synchronized to the video, providing powerful capabilities for effective retrieval and precise playback of the video based on its speech content. With this system, intelligence analysts can sift through vast collections of news content in other languages quickly and efficiently.

2-58. These systems provide real-time transcription and translation of broadcast television news, allowing English speakers to rapidly triage non-English television content, be alerted when new content that matches a profile is captured by the system, and work closely with human linguists and cultural experts to create actionable high-quality translations of extracted content.

2-59. The interface allows users to quickly search for specific spoken content in the video archive through keyword queries in English or the source language. Search terms are highlighted in the results, which show an image thumbnail, the transcript segment in the original language, and an English translation. Clicking on a result begins playback of the segment.

2-60. Users interact with the system from any personal computer (PC) or laptop via a common high-speed Internet connection. The only required client software is Microsoft® Internet Explorer and Windows Media® Player.

2-61. The BBN BMS™ continuously captures, encodes, analyzes, and stores live video streams in an automatically maintained, dynamic cache containing 30 days of recorded audio or video. As the video plays back, the system highlights the spoken words in both the original language and the translation. The transcript is enriched by highlighting the names of people, locations, and organizations, and by separating the speakers in the audio file. Users can jump to any point in the cache and begin playback.

2-62. Users can extract video segments or still photos for sharing, presentation, and collaboration. Demonstration compact discs (CDs) contain extracted segments that preserve the highlighting and synchronization of video, transcript, and translation during playback.

2-63. The BBN BMS™ currently translates—

- Modern Standard Arabic.
- Mandarin Chinese.
- Western Hemisphere Spanish.
- Persian Farsi.
- North American English.
- United Kingdom English.
- French.
- Bahasa Indonesian.
- Hindi.
- Urdu.

2-64. The BBN BMS™ does not require any hardware setup, software installation, or onsite administration or maintenance by the customer.

SPEECH-TO-SPEECH

2-65. Army and Marine units continue to attempt to integrate available COTS S2S translation devices into predeployment training and military operations while deployed. The primary tactical use for these devices has been language translation within security operations conducted in and among a general population of non-English speaking people.

SECTION IV – MANNING THE OSINT SECTION

2-66. OSINT personnel that comprise the OSINT section within the intelligence staff section can consist of both intelligence and nonintelligence individuals with the technical competence, creativity, forethought, cultural knowledge, and social awareness to exploit open sources effectively. The designation of OSINT personnel to satisfy requirements, missions, and tasks is generally identified by commanders and task-organized through organic assets (intelligence personnel, nonintelligence personnel, U.S. and non-U.S. contractor personnel, or linguists) in support of unified land operations.

OSINT SECTION DUTIES

2-67. The duties of the OSINT section are to—

- **Monitor operations.** This ensures responsiveness to the current situation and to anticipate future acquisition, processing, reporting, and synchronization requirements.
- **Correlate reports.** Reports (written, verbally, or graphically) should correlate classified reports through OSINT validation.
- **Screen reports.** Information is screened in accordance with the CCIRs and commander's guidance to ensure that pertinent and relevant information is not overlooked and the information is reduced to a workable size. Screening should encompass the elements of timeliness, completeness, and relevance to satisfy intelligence requirements.
- **Disseminate intelligence and information.** Satisfied OSINT requirements are disseminated to customers in the form of useable products and reports.
- **Cue.** Effective cueing by OSINT to more technical information collection assets, such as human intelligence (HUMINT) and counterintelligence (CI) improves the overall information collection effort by keeping organizations abreast of emerging unclassified information and opportunities as well as enabling the use of a multidiscipline approach to confirm or deny information by another information source, collection organization, or production activity.
- **Provide feedback.** An established feedback mechanism is required to the supported commander or customer on the status of intelligence and information requirements.

OSINT SECTION AT THE BRIGADE COMBAT TEAM LEVEL

2-68. Each combatant command may have a task-organized OSINT cell or section to some varying degree in scope and personnel. At the tactical level of operations, it is commonplace for commanders to create OSINT cells from organic intelligence personnel to satisfy intelligence requirements.

2-69. The following quote illustrates how task organization of organic personnel within the common ground station (CGS) can assist in satisfying intelligence and information requirements using the Nonsecure Internet Protocol Routing Network (NIPRNET) and various electronic devices, such as an amplitude modulation and frequency modulation (AM/FM) radio, video cassette recorder (VCR), and digital video disc (DVD) player, to ensure the success of their BCT to perform information collection at the tactical operations center (TOC):

> *With their CGS team, four to five interpreters, 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 NIPRNET, AM/FM radio, and the daily newspaper. Also, the team acquired a VCR and DVD player to study confiscated propaganda and other media. They understand the importance of local reporting to the success of the BCT 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 (information collection) analysis team at the BCT TOC prior to submission to the BCT S-2 and dissemination to battalions or division.*
>
> Military Intelligence Company Commander, 3ID,
> Operation Iraqi Freedom 2004—2005

2-70. As displayed in figure 2-1, personnel comprising the OSINT section at the BCT level include—

- Section leader.
- Requirements manager.
- Situation development analyst.
- Target development analyst.

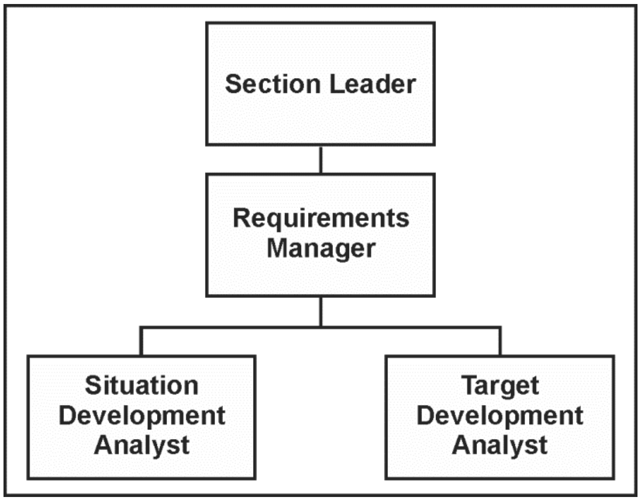

Figure 2-1. Brigade combat team's OSINT section

SECTION LEADER

2-71. The section leader—

- Is the primary liaison and coordinator with the BCT S-2.
- Provides supervisory and managerial capacity oversight.
- Sets the priority of tasks.
- Monitors ongoing intelligence support required by the BCT S-2.
- Ensures that all OSINT products are included in the planning for current and future operations.

REQUIREMENTS MANAGER

2-72. The requirements manager—

- Ensures that situation development and target development support the overall efforts of the section.
- Verifies the availability of collection assets.
- Performs quality control for situation development and target development products.
- Supervises the receipt, analysis, and dissemination of OSINT products.

SITUATION DEVELOPMENT ANALYST

2-73. The situation development analyst—

- Monitors publicly available information and open sources in order to ensure the most accurate common operational picture.
- Analyzes information and produces current intelligence about the operational environment, enemy, terrain, and civil considerations before and during operations.
- Refines information received on threat intentions, objectives, combat effectiveness, and potential missions.
- Confirms or denies threat COAs based on publicly available indicators.
- Provides information to better understand the local population in areas that include, but are not limited to—
  - Tribal affiliations.
  - Political beliefs.
  - Religious tenets.
  - Key leaders.
  - Support groups.
  - Income sources.

TARGET DEVELOPMENT ANALYST

2-74. The target development analyst—

- Identifies the components, elements, and characteristics of specific targets, both lethal and nonlethal.
- Identifies civil and other non-target considerations within the AO.
- Provides publicly available information on threat capabilities and limitations.

TASK ORGANIZATION CONSIDERATIONS

2-75. When task-organizing the OSINT section to satisfy intelligence and information requirements, units must consider—

- Mission command.
- Acquisition.
- Collecting and processing.
- Production.
- Computer systems.

MISSION COMMAND

2-76. Dedicated mission command personnel are needed in order to provide management and oversight of OSINT exploitation to ensure continued synchronization with maneuver elements, tasks, and requests.

ACQUISITION

2-77. Due to the volumes of publicly available information, acquisition through established information collection activities and systems are necessary in order to ensure that open-source information is not lost or misplaced that could provide essential and necessary mission-related information. Publicly available information acquired from open sources should be reported in accordance with established unit SOPs.

COLLECTING AND PROCESSING

2-78. OSINT properly integrated into overall collection plans during operations are used to satisfy CCIRs. In order to access the full array of domestic and foreign publicly available information, the processing of materials oftentimes requires OSINT support to personnel operating in the areas of document exploitation (DOCEX).

> ***Note.*** Personnel engaging in the collecting and processing of information involving these aspects will require an understanding of those items and materials that are commonplace and those that could possess intelligence value. They must further be versed in the additional regulations for Director, National Security Agency (DIRNSA) oversight. Unless foreign publicly available information and open sources are collected and subsequently processed into a suitable form, the information will lose intelligence value.

PRODUCTION

2-79. Production of actionable and timely publicly available information through open sources is vital in OSINT exploitation. Research methods, Internet techniques (basic and advanced), and other associated tools are utilized to retrieve, integrate, evaluate, analyze, and interpret information into OSINT. Research information and finalized metadata as products are stored in databases accessible to other intelligence and nonintelligence personnel that have vested OSINT exploitation requirements.

COMPUTER SYSTEMS

2-80. OSINT personnel conducting OSINT exploitation need to have software allocated to the appropriate task. The necessary unfettered exploitation suite includes such programs as Analyst Notebook, Portable Document Format (PDF) Maker, and Text Chart.

Chapter 3

Collecting OSINT

Due to the unclassified nature of publicly available information, those engaging in OSINT collection activities can begin researching background information on their assigned area of responsibility long before the issuance of an official military deployment order while generating intelligence knowledge. IPB, an integrating process for Army forces, is the mechanism identifying intelligence and information requirements that can be satisfied utilizing publicly available information and open sources.

COLLECTING PUBLICLY AVAILABLE INFORMATION

3-1. Publicly available information and open-source research, applied as an economy of force, is an effective means of assimilating authoritative and detailed information on the mission variables (METT-TC) and operational variables (political, military, economic, social, information, infrastructure, physical environment, time [PMESII-PT]). The compilation of unanswered intelligence and information requirements determined at the conclusion of the MDMP and IPB are exercised through the commander's input. Commander's input—

- Is expressed in the terms of describe, visualize, and direct.
- Is the cornerstone of guidance used by OSINT personnel.
- Validates intelligence and information requirements.

3-2. Commander's input is expressed as CCIRs and categorized as friendly force information requirements (FFIRs) and PIRs. Continuous research and processing methods, coupled with the commander's input and intelligence and information requirements, OSINT personnel collect publicly available information for exploitation. The *collect* step of the intelligence process involves collecting, processing, and reporting information in response to information collection tasks. Collected information is the foundation of intelligence databases, intelligence production, and situational awareness.

3-3. OSINT is integrated into planning through the continuous process of IPB. Personnel engaging in OSINT exploitation must initiate collection and requests for information to satisfy CCIRs to the level of detail required. Collecting open-source information comprises four steps, as shown in figure 3-1 on page 3-2:

- Identify information and intelligence requirements.
- Categorize intelligence requirements by type.
- Identify source to collect the information.
- Determine collection technique.

IDENTIFY INFORMATION AND INTELLIGENCE REQUIREMENTS

3-4. Intelligence and information gaps are identified during the IPB process. These gaps should be developed and framed around the mission and operational variables in order to ensure the commander receives the information needed to support all lines of operations or lines of effort. As information and intelligence are received, OSINT personnel update IPB products and inform the commander of any relevant changes. OSINT needs clearly stated information and intelligence requirements to effectively focus acquisition and production and should be incorporated into collection plans in order to satisfy these requirements.

> ***Note.*** OSINT cannot eliminate all the unknown aspects or uncertainties that concern commanders and staffs. The G-2/S-2 must be prepared to fill gaps with reasonable assumptions; once gaps are filled, the G-2/S-2 must begin developing databases at the unit level in order to have information readily available. This reduces the number of new requests for information from subordinate units or organizations.

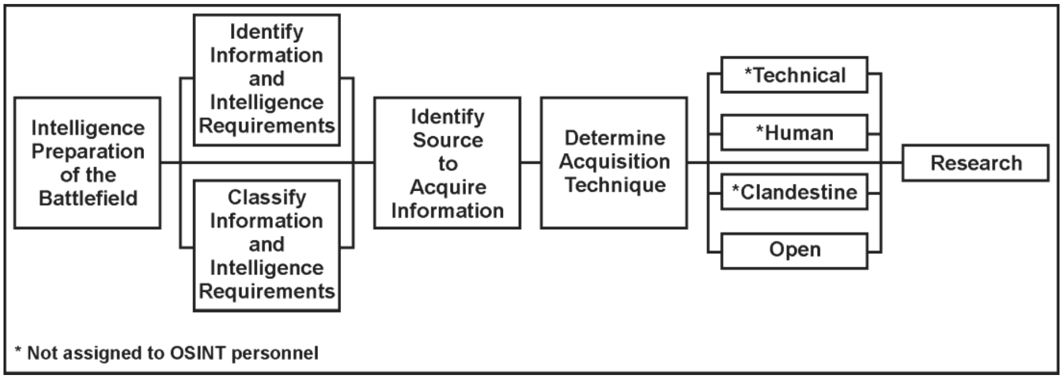
Intelligence Preparation of the Battlefield
Identify Information and Intelligence Requirements
Classify Information and Intelligence Requirements
Identify Source to Acquire Information
Determine Acquisition Technique
*Technical
*Human
*Clandestine
Open
Research
* Not assigned to OSINT personnel

Figure 3-1. Process for collecting publicly available information

CATEGORIZE INTELLIGENCE REQUIREMENTS BY TYPE

3-5. Intelligence requirements that need to be satisfied can extend beyond the scope of OSINT, resulting in gaps. OSINT is subject to information and intelligence gaps that need to be satisfied using other appropriate methods to close those gaps.

3-6. IPB is used to classify intelligence and information requirements by type based on mission analysis and friendly COAs. OSINT personnel provide input during this step. Two important related terms that work in concert with OSINT are private information and publicly available information:

- **Private information** comprises data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization. Intelligence requirements that require private information are not assigned to OSINT sections. There are two subcategories of private information:
  - ***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*).
  - ***Classified information*** requires protection against unauthorized disclosure and is marked to indicate its classified status when produced or disseminated.
- **Publicly available information** comprises 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.

> ***Note.*** The amount of classified information produced on any one topic can be limited and taken out of context if viewed from a solely classified perspective. OSINT validation is necessary when dealing with a large amount of classified information. OSINT validation is used when classified sources are unavailable or to confirm or support preexisting classified sources. This strengthens the credibility of OSINT products in support of all-source intelligence. OSINT validation provides the ability to cue other assets thus enhancing the accuracy and precision of gained intelligence.

IDENTIFY SOURCE TO COLLECT INFORMATION

3-7. Identifying the source is part of planning requirements and assessing collection plans. The two types of sources used to collect information are confidential sources and open sources:

- **Confidential sources** comprise any persons, groups, or systems that provide information with the expectation that the information, relationship, or both are protected against public disclosure. Information and intelligence requirements that require confidential sources are not assigned to OSINT sections.
- **Open sources** comprise any person or group that provides information without the expectation of copyright or privacy—the information, the relationship, or both is not protected against public disclosure. Open sources include but are not limited to—
  - ***Academia.*** Courseware, dissertations, lectures, presentations, research papers, and studies in both hardcopy and softcopy covering subjects and topics on economics, geography (physical, cultural, and political-military), international relations, regional security, and science and technology.
  - ***Government agencies and nongovernmental organizations.*** Databases, posted information, and printed reports on a wide variety of economic, environmental, geographic, humanitarian, security, and 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.
  - ***Individuals and groups.*** Handwritten, painted, posted, printed, and broadcasted information on subjects and topics on art, graffiti, leaflets, posters, tattoos, and Web sites.
  - ***Gray literature.*** Materials and information that are found using advanced Internet search techniques on the Deep Web consisting of technical reports, scientific research papers, and white papers.

DETERMINE COLLECTION TECHNIQUE

3-8. Collection implies gathering, by a variety of means, raw data and information from which finalized intelligence is then created or synthesized, and disseminated. Collected information is analyzed and incorporated into all-source and other intelligence discipline products. These products are disseminated per unit SOPs, OPORDs, other established feedback mechanism, or intelligence architecture. These techniques confirm the presence of planned targets and provide a baseline of activity and information on sources within the AO for further development and future validation. When gathering information, the utilized technique includes specific information requests, objectives, priorities, timeframe of expected activity, latest (or earliest) time the information is of value (LTIOV), and reporting instructions.

3-9. Open-source information that satisfies a CCIR is disseminated as quickly as possible to the commander and other staff personnel per unit SOPs or OPORDs. OSINT can use unintrusive collection techniques to cue more technical collection assets. Collection techniques, depending on operation complexities, can enhance the chances of satisfying intelligence and information requirements.

3-10. Open-source acquisition of information and intelligence requirements are assigned to OSINT personnel. Open-source collection includes the acquisition of material in the public domain. The extent to which open-source collection yields valuable information varies greatly with the nature of the target and the subject involved. The information might be collected by individuals who buy books and journals, observe military parades, or record television and radio programs.

RESEARCH

3-11. After determining the collection technique, OSINT personnel conduct research to satisfy intelligence and information requirements.

3-12. Research—

- Leads to the population of information and intelligence databases. These databases enable OSINT personnel to accurately respond to changes within the AO by providing requested information to satisfy requirements.
- Is used to gather information that contributes to providing an understanding of a problem and organizing the results comprehensively.
- Is used to generate intelligence knowledge before and during deployments.

3-13. Two types of research methods that can be used are—

- **Field research.** Personnel from academic, governmental, intergovernmental, and nongovernmental organizations acquire data from primary sources, as well as retrieve data and information from secondary sources. Field research—
  - Consists of participant observation, data collection, and survey research.
  - Is typically conducted at the operational and strategic levels when time is not a factor in the development of information and intelligence of the operational variables (PMESII-PT) to provide commanders situational awareness.
- **Practical research.** Intelligence personnel retrieve existing data and information from secondary sources. Practical research—
  - Is typically conducted at the tactical level when time is a factor in the development of information and intelligence of the mission variables (METT-TC) in providing commanders situational awareness.
  - Is primarily used among intelligence personnel that engage in OSINT exploitation.

3-14. All research begins with the determination of a research question and the development of a research plan.

DETERMINE RESEARCH QUESTION

3-15. Research begins with the determination of a research question expressed in the form of CCIRs regarding a given topic. In OSINT exploitation, the research question can be based on the mission variables (METT-TC) and operational variables (PMESII-PT). The research question is refined through the development of information and intelligence requirements to be satisfied. Those requirements that are not satisfied are included in the planning requirements and assessing collection plan where more technical means of collection can be utilized.

DEVELOP RESEARCH PLAN

3-16. Different facets of a question may be expressed as information and intelligence requirements. These requirements form the basis for the research plan. A research plan can use both field research and practical research. The plan consists of—

- Identification of information sources (both primary and secondary).
- Description of how to access those sources.
- Format for compiling the data.
- Research methodology.
- Dissemination format.

IMPLEMENT RESEARCH PLAN

3-17. Utilizing open-source media—the means of sending, receiving, and recording information—components, and associated elements (see table 3-1), OSINT personnel implement a research plan. The primary media used to implement a research plan include—

- Public speaking forums.
- Public documents.
- Public broadcasts.
- Internet Web sites.

Note. The table does not illustrate an all-inclusive list of open-source media types but rather the categories of open-source media to consider when collecting open-source information.

Table 3-1. Open-source media, components, and elements

Media	*Components*	*Elements*	
Public Speaking	Speaker	• Sponsor • Relationship	• Message
	Format	• Conference • Debate • Demonstration • Speeches	• Lecture • Rally • Loud speakers • Talk shows
	Audience	• Location	• Composition
Public Documents	Graphic	• Drawing • Engraving • Painting • Graffiti	• Photograph • Print • Posters
	Recorded	• Compact data storage device • Digital video disk	• Hard disk • Tape
	Printed	• Book • Brochure • Newspapers • Magazines • Government releases • "Dumpster diving" • Annuals	• Periodical • Pamphlet • Report • Novelties • Non-government releases • Leaflets • Business cards
Public Broadcasts	Radio	• Low frequency AM radio • Medium frequency AM radio • Short wave radio	• VHF FM radio • Satellite radio • Standard wave radio
	Television	• Ku band satellite television • VHF and UHF terrestrial television • Advertisements • Motion pictures	
Internet Web Sites	Communications	• Chat • E-mail • News; newsgroup	• Web cam • Web cast • Web log
	Databases	• Commerce • Education	• Government • Military organizations
	Information (Web page content)	• Commerce • Education	• Government • Military organizations
	Services	• Dictionary • Directory • Downloads • Financial	• Geospatial • Search and URL lookup • Technical support • Translation
AM	amplitude modulation	URL	uniform resource locator
FM	frequency modulation	VHF	very high frequency
UHF	ultrahigh frequency		

Public Speaking Forums

3-18. OSINT personnel conduct research by attending public speaking forums such as conferences, lectures, public meetings, working groups, debates, and demonstrations. Attending these and similar events are opportunities to build relationships with nonmilitary professionals and organizations. Intelligence personnel require a thorough understanding of the local culture and laws to ensure any collection activities are unintrusive and do not violate local customs or laws, such as the Chatham House Rule. It is recommended to have the SJA's oversight during such collection missions to ensure compliance with AR 381-10, procedure 10. OSINT personnel require situational awareness and cultural understanding that is typically done by establishing both military and nonmilitary relationships with attendees, identifying any modifications of a speaker's message, and identifying personnel of interest attending the event.

3-19. OSINT personnel engaging in open-source exploitation, utilize public speaking forums typically in operational environments dominated by either stability operations or counterinsurgency operations where the level of violence is low.

Note. The Chatham House Rule states, "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 speakers, nor any other participants, may be revealed." Questioning the invocation of the Chatham House Rule should be inquired before the engagement begins. An invoked Chatham House Rule changes the characterization of the source from an open to a confidential source and may demand collection restrictions to ensure compliance with intelligence oversight limitations. (See appendix A.)

Public Documents

3-20. When acquiring public documents, OSINT personnel must be aware of the local environment and use a technique that is unintrusive and appropriate for the situation. These techniques include but are not limited to—

- Photographing and copying 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, and posters.
- 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.

Public Broadcasts

3-21. Regional bureaus of the DNI OSC collect on regional and international broadcast networks in accordance with open-source information and intelligence requirements. Coverage of regional and international broadcasts enables OSINT personnel and organizations to use assets from already identified sources. The four techniques used to acquire information of public broadcasts are—

- **Spectrum search.** Searching the entire spectrum to detect, identify, and locate all emitters to confirm overall activity. This search provides an overview of the amount and types of activities and where they are located in the spectrum.
- **Band search.** Searching a particular segment of the spectrum to confirm overall activity. By limiting the size of the search band, the asset can improve the odds of acquiring a signal.
- **Frequency search.** Searching for radio or television frequencies.
- **Program search.** Searching for radio or television programs. Programs vary by type, content characteristics, and media format. Program surveillance verifies and expands upon initial results.

Note. For best results, OSINT personnel should use these techniques in combination rather than independently to generate intelligence knowledge. The selection of the techniques depends on the mission, the number of personnel, and capabilities.

3-22. For detailed information on collecting information from public broadcasts, see the DNI OSC.

Internet Web Sites

3-23. The four steps to acquire information on Internet Web sites are—

- Plan Internet search.
- Conduct Internet search.
- Refine Internet search.
- Record results.

3-24. For more detailed information on research using Internet Web sites, see appendix C.

Chapter 4

Producing OSINT

The Army operates in diverse environments around the world. This diversity requires proper use of publicly available information and open sources in the production of OSINT. Given the volume of existing publicly available information and the unpredictability of requests for information and intelligence requirements, OSINT personnel engaging in open-source exploitation must be fluidly aware of and flexible when producing OSINT. Effective production ensures that commanders and subordinates receive timely, relevant, and accurate intelligence. OSINT personnel produce OSINT by evaluating, analyzing, reporting, and disseminating intelligence as assessments, studies, and estimates.

CATEGORIES OF INTELLIGENCE PRODUCTS

4-1. After receiving a mission through the MDMP and commander's intent—expressed in terms of *describe*, *visualize*, and *direct*—intelligence and information requirements are identified. Personnel engaging in OSINT exploitation typically gather and receive information, perform research, and report and disseminate information in accordance with the categories of intelligence products. (See table 4-1.) OSINT products are categorized by intended use and purpose. Categories can overlap and some publicly available and open-source information can be used in more than one product. (For more detailed information on the categories of intelligence products, see FM 2-0.)

Table 4-1. Categories of intelligence products

Indications and Warning
Indications and warning are intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve an threat to the United States, U.S. ally, or U.S. citizens abroad. It includes forewarning of hostile actions or intentions against the United States, its activities, overseas forces, or allied/coalition nations (JP 2-0).
Current Intelligence
Current intelligence supports ongoing operations; it involves the integration of time-sensitive, all-source intelligence and information into concise, accurate, and objective reporting on the area of operations (AO) and current threat situation. One of the most important forms of current intelligence is the threat situation portion of the common operational picture. The intelligence officer is responsible for producing current intelligence for the unit. In addition to the current situation, current intelligence should provide projections of the threat's anticipated actions and their implications on the friendly operation. (See JP 2-0.)
General Military Intelligence
General military intelligence is intelligence concerning (1) military capabilities of foreign countries or organizations or (2) topics affecting potential U.S. or multinational military operations relating to armed forces capabilities, including threat characteristics, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness and area terrain intelligence… (excludes scientific and technical intelligence (JP 2-0). This broad category of intelligence is normally associated with long-term planning at the national level. ***Note.*** This definition was shortened for brevity. The complete definition is available in JP 2-0.

Table 4-1. Categories of intelligence products (continued)

Target Intelligence
Intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance (JP 3-60). Target intelligence is the analysis of threat units, dispositions, facilities, and systems to identify and nominate specific assets or vulnerabilities for attack, reattack, or exploitation. It consists of target development and combat assessment. Target development is the systematic evaluation and analysis of target systems, system components, and component elements to identify high-value targets for potential engagement through lethal or nonlethal means. Combat assessments provide a timely and accurate estimate of the effects of the application of military force (lethal or nonlethal) and mission command warfare on targets and target systems based on predetermined objectives.
Scientific and Technical Intelligence
Scientific and technical intelligence is the product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information. Scientific and technical intelligence covers foreign developments in basic and applied research and in applied engineering techniques and scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the related research and development, and the production methods employed for their manufacture (JP 2-01).
Counterintelligence
Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities (EO 12333). Counterintelligence analyzes the threats posed by foreign intelligence and security services, and international terrorist organizations, and the intelligence activities of non-state actors such as organized crime, terrorist groups, and drug traffickers.
Estimative
Intelligence that identifies, describes, and forecasts adversary capabilities and the implications for planning and executing military operations (JP 2-0). Estimates provide forecasts on how a situation may develop and the implications of planning and executing military operations. Estimative intelligence goes beyond descriptions of threat capabilities or reporting of threat activity and tries to forecast the unknown based on an analysis of known facts using techniques such as pattern analysis, inference, and statistical probability.

EVALUATE INFORMATION

4-2. Open sources are overt and unclassified. Due to these aspects of publicly available information and open sources, deception, bias, and disinformation are of particular concern when evaluating sources of information during OSINT exploitation. Information is evaluated in terms of—

- Communications.
- Information reliability and credibility.

COMMUNICATIONS

4-3. A simple communications model is typically two-way and consists of six parts:

- Intended message.
- Speaker (sender).
- Speaker’s encoded message.
- Listener (receiver).
- Listener’s decoded message.
- Perceived message.

4-4. The speaker and listener each have different perspectives and aspects of communications (as shown in table 4-2 on page 4-4). There are great challenges facing communicators as the message becomes encoded by the speaker and decoded by the listener.

4-5. Communications during public speaking engagements are often difficult to evaluate given the myriad of elements that can prevent a successfully transmitted message. Given the multiple elements taken simultaneously, public speaking events are subjective and can be misunderstood.

4-6. The speaker has an intended message through a verbal, nonverbal, vocal, or visual media channel or combination thereof. Within communications, the areas typically involved in preventing the true intent of the message are the sending method, environment, and receiving method. Having an understanding of these areas generally yields a greater success rate between the speaker and listener.

4-7. Verbal communication begins with a speaker imparting or interchanging thoughts, opinions, or information. This communication can be either positive or negative. The typical speaker has a communication type:

- Passive.
- Aggressive.
- Passive-aggressive.
- Assertive.

4-8. Speakers communicate verbally and nonverbally based on their beliefs, emotions, or goals. These types of communication are indicated in table 4-2 on page 4-4. It is important to understand the differences in communication styles, how they are interpreted by an audience in order to effectively communicate the message intended and avoid misunderstandings. Evaluating information acquired through public speaking venues can be challenging based on these factors. Using the table to compare these types of communication can assist collection personnel in determining the influences surrounding communicators and predicting how the messages may be perceived. Table 4-2 illustrates and provides a guideline to assist in determining the type of displayed behavior, beliefs, emotions, and goals.

> ***Note.*** Table 4-2 is not intended to stand alone but used in support of all-source intelligence. Publicly available information and open sources are used to develop personality and characteristic traits of an individual. These traits include previous speeches, lectures, sermons, or statements that are used to determine a baseline of anticipated behavior and responses. There are external influences that can positively or negatively affect an individual. These external influences include but are not limited to consequences of disputing a superior’s opinion, the atmosphere or setting (such as academic, religious, or political), or an impromptu public interview using a question and answer format.

INFORMATION RELIABILITY AND CREDIBILITY

4-9. OSINT personnel evaluate information with respect to reliability and credibility. It is important to evaluate the reliability of open sources in order to distinguish objective, factual information; bias; or deception. The rating is based on the subjective judgment of the evaluator and the accuracy of previous information produced by the same source.

4-10. OSINT personnel must assess the reliability and the credibility of the information independently of each other to avoid bias. The three types of sources used to evaluate and analyze received information are—

- **Primary sources.** Have direct access to the information and conveys the information directly and completely.
- **Secondary sources.** Conveys information through intermediary sources using the vernacular and summarizes or paraphrases information.
- **Authoritative sources.** Accurately reports information from the leader, government, or ruling party.

> ***Note.*** Secondary and authoritative sources, such as government press offices, commercial news organizations, political campaign staffs, research center publications, newspapers, periodicals, databases, and libraries, can intentionally or unintentionally add, delete, modify, or filter the information made available to the public.

Table 4-2. Comparison of communication types

	Passive	*Aggressive*	*Passive-Aggressive*	*Assertive*
Behavior	• Keeps quiet. • Does not say what is actually felt, needed, or wanted. • Frequently puts oneself down. • Apologizes when expressing oneself. • Denies feelings of disagreements or indifferences.	• Expresses feelings and wants as though any other view is unreasonable or stupid. • Dismisses, ignores, or insults the needs, wants, and opinions of others.	• Fails to meet the expectations of others through 'deniable' means (such as forgetting or delays). • Denies personal responsibility for actions.	• Expresses needs, wants, and feelings directly and honestly. • Does not assume correctness or everyone feels similar. • Allows others to hold other views without dismissal or insults.
Nonverbal Communication	• Minimizes oneself. • Looks down, hunches shoulders, avoids eye contact. • Speaks softly.	• Enlarges oneself and appears threatening. • Eye contact is fixed and penetrating. • Voice is loud, perhaps shouting.	• Typically mimics the passive style.	• Body is relaxed, and movements are casual. • Eye contact is frequent but not glaring.
Beliefs	• Others' needs are more important. • Others have more rights. • Others' contributions are more valuable.	• Personal needs are more important and more justified than others'. • Others have no personal rights. • Personal contributions are more valuable.	• Entitled to get own way, even after making commitments to others. • Not responsible for personal actions.	• Everyone's needs are equally important. • Everyone has equal rights to be expressive. • Everyone has valuable contributions. • Responsible for personal behavior.
Emotions	• Fears rejection. • Feels helpless, frustration, and anger. • Bears resentment toward others' mistreatment. • Has reduced self-respect.	• Angry or powerful at the time of victory. • Feels remorse, guilt, or self-hatred for hurting others.	• Fears assertiveness. • Resents the demands of others. • Fears of being confronted.	• Feels positive about oneself and the treatment of others. • High level of self-esteem.
Goals	• Avoids conflict. • Pleases others at any expense. • Gives others control.	• Wins at any expense to others. • Gets control over others.	• Gets personal way without having to take responsibility.	• Self-respect is kept by everyone. • Expresses oneself without having to win all the time. • No one controls anyone else.

4-11. Nonauthoritative sources lack reliability and trustworthiness and seldom stand apart from authoritative sources. The information provided by nonauthoritative sources generally does not support topics agreed upon as being true and reliable in academia. Nonauthoritative sources also make finding additional in-depth information difficult to locate.

4-12. Nonauthoritative sources are generally unavailable and inaccessible by the public. Nonauthoritative sources are uncorroborated by multiple public sources of information. Examples of nonauthoritative sources include but is not limited to—

- Unreviewed documents from self-published Web repositories such as blogs, Wikipedia, political sites, and commercial advertising.
- Material received via uncorroborated e-mail, hearsay, or statements solely in oral form.
- Informal personal communications such as letters to the editor and opinion essays.

4-13. When evaluating sources of information to determine reliability and credibility consider—

- **Identity.** *Who* produced the information (for example a student, teacher, political organization, or reporter)?
- **Authority.** *How* much does the source know about the information?
- **Motive.** *Why* was the information published?
- **Access.** Did the source have direct access to the event or information?
- **Timeliness.** *What* is the date of the information?
- **Internal and external consistency.** Does the information contradict governmental policies among local citizens?

PROCESS INFORMATION

4-14. *Process* is an information management activity: to raise the meaning of information from data to knowledge (FM 6-0). The function of processing, although not a component of the intelligence process, is a critical element in the analyzing and producing of OSINT. Publicly available information answers intelligence and information requirements. Based on the type of information received, it must be processed before being reported and disseminated as finalized OSINT. Intelligence personnel transform publicly available information and open sources into a form suitable for processing by—

- Digitizing.
- Transcribing and translating.

DIGITIZING

4-15. OSINT personnel create a digital record of documents by scanning or taking digital photographs. Pertinent information about the document must be annotated to ensure accountability and traceability. Digitization enables the dissemination of the document to external databases and organizations, as well as enables the use of machine translation tools to screen documents for keywords, names, and phrases.

TRANSCRIBING AND TRANSLATING

4-16. A *transcript* refers to a written verbatim, native language rendering of the spoken words in an audio or video recording. Both listening and writing proficiency in the source language are essential for an accurate transcript. The transcript includes descriptions of the activity, background, and conditions that the transcriber hears in the audio and observes in the video. The linguist uses online dictionaries, gazetteers, working aids, and software to improve the transcript. Once completed, the transcription is sent to a quality control linguist.

4-17. A *translation* is not verbatim but an approximation of the literal and implied meaning of the foreign language. The linguist must be able to read and comprehend the source language, write comprehensibly in English, and choose the equivalent expression in English that fully conveys and best matches the meaning intended in the source language.

4-18. During processing, a linguist creates either an extract, a summary, or a full translation of the original document or transcript into a standardized format established by unit SOPs. The linguist uses online dictionaries, gazetteers, working aids, and software to improve the translation. Once completed, the translation is sent to a quality control linguist.

4-19. Linguists perform quality control reviews of each transcription and translation to ensure both quality and consistency with established unit SOPs. A U.S. Government or military linguist should review all information that a non-U.S. Government linguist processes with exceptions involving long-term multinational partners of the United States and U.S. contractors with the requisite skills and the confidence of the command. Linguistic quality control is an important facet to process foreign publicly available information. Each transcription and translation undergoes two levels of review:

- **Quality control.** During quality control, a qualified linguist ensures that the transcription or translation is accurate, complete, free of bias, and in accordance with reporting and dissemination standards. The U.S. linguist returns the transcript or translation for correction, adds or corrects missed content, or corrects minor format errors. Upon completion of quality control, the transcription or translation is available for processing.
- **Quality assurance.** During quality assurance, a qualified U.S. linguist or OSINT analyst reviews the transcript or translation to ensure that it contains all required information and reads naturally in English. Once reviewed, the completed transcription or translation is saved to internal databases to be processed for reporting and dissemination.

ANALYSIS OF MEDIA SOURCES

4-20. Analysis of the media is the systematic comparison of the content, behavior, patterns, and trends of organic media organizations and sources of a country. Analysis of the media as an activity was developed and based on methods and experience gained during OSINT exploitation against authoritarian political systems during the World War II and Cold War eras where media was government-controlled. Publicly available information and open sources must be analyzed for proper inclusion in OSINT processing. OSINT personnel weigh media analysis against set criterion. These criterions assist OSINT personnel to discern facts, indicators, patterns, and trends in information and relationships. This involves inductive or deductive reasoning to understand the meaning of past events and predict future actions.

4-21. Comparison of trends in the content of individual media with shifts in official policy suggests that some media continues to mirror the dominant policy line. By establishing a track record for media that is vulnerable to external and internal pressure to follow the central policy line, OSINT personnel can identify potential policy shifts. 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 media source analysis.

4-22. Media source analysis is also important in semi-controlled and independent media environments. In media environments where both official and nonofficial media are present, official media may be pressured to follow the central policy line. Analyzing media in these environments must encompass both the journalist and commentator level. It is important to establish the track record of such individuals to discover access to insider information from parts of the government or being used by officials to float policies.

Note. Differences in content between media outlets controlled by different official elites can reveal policy and leadership disputes. For example, a report on a speech by the President covered by government-controlled media may reveal differences from reports covering the same speech in either a semi-controlled or independent media environment.

4-23. The three aspects of media source analysis are—

- Media control.
- Media structure.
- Media content.

Media Control

4-24. Analyzing media environments in terms of media control requires awareness by intelligence personnel of how different elements of the media act, influence, and are of intelligence value. Careful examination of the differences in how media is handled in different types of environments can provide insight into domestic and foreign government strategies. Media environments are categorized as—

- **Government-controlled.**
  - Control over the media is centralized.
  - The dominant element of control is the government and higher tiers of political leadership.
  - Governments use censorship mechanisms to exercise control over media content prior to dissemination of information.
- **Semi-controlled.**
  - Control over the media is semi-centralized.
  - Governments exercise and promote self-censorship by pressuring media managers and journalists prior to dissemination of information.
- **Independent.**
  - Control over the media is decentralized.
  - Governments may regulate allocation of broadcast frequencies, morality in content, ownership in media markets, and occasionally apply political pressure against media or journalists.
  - 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.

4-25. All media environments are controlled to some degree and therefore easier to perform media source analysis. The challenge for OSINT personnel is to determine the level, factors, and elements (see table 4-3) that elites, institutions, or individuals exercise control, how much power each possesses, and what areas are of interest to satisfy intelligence and information requirements.

Table 4-3. Level, factors, and elements of media control

Level	*Factor*	*Elements*
Political	The laws and norms governing operations of the media, officials, and the distribution of power	• Top leadership consensus • Top leaders individually • Institutions
Journalist	The degree of freedom afforded to the media by the political system that is subordinated from media executives, to media managers, and to individual journalists	• Board of directors of media companies • Individual directors • Influential shareholders • Managing editors • Department editors • Program producers • Anchors • Individual journalist
Individual	The laws and norms governing the appearance and behavior of individuals in the media	• Group of subjects or participants • Individual subject or participant

Media Structure

4-26. Media structure encompasses attributes of media material. There are structural elements that affect the meaning and significance of the content of the item and are often as important as the content itself. Analysis of these elements uncovers insights into the points of view of personnel in government-controlled, semi-controlled, and independent environments to establish the structure of media elements.

4-27. The media structural elements are—

- Selection, omission, and slant.
- Hierarchy of power.
- Format.
- Media type.
- Prominence.
- Dissemination.
- Timing.

Selection, Omission, and Slant

4-28. Selection of media items is a fundamental editorial decision at the core of news reporting. Selection includes media manager decisions about which stories are covered, which stories are not covered, and which slant (viewpoint), images, and information should be included, emphasized, deemphasized, or omitted in a news item.

Hierarchy of Power

4-29. All political systems involve a hierarchy of power (see table 4-4) that logically follows official statements issued by elements in corresponding hierarchy of authoritativeness. Authoritativeness is the likelihood that the views expressed in the statement represent the dominant viewpoint within the political system. The hierarchy is obvious at the political level—a statement by the prime minister trumps a statement by a minister. In other cases, the hierarchy may not be so obvious—a speech by the party chairman is more authoritative than the head of state.

Table 4-4. Hierarchy of media power

Information Type	***Purpose***	***Example***
Reports	Inform the viewer, listener, or reader	Authoritative or nonauthoritative 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 • Associated with major party • Contributor to a major paper **Editors** 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 interests or radical views • Local officials and citizens
Official Statement	Declaration of policy or position by an officer or an executive body of the government or ruling party	Authoritative: • President • Secretary of State • State Department spokesperson

Format

4-30. Format consists of how media is produced and disseminated for public consumption. Format can be in the form of a live news report, a live interview, or a prerecorded report or interview that gives individuals more opportunity to influence the context delivered to consumers.

Media Type

4-31. Television is the medium with the largest potential audience in media environments and has a significant impact in shaping the impressions of the general viewing public. Television has replaced radio as the main source of news except in media environments where poverty prevents mass access to television. Fewer people may get information from newspapers and Internet news Web sites, but these people may be richer, better educated, and more influential than the general television audience. Specialized print publications and Internet Web sites reach a still smaller audience, but the audience will likely include officials and experts who that have influence on policy debates and outcomes.

Prominence

4-32. Questions to consider pertaining to prominence of media stories are—

- Does the story appear on the front page of newspapers or on the homepage of news Web sites?
- 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?
- How much airtime did it get?

Dissemination

4-33. Attention to patterns of dissemination of leader statements is important in government-controlled media environments. Leaders communicate publicly in a variety of ways such as formal policy statements, formal interviews, and impromptu remarks. By comparing the volume of media attention given to a statement, determination is made to whether the statement was intended to be taken as a pronouncement of established policy or merely as an ad hoc, uncoordinated expression prompted by narrow contextual or temporal conditions.

Timing

4-34. OSINT personnel have traditionally paid close attention to the timing of the appearance of information in the media as the information corresponds to the news cycle. A news cycle is the process and timing by which different types of media sources obtain information, incorporate or turn the information into a product, and make the product available to the public.

Media Content

4-35. Understanding the significance of media content can enhance the value of media source analysis. Media content encompasses the elements of—

- Manifest content.
- Latent content.

Manifest Content

4-36. Manifest content is the actual words, images, and sounds conveyed by open sources. One of the most important forms of media source analysis involves the careful comparison of the content of authoritative official statements to identify the policies or intentions represented. Governments, political entities, and actors use statements and information released to the media to strengthen, support, and promote policies.

4-37. Manifest content analysis of authoritative public statements is an effective tool to discern leadership intentions and attitudes. Manifest content, in order to be effective, consists of the following:

- **Esoteric communications** or "reading between the lines" are public statements whose surface meaning (manifest content) does not reveal the real purpose, meaning, or significance (latent content) of the author. Esoteric communication is particularly evident in political systems with strong taboos against public contention or in cases where sensitive issues are at stake. Esoteric communication is more formalized in some media environments than in others but is common in all political communications.
- **Multimedia content** analysis considers elements of content beyond the words used such as facial expressions, voice inflections of leaders giving a speeches or while being interviewed, or the reading of a script by a news broadcaster all provide indicators about the views of a subject or topic. These indicators assist to determine whether a statement was seriously considered, intended to be humorous, or simply impromptu.
- **Historical or past behavior** of open sources must be considered. Influences such as media outlet, journalist, newsmaker, or news broadcaster are factors beyond immediate control. Other issues such as time pressures, deadlines, or technical malfunctions, may also affect the content or context of public information. Analysts' judgments about source behavior must be made with careful consideration of previous behavior.

Latent Content

4-38. Latent content refers to the hidden meaning of a thought. Latent content can reveal patterns about the views and actions of the media controllers. These patterns and rules come from the unstated content that provides the underlying meaning of media content and behavior. When a pattern of content is changed, inference of a change in the viewpoint of the controller or a change in the balance of power among different controlling elements has occurred.

REPORT AND DISSEMINATE INFORMATION

4-39. Intelligence and information requirements satisfied through publicly available information and open sources should be immediately reported and disseminated in accordance with unit SOPs that are generally centered on intelligence requirements, information criticality, and information sensitivity.

> ***Note.*** Staff personnel not directly assigned to the OSINT section also acquire information that is incorporated within the running estimate of each staff element. Close cooperation between these individuals fosters a supportive environment about *what* and *how* to report information of potential operational or intelligence value through the proper channels.

4-40. Finalized OSINT serves no purpose unless it is timely, accurate, and properly disseminated to commanders and customers in a useable form. Reporting and disseminating a finalized OSINT product that satisfies intelligence and information requirements include but are not limited to—

- Single discipline or multidiscipline estimates or assessments.
- Statements of facts.
- Evaluations of threat capabilities and limitations.
- The threat's likely COAs.

REPORTING GUIDELINES AND METHODS

4-41. Effective dissemination creates a mechanism of feedback in order to assess usefulness and predict or assess future intelligence and information requirements. The objective in reporting and disseminating intelligence and information is to provide relevancy to support conducting (planning, preparing, executing, and assessing) operations.

4-42. The basic guidelines in preparing products for reporting and disseminating information are—

- **Timely.** Information should be reported to affected units without delay for the sole purpose of ensuring the correct format.
- **Relevant.** Information must contribute to the answering of intelligence requirements. Relevant information reduces collection, organization, and transmission times.
- **Complete.** Prescribed formats and SOPs ensure completeness of transmitted information.

4-43. The three reporting methods used to convey intelligence and information are—

- **Written.** Methods include formats (spot reports), tactical reports (TACREPs), or information intelligence reports (IIRs).
- **Graphic.** Web-based report dissemination is an effective technique to ensure the widest awareness of written and graphical information across echelons. OSINT personnel can collaborate and provide statuses of intelligence requirements through Web sites. Information can also be uploaded to various databases to support future open-source missions and operations.
- **Verbal and voice.** The most common way to disseminate intelligence and information verbally is through a military briefing. Based on the criticality, sensitivity, and timeliness of the information, ad hoc and impromptu verbal communication methods are the most efficient to deliver information to commanders.

SECURITY DOMAINS

4-44. OSINT is disseminated via security domains. A security domain is an application or collection of applications that share the same authentication or authorization. A security domain determines the overall classification of an enclave of servers, computers, or networks. Networks are separated by classification in order to prevent the compromise of information. OSINT organizations can exchange publicly available information on unclassified and classified networks across echelons between Army and other armed forces as well as joint organizations and federal, state, and local government agencies.

4-45. The replication of Web sites and databases from unclassified networks to classified networks ensure publicly available information, open sources, and finalized OSINT products are reported and disseminated to intelligence and nonintelligence personnel to support unified land operations. The establishment of an effective OSINT architecture involves the proper utilization of the three primary security domains:

- Joint Worldwide Intelligence Communications System (JWICS).
- SIPRNET.
- NIPRNET.

Joint Worldwide Intelligence Communications System

4-46. JWICS is a system of interconnected computer networks used by various U.S. Government departments to transmit TS/SCI over the transmission control protocol/Internet protocol (TCP/IP) suite in a secure environment. JWICS supports the synchronization of OSINT exploitation, dissemination of OSINT and supporting metadata, and collaboration between deployed and supporting intelligence personnel.

SECRET Internet Protocol Router Network

4-47. SIPRNET is a system of interconnected computer networks used by various U.S. Government departments to transmit classified information over the TCP/IP in a secure environment. SIPRNET is the principal mission-command data network at the tactical level. The network allows access to OSINT services and products through various databases, as well as gives intelligence and nonintelligence personnel the ability to collaborate, view, submit, and track OSINT intelligence and information requirements.

Nonsecure Internet Protocol Router Network

4-48. NIPRNET is used by various U.S. Government departments to exchange information up to the sensitive but unclassified level. NIPRNET is configured to provide access to Internet-based capabilities across all DOD components. It is the domain most commonly used to conduct open-source research and produce OSINT.

REPORTING AND DISSEMINATION CONSIDERATIONS

4-49. When reporting and disseminating OSINT products, considerations include but are not limited to—

- **Classification.** When creating products from raw information, write-to-release at the lowest classification level to facilitate the widest distribution of the intelligence. Use tearline report formats to facilitate the separation of classified and unclassified information for users operating on communications networks of differing security levels. 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 publicly available information and open sources in accordance with the policy and procedures in AR 380-5.
- **Feedback-mechanism development.** E-mail, postal addresses, rating systems, and survey forms are mechanisms that OSINT personnel can use in order to understand the information requirements for customers.
- **Intellectual property identification.** Identify intellectual property that an author or an organization has copyrighted, patented, or trademarked taken to preserve rights to the information. OSINT exploitation does not involve the selling, importing, or exporting of intellectual property. OSINT personnel engaging in exploitation should cite all sources used in reported and disseminated products. When uncertain, OSINT personnel should contact the supporting SJA office before reporting and disseminating a finalized OSINT product.
- **Use of existing dissemination methods, when and if possible.** Creating new dissemination methods can at times complicate existing dissemination methods.
- **Analytical pitfalls.** Analysts need to be cognizant that there are pitfalls when reporting and disseminating OSINT. The errors, referred to as fallacies (omission and assumption), are usually committed accidentally although sometimes they are deliberately used to persuade, convince, or deceive. Analysts must also be aware of hasty generalization, false cause, misuse of analogies and languages, biases (cultural, personal, organizational, cognitive), and hindsight. (For more information on analytical pitfalls, see TC 2-33.4.)

Appendix A

Legal Restrictions and Regulatory Limitations

Publicly available information and open sources cover a wide array of areas. Exploring, assessing, and collecting publicly available information and open sources has the potential to adversely affect organizations that execute OSINT missions. In some regards, OSINT missions could involve information either gathered against or delivered by U.S. persons. Given the scope of OSINT and its applicability within the intelligence community, having a firm awareness of intelligence oversight and its regulatory applications is necessary.

EXECUTIVE ORDER 12333

A-1. All OSINT exploitation conducted by intelligence and nonintelligence personnel must comply with the legal restrictions, policies, and guidelines outlined in EO 12333 and other associated regulations, instructions, or directives.

A-2. EO 12333 states the goal of the national intelligence effort is to provide the President and the National Security Council the necessary information on which to base decisions concerning the conduct and development of foreign defense, economic policy, and protection of U.S. national interests.

A-3. EO 12333 originated from operations that DOD intelligence units conducted against U.S. persons involved in the Civil Rights and anti-Vietnam War movements. DOD intelligence personnel used overt and covert means to collect information on the political positions of U.S. persons, retained the information in a nationwide database, and disseminated the information to law enforcement authorities.

A-4. The purpose of EO 12333 is to enhance human and technical collection techniques, the acquisition of foreign intelligence, and the countering of international terrorist activities conducted by foreign powers 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, and subordinate agents is essential to informed national defense decisions. Collection of such information is a priority objective, pursued in a vigorous, innovative, and responsible manner that is consistent with the U.S. Constitution and applicable laws and principles.

INTERPRETATION AND IMPLEMENTATION

A-5. AR 381-10 interprets and implements EO 12333 and DOD 5240.1-R. AR 381-10 enables the intelligence community to perform authorized intelligence functions in a manner that protects the constitutional rights of U.S. persons. The regulation does not authorize intelligence activity. An Army intelligence unit or organization must have the mission to conduct any intelligence activity directed against U.S. persons. In accordance with the Posse Comitatus Act (Section 1385, Title 18, USC), the regulation does not apply to Army intelligence units or organizations when engaged in civil disturbance or law enforcement activities without prior approval by the Secretary of Defense.

ASSIGNED FUNCTIONS

A-6. Based on EO 12333, the assigned intelligence functions of the Army are to—

- Collect, produce, and disseminate military-related foreign intelligence as required for execution of responsibility of the Secretary of Defense.
- Conduct programs and missions necessary to fulfill departmental foreign intelligence requirements.
- Conduct activities in support of DOD components outside the United States in coordination with the Central Intelligence Agency (CIA) and within the United States in coordination with the Federal Bureau of investigation (FBI) pursuant to procedures agreed upon by the Secretary of Defense and the Attorney General.
- Protect the security of DOD installations to include its activities, property, information, and employed U.S. persons by appropriate means.
- Cooperate with appropriate law enforcement agencies to protect employed U.S. persons, information, property, and facilities of any agency within the intelligence community.
- Participate with law enforcement agencies to investigate or prevent clandestine intelligence activities by foreign powers or international terrorists.
- Provide specialized equipment, technical knowledge, or assistance to U.S. persons for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies.

ARMY REGULATION 381-10

A-7. AR 381-10 enables any Army component to perform intelligence functions in a manner that protects the constitutional rights of U.S. persons. It also provides guidance on collection techniques used to obtain information for foreign intelligence and CI purposes. Intelligence activity is not authorized by this regulation.

COLLECTION OF U.S. PERSON INFORMATION

A-8. Collection, in this context, is the 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. Action must be taken to demonstrate intended use of the collected information such as producing an intelligence information report, incident report, or adding the information to an intelligence database.

A-9. There must be a link between the collection of the U.S. person information and the intelligence agency assigned mission. This link is particularly important when dealing with publicly available information, open-source information, and information data exploitation.

A-10. Army intelligence components may collect U.S. person information by lawful means but must be limited to the least intrusive means feasible and shall not violate the law (see DOD 5240.1-R). These least intrusive collection means must be attempted before utilizing more intrusive collection means such as—

- Acquisition from publicly available sources or with the consent of the U.S. person of interest.
- If proven unfeasible or inefficient, acquisition from cooperating sources.
- If proven unfeasible or inefficient, acquisition from other lawful means that do not require a warrant or Attorney General approval.
- If proven unfeasible or inefficient, an approval request for the use of techniques requiring a warrant or Attorney General approval.

A-11. Within the United States, Army intelligence components may collect foreign intelligence concerning U.S. persons by overt means when the following conditions are met:

- The foreign intelligence sought is significant and does not concern the domestic activity of the U.S. person.
- The foreign intelligence cannot be reasonably obtained by overt means.

- Collection has been coordinated with the FBI in order to prevent the disruption of current operations.

A-12. The following considerations apply to the collection of U.S. person information from the Internet:

- Army intelligence components must use government computers to access the Internet for official government business unless otherwise authorized.
- IP addresses, uniform resource locators (URLs), and e-mail addresses that are not associated with a U.S. person may be acquired, retained, and processed by Army intelligence components without making an effort to determine association with a U.S. person as long as the component does not engage in analysis focused upon specific addresses.

A-13. AR 381-10 does not authorize the collection of any information relating to a U.S. person solely because of personal lawful advocacy of measures opposed to government policy as embodied in the First Amendment to the U.S. Constitution. The First Amendment states that 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 U.S. PERSON INFORMATION

A-14. *Retention* refers only to maintaining information about U.S. 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 U.S. person information that an Army intelligence component may knowingly retain without the individual’s consent.

A-15. AR 381-10 authorizes the retention of U.S. person information under the following criteria:

- Information properly collected in accordance with AR 381-10, procedure 2.
- 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.

> ***Note.*** *Electronic surveillance* refers to 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 nonelectronic 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.

A-16. *Temporary retention* refers to the authorization for Army intelligence components to 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.

A-17. *Other information* retained by Army intelligence components must be reported for oversight purposes and for necessary subsequent proceedings.

A-18. Access to U.S. person information retained in intelligence files, databases, and repositories is limited to those with a need to know the information. U.S. 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 U.S. person information to ensure its retention is still necessary to an assigned function. This ensures U.S. 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 U.S. PERSON INFORMATION

A-19. *Disseminate*, an information management activity, refers to communicating relevant information of any kind from one person or place to another in a usable form by any means to improve understanding or to initiate or govern action (FM 6-0). In other words, dissemination is the delivery of intelligence to users in a suitable form with application of the intelligence to appropriate missions, tasks, and functions. AR 381-10, procedure 4, governs the types of information regarding U.S. persons that Army intelligence organizations may disseminate without the person's consent outside the component which collected and retained the information.

QUESTIONABLE INTELLIGENCE ACTIVITY

A-20. Questionable intelligence activity occurs when intelligence operations potentially violate—

- Laws.
- EOs.
- Presidential directives.
- DOD or Army policies.

A-21. Intelligence personnel should report questionable intelligence activity through the chain of command, the inspector general, or directly to the Assistant to the Secretary of Defense for Intelligence Oversight in accordance with AR 381-10. The following are examples of questionable intelligence activity on improper collecting, retaining, or disseminating of U.S. person information:

- Collecting and gathering information about U.S. domestic groups not connected with a foreign power or international terrorism.
- Producing and disseminating intelligence threat assessments containing U.S. person information without a clear explanation of the intelligence purpose for which the information was collected.
- Collecting and gathering U.S. person information for force protection purposes without determining if the intelligence function is authorized.
- Collecting and gathering U.S. person information from open sources without a logical connection to the mission of the unit.

A-22. AR 381-10 directs intelligence organizations to refer questions concerning the interpretation of the instructions on collection, retention, and dissemination of U.S. person information to the local SJA's office.

ASSISTANT DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE FOR OPEN SOURCE

A-23. The responsibilities of the ADDNI/OS include—

- Exercising the integration, evaluation, and oversight for the NOSE.
- Providing strategic oversight of and guides strategic involvement of OSINT.
- Chairing the National Open Source Committee (NOSC) and Open Source Board of Advisors.
- Overseeing the DNI OSC and the distributed NOSE.
- Ensuring the integration of the open-source collection management strategy.
- Developing oversight of the NOSE.
- Overseeing interagency sharing of open-source information.

INTELLIGENCE COMMUNITY

A-24. The responsibilities of the intelligence community include—

- Developing programmatic oversight and evaluation to be centralized under the ADDNI/OS.
- Supporting all intelligence disciplines.
- Establishing appropriate source and information validation and verification procedures of all open-source exploitation efforts.
- Developing metrics for overall open-source activities.
- Making all open-source information, products, and services available throughout the intelligence community.

NATIONAL OPEN-SOURCE COMMITTEE

A-25. The NOSC provides guidance to the NOSE. The responsibilities of the NOSC include—

- Developing appropriate operational standards for source or information verification, tradecraft, and training.
- Developing science and technology standards for metadata tagging and storage.

DIRECTOR OF NATIONAL INTELLIGENCE OPEN-SOURCE CENTER

A-26. The DNI OSC serves to advance the exploitation of open-source information through acquisition, procurement, analysis, and dissemination of products and services. The responsibilities of the DNI OSC include—

- Facilitating open-source exploitation for U.S. Government partners and customers.
- Securing appropriate licensing agreements for open-source customers.
- Developing open-source programs.
- Training personnel to properly exploit open-source information in accordance with security practices.

Appendix B

Cyberspace Internet Awareness

Intelligence and nonintelligence personnel conducting open-source research must be aware of the digital operational environment by minimizing and reducing cyber "footprints," practicing effective cyber OPSEC, utilizing safe online surfing techniques and habits, and understanding that embedded metadata can be contained in documents.

CYBERSPACE SITUATIONAL AWARENESS AND CYBER SECURITY

B-1. More than any other intelligence discipline, research involving publicly available information and open sources could unintentionally reveal CCIRs. Open-source research sometimes requires access to Internet Web sites that block browsing sessions originating from *.mil* or *.gov* sources. In the areas of computer information assurance and Internet security, internet awareness is needed in order to be effective, aggressive, and to successfully conduct open-source research and exploitation. Unjustified Internet Web-site restrictions have the potential to severely impede acquiring and the subsequent processing, reporting, and disseminating of publicly available information and open sources.

B-2. Awareness is the beginning of effective cyber security. Computers transmit machine specifications such as operating system, type of version of each enabled program, security levels, a history of Web sites visited, cookie information, user preferences, IP addresses, enabled languages, and referring URL when searching the Internet. Visitors are frequently redirected to alternate Web sites based on search criterion, location, language, and time the search is conducted.

B-3. The Internet is described as a "network of networks" due to the hundreds of thousands of interconnected networks consisting of millions of computers. Computers and users connected to the Internet are identified by a system-specific IP address that designates location. The IP address serves as the address where transferred information and datum is delivered. The concern therein rests in the understanding that while visiting nonstandard or questionable Internet Web sites in accordance with official duties, sensitive unit information could inadvertently be revealed.

B-4. *Cyberspace* is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, embedded processors, and controllers (JP 1-02). The Army operates in and through the cyberspace domain, using and managing the electromagnetic spectrum as a holistic and integrated part of unified land operations. Personnel engaging in OSINT exploitation need to understand the cyberspace environment in order to develop and identify outcomes-based, integration-focused, and resource-informed solutions for cyber situational awareness concerns.

B-5. *Cyber situational awareness* is the knowledge of friendly, neutral, and threat relevant information regarding activities in and through cyberspace and the electromagnetic spectrum (FM 1-02). Cyberspace and cyber security involve increasing cyber situational awareness by—

- Identifying threat operations to determine the effect on friendly operations and countermeasures.
- Determining how to use cyberspace to gain support from friendly and neutral entities.
- Determining how to gain, maintain, and exploit technical and operational advantages.

B-6. There are OPSEC and computer security risks to searching and interacting with Internet Web sites. Searching the Internet can compromise OPSEC by leaving "digital footprints" on visited Web sites. "Surfing" on Internet Web sites can compromise computer security by exposing the computer and network to malicious software (such as viruses, worms, and Trojan Horses) or unauthorized access. Intelligence personnel must be vigilant to potential threats, use only authorized hardware and software, and comply with established unit operations security measures.

B-7. URL information from the previous Web site visited is frequently an OPSEC issue and it identifies characteristics and interests of the user. While necessary for an effective research, the use of specific and focused search terms have potential OPSEC implications.

Cyber Security 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 Army General of the Army Omar N. Bradley or the U.S. Army's Bradley infantry fighting vehicle.

B-8. All actions on a Web site are logged and saved. The information is saved and linked to what is referred to as *cookie data*. User actions include but are not limited to—

- Words typed in search parameter fields.
- Drop-down menu choices.
- Check boxes.
- Web site movement patterns such as changing domain name or Web site address.

B-9. On many Web sites, information that the user provides or fills in becomes part of the Web site and is searchable. Key information to avoid sharing includes but is not limited to—

- Military plans.
- Operations.
- Exercises.
- Maps and charts.
- Locations.
- Schedules.
- Equipment vulnerabilities, capabilities, and shortfalls.
- Names and related numbers:
  - Telephone numbers.
  - Birth dates.
  - Identification numbers.

B-10. Traditional and irregular threats are disruptive in nature and use the cyberspace domain to conduct operations against the Army. These threats are innovative, networked, and technologically adept. These threats capitalize on emerging technologies to establish and maintain a cultural and social advantage leveraging areas, to include but not limited to mission command, recruiting, logistics, fund raising and laundering, IO, and propaganda.

B-11. When engaged in OSINT exploitation utilizing computer systems and Internet usage, cyberspace awareness assessments should be developed and cover areas including but not limited to network vulnerabilities, network threats (physical and virtual), and future risks.

B-12. For more detailed information about cyber security threats and tips see the U.S. Computer Security Readiness Team's Web.

Appendix C

Basic and Advanced Internet Search Techniques

The ability to search the Internet is an essential skill for open-source research and acquisition. The Internet, considered a reconnaissance and surveillance research tool, provides access to Web sites and databases that hold a wide range of information on current, planned, and potential areas of operation. The exponential growth in computer technology and the Internet has placed more publicly available information and processing power at the fingertips of Soldiers than ever before. A body of knowledge on culture, economics, geography, military affairs, and politics that was once inaccessible to some degree, now rest in the hands of high school and college students—future leaders of the Army.

THE WORLD WIDE WEB AND DEEP WEB

C-1. The Internet is a dynamic information environment consisting of stationary and moving virtual and target Web sites containing a mixture of old and new content. There are numerous virtual databases that grow at exponential rates. Keeping pace with technology is an enduring challenge for personnel that engage in OSINT exploitation utilizing the WWW and Deep Web.

WORLD WIDE WEB

C-2. The WWW is indexed by standard search engines. Standard search engines are typically incapable of accessing or retrieving the type of information necessary for conducting effective open-source research. The total amount of Internet information is estimated to be over 7,500 terabytes and continues to increase. Of this amount, customary search engines on the Internet are estimated to index only one-quarter of the information. Considered a very large amount of information, it only represents a fraction of the amount of open-source information available during research utilizing publicly available information. The other three-quarters (or roughly 5,625 terabytes) are contained on what is called the Deep Web.

THE DEEP WEB

C-3. The *Deep Web* refers to content that is not part of the traditional WWW. This content is estimated to be more than twice the content saved and accessible on the traditional WWW. The content and information contained on the Deep Web is designed around Web-based databases. Unlike the WWW, the Deep Web is not indexed. Nonstatic Web sites and databases located on the Deep Web cannot be accessed or indexed by traditional search engines. The Deep Web offers a tremendous amount of resources. Deep Web resources could fall into one or more of the following:

- **Dynamic content.** Web pages that are returned in response to a submitted query.
- **Unlinked content.** Web pages that are not linked to other Web pages that prevent standard Web crawling programs from accessing the content.
- **Private Web content.** Web pages without backlinks or inlinks.
- **Limited access content.** Web sites that limit access to information.
- **Nonhypertext markup language content.** Textual content encoded in multimedia files that are not handled by search engines.

SEARCH ENGINES

C-4. Search engines are the primary tools that personnel engaging in OSINT activities use when conducting research of publicly available information through open sources. OSINT personnel use search engines and search terms to locate text, images, and information on thousands of Web sites. Technically, search engines are actually searching through the index of Web sites. Commercial and government search engines vary in what parameters are searched, how searches are processed, and how search results are displayed. Most search engines use programs called *web crawlers* to build indexed databases. A web crawler searches Internet Web sites and files and saves the results in a database.

C-5. Most search engines use relevancy formulas to display results in a specific order with a brief description and hyperlink to the reference Internet file. Relevancy formulas evaluate how well the query matches the request. Relevancy formulas are significant to the user as search engines evolve and will not all yield similar results. The placement of keywords yield different results if rearranged due to more emphasis placed on one word over another. As search engines have evolved, some have become adept at finding specific types of information, such as statistical, financial, and news, more effectively. To overcome this specialization, software engineers have developed metasearch engines that allow the user to query more than one search engine at a time.

Search Engines

If a particular search engine cannot accommodate phrases in quotation marks or other types of Boolean functions, then the metasearch engine eliminates that function from the search. The resulting search then becomes too broad and less useful than a well-formatted search using a specialized search engine.

C-6. With an understanding of how search engines work, intelligence personnel—

- Conduct initial searches using unique keywords and combinations.
- Apply Boolean logic to improve search parameters.
- Conduct follow-on searches using natural language.

SEARCH BY KEYWORD

C-7. In keyword-based searches, OSINT personnel should consider what keywords are unique to the information being researched. Keywords should be balanced to yield relevant results without an over abundance of irrelevant information. Common words to be avoided include—

- A.
- An.
- And.
- The.

C-8. These words should be avoided in search terms unless 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, do not use *tank* as the only keyword in the search. Instead, use additional defining words such as “Russian Chinese tank sales Iraq.”

BOOLEAN LOGIC OPERATORS, CONNECTORS, AND DELIMITERS

C-9. When searching the Internet, the vast data available can be searched according to the rules of computer database searches. The logical relationship between search terms is referred to as *Boolean logic*. This method of searching provides options for constructing logical relationships among search terms using local operators, connectors, and delimiters.

C-10. Boolean logic operators, connectors, and delimiters assist intelligence personnel in establishing relationships between keywords to improve search activities.

Example of Using Boolean Logic Operators

Applying the following example, using the operators (see table C-1), the search engine searches for *Russian* and *tank* together when placed within parentheses—for example, *(Russian tank)*—and to exclude Chinese tank sales from the search result, use *(Russian tank) NOT (Chinese tank) sale Iraq* in the search. Intelligence personnel can also use a *NEAR* search when the relationship and the distance between the terms are well established. For example, if intelligence personnel are looking for incidents of tank sales in Baghdad and news articles normally place the name of the location within five words of *tank sales* in the title of the body of the article then use *tank sales NEAR/5* in the search.

Table C-1. Boolean logic operators, connectors, and delimiters

Function	*Boolean*	*Example*
Must be present *	AND	Chemical AND weapon chemical *weapon
Must not be present	NOT	Africa NOT 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)

Note. Boolean searches may not work on all search engines. Using the “Advanced Search” option is available on many web browsers. Advanced search pages include fields to fill in such as “Find web pages that contain all these words;” “this exact wording or phrase;” or “Do not show pages including any of these words.”

SEARCH IN NATURAL LANGUAGE

C-11. An alternative to using a keyword search is the *natural language* question format as most of the major search engines allow this capability. OSINT personnel obtain 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 results of the first few pages the question should be refined to initiate a new search using different parameters.

INTERNET WEB SITES

C-12. The four steps used to exploit publicly available information and open sources on Internet Web sites are—

- Plan Internet search.
- Conduct Internet search.
- Refine Internet search.
- Record results.

PLAN INTERNET SEARCH

C-13. OSINT personnel use an understanding of intelligence and information requirements to plan Internet searches. Intelligence and information requirements help to determine what information to search for, where to search, and provides the focus and initial keywords used in the search. After determining the focus and keywords, OSINT personnel use Internet browsers and search engines to connect to a previously identified Internet Web site.

Keyword Searches

If a unit is planning a humanitarian assistance operation in a particular country, intelligence requirements may be to locate refugee concentrations in that country. The task for an OSINT cell could include to locate—

- Humanitarian relief organizations operating food distribution centers.
- Population centers in the country.
- Concentrations of militia forces.
- Areas of militia operations within in the last 30 days.

Useful search terms would include—

- Refugee.
- Humanitarian relief.
- Militia.
- Water sources.
- Food distribution.

Locating possible indicators of where refugees may or may not concentrate include—

- Nongovernmental organization aid centers.
- Food.
- Water.
- Hostile militia forces.

Based on intelligence requirements, the search objective is to locate refugee concentrations based on the position of supplies and militia forces in the country.

CONDUCT INTERNET SEARCH

C-14. OSINT personnel conduct an initial search of likely sources using related terms or subject matter for the research question. The initial search is the first of potentially many subsequent searches for data and information that is retrieved and recorded in accordance with the research plan. Once retrieved, the information is integrated into the appropriate digital or analog database. OSINT personnel should avoid the temptation of using only one search engine as each has strengths and weaknesses. Organizational standards, research experience, and peer recommendations typically guide the selection of which search engine to use.

Note. If the information is not identified using multiple search engines within 30 minutes, it is possible that the information does not exist on the Internet, has not been indexed, or is not in a retrievable format.

REFINE INTERNET SEARCH

C-15. Typically, the first few pages of search results are the most relevant. Based on these pages, OSINT personnel exploit the initial search results for relevancy and accuracy for follow-on searches to determine if the results satisfied the intelligence or information requirement. Initial Internet searches can yield undesired results to satisfy intelligence and information requirements. OSINT personnel typically use measures to refine Internet results, including but not limited to—

- Reordering search terms.
- Adjusting upper or lower case.
- Searching within results.
- Searching in the cache and archive.
- Web site domains.
- Changing spelling and grammar.
- Using keyword variants.
- Searching by field.
- Truncating the URL.

Reorder Search Terms

C-16. Search engines may place a higher value on the first word or words in a multiple word or phrase search string. For example, changing the word order from *devices explosive* to *explosive devices* may yield different search results.

Change Spelling and Grammar

C-17. Search engines attempt to match the exact spelling of the words in the search string. There are search engines that recognize alternate spellings or prompt the user to correct common misspellings. For example, changing the spelling of a word from the American-English *center* to the British-English *centre* may yield different results. Boolean logic can also be used in order to circumvent potential spelling mistakes. Additionally, changing the spelling of a transliterated name generates different results that may be useful depending upon the objective of the search, such as the spelling variations of the name—

- *Al-Qaeda*.
- *al-Qaida*.
- *al-Qa'ida*.
- *el-Qaida.*
- *al Qaeda.*

Adjust Upper or Lower Case

C-18. Search engines may or may not support case sensitive searches. Some search engines attempt to match the word exactly as entered in the search. Most searches should be all lowercase letters. When looking for the name of a person, geographical location, title, or other normally capitalized word, use a case sensitive search engine. For example, changing the case of a word such as *java* to *JAVA* changes the results from coffee Web sites to software program Web sites.

Use Keyword Variants

C-19. OSINT personnel use terms that are culturally or geographically common. Using variants of a keyword such as changing *policeman* to *cop*, *bobby*, *gendarme*, *carabiniere*, *policía*, *politzei*, or other forms may improve search results.

Search Within Results

C-20. If the initial or follow-on search produces good but still unsatisfactory results, OSINT personnel can search within these results to produce a higher probability of finding the desired results. Most search engines display an option such as *search within these results* or *similar pages* to assist the user.

Search by Field

C-21. In a field search, OSINT personnel look for keywords within the URL as opposed to searching the Internet. This is typically done when the search engine returned a large number of results. While capabilities vary by search engine, some of the common field search operators are—

- **Anchor.** Searches for Web sites with a specified hyperlink.
- **Domain.** Searches for specific domains.
- **Like.** Searches for Web sites similar or related in some way to specified URLs.
- **Link.** Searches for specific hyperlinks embedded in a Web site.
- **Text.** Searches for specific text in the body of the Web site.
- **URL.** Searches for specific text in complete Web site addresses.

Search in Cache and Archive

C-22. Sometimes a search or an attempt to search with results returns a URL that matches exactly the search objective but when accessed the Web site is no longer active. If the search engine captures data as well as the URL locator, select the cached link to access the original data. OSINT personnel can also search an Internet archive Web site, such as www.archive.org, for the content. OSINT personnel need to have awareness that this information is historical and not subject to update by original creators.

Truncate the Uniform Resource Locator

C-23. Based on the topic of the information or intelligence requirement, OSINT personnel can manually search within the results by truncating the URL to a Web site. OSINT personnel work backwards from the original search result to the Web site containing the desired information or database by deleting the end segments of the URL at the forward slash. See manually truncating a URL example in table C-2.

C-24. There are also URL shortening assistance Web sites that redirect a user from a short URL (such as in the second part of table C-2) to a much longer URL serving as the actual address of the Web site. These are often used in social media services like Twitter due to the character restrictions placed on users.

Table C-2. Truncating and shortening uniform resource locators

Manually Truncating a Uniform Resource Locator (URL)	
Example URL to truncate	http://www.website.com/default.aspx?utm_source=twitter&utm_medium=social-media
Delete all but the main part of the Web site address	http://www.website.com/
Shortening URLs Using Shortening Assistance	
Example URL to paste into shortening assistance Web site	http://www.amazon.com/Kindle-Wireless-Reading-Display-Globally/dp/B003FSUDM4/ref=amb_link_353259562_2?pf_rd_m=ATVPDKIK X0DER&pf_rd_s=center-10&pf_rd_r=11EYKTN682A79T370AM3&pf_rd_t=201&pf_rd_p=1270985982&pf_rd_i=B002Y27P3M
The shortening Web site produces the example URL to use in social media settings or in e-mail	http://tinyurl.com/KindleWireless

Web Site Domains

C-25. Domain names on the Internet are identifying labels and are used in various networking contexts. They are used as simple identification labels to indicate ownership or control of a resource. With the millions of URLs on WWW, intelligence personnel are faced with a myriad of Web sites that may or may not produce or maintain the information presented in that domain. Certain domains, such as those listed in table C-3, are consistently reliable as being administered and authored by those types of organizations.

> ***Note.*** OSINT personnel exploiting publicly available information and open sources must not take *.org*, *.info*, or *.net* extensions as necessarily produced by a bona fide organization for that domain.

Table C-3. Common Web site domains

Domain	*Description*
.aero	Reserved for members of the air transport industry
.biz	Restricted to businesses
.com	Unrestricted top-level domain intended for commercial content
.coop	Reserved for cooperative associations
.edu	Reserved for postsecondary institutions accredited by an agency on the U.S. Department of Education's list of Nationally Recognized Accrediting Agencies
.gov	Reserved exclusively for the U.S. Government
.info	Unrestricted top-level domain
.int	Used only for registering organizations established by international treaties between governments
.jobs	Reserved for human resource managers
.mil	Reserved exclusively for the U.S. military
.museum	Reserved for museums
.name	Reserved for individuals
.net	Reserved for networking technological individuals
.org	Intended for noncommercial use but open to all communities
.pro	Restricted to credentialed professionals and related entities

OPEN-SOURCE DATABASES, SOFTWARE, AND TOOLS

C-26. There are numerous COTS software applications, tools, and databases that are searchable using query words for research. Search engines used for research include but are not limited to—

- **Google Scholar.** Google Scholar provides a simple way to broadly search for scholarly literature. From one place, searches expand across many disciplines and sources that include articles, theses, books, and abstracts. Google Scholar helps locate relevant work across the world of scholarly research.
- **Spokeo.** Spokeo specializes in organizing people-related information (names, addresses, phone numbers) from phone books, social networks, marketing lists, business Web sites, and other public sources. Spokeo uses algorithms to piece together data into coherent profiles.
- **Blog Pulse.** BlogPulse is an automated trend discovery system for blogs by applying machine-learning and natural language processing techniques.
- **Pipl.** Pipl query engine helps locate Deep Web pages that cannot be found on regular or standard search engines. Pipl uses advanced language-analysis and ranking algorithms to retrieve the most relevant information about an individual.
- **Monitter.** Monitter is a browser-based Twitter search engine. Monitter displays three constantly updated keyword searches parallel to each other in your browser.
- **Maltego.** Maltego is a forensic application that offers data-mining and gathering of information into packaged representations. Maltego allows the identification of key relationships between information and identify previously unknown relationships.

GOOGLE TOOLS

C-27. Google tools assist in exploiting publicly available information and open sources through—

- Query words.
- Query types.
- Query modifiers.

QUERY WORDS

C-28. Google supports several advanced Boolean logic operators, which are query words that have special meaning to Google. Typically query types and query modifiers, when applied by operators, modify the parameters and results of search engines.

QUERY TYPES

C-29. Four categories covering most Web-search queries include—

- **Cache.** If other words are included in the query, Google highlights those words within the cached document. For example, [cache:www.google.com web] shows the cached content with the word "web" highlighted.
- **Link.** The query [link:] lists Web pages that have links to the specified Web page. For example, [link:www.google.com] lists Web pages that have links pointing to the Google homepage.
- **Related.** The query [related:] lists Web pages that are similar to a specified Web page. For example, [related:www.google.com] lists Web pages that are similar to the Google homepage.
- **Info.** The query [info:] presents some information that Google has about that Web page. For example, [info:www.google.com] shows information about the Google homepage.

QUERY MODIFIERS

C-30. Research using a specific search query can be modified using the following modifiers:

- **Site.** If [site:] is included in the query, the results are restricted to those Web sites in the given domain. For example, [help site:www.google.com] finds pages about *help* within www.google.com. [help site:com] finds pages about *help* within *.com* URLs.
- **Allintitle.** If a query starts with [allintitle:], the results are restricted to those Web sites with all of the query words in the title. For example, [allintitle: google search] returns only documents that have both *google* and *search* in the title.
- **Intitle.** If [intitle:] is included in the query, the results are restricted to documents containing that word in the title. For example, [intitle:google search] returns documents that have the word *google* in their title, and have the word *search* anywhere in the document (title or not). Putting [intitle:] in front of every word in the query is equivalent to putting [allintitle:] at the front of the query: [intitle:google intitle:search] is the same as [allintitle: google search].
- **Allinurl.** If a query starts with [allinurl:], the results are restricted to those Web sites with all of the query words in the URL. For example, [allinurl: google search] returns only documents that have both *google* and *search* in the URL.
- **Inurl.** If [inurl:] is included in the query, the results are restricted to those documents containing that word in the URL. For example, [inurl:google search] returns documents that have the word *google* in their URLs, and have the word *search* anywhere in the document (URL or not). Putting "inurl:" in front of every word in the query is equivalent to putting "allinurl:" at the front of the query: [inurl:google inurl:search] is the same as [allinurl: google search].

INTERNATIONAL INTERNET WEB SITES

The number of non-English-language users on the WWW and Deep Web are increasingly surpassing English users. This international reach results in the creation of foreign Web sites with specific country codes. OSINT personnel must be aware of the origin of foreign Web sites and the potential vulnerabilities inherent in accessing these Web sites.

INTERNET SEARCH TECHNIQUE CONSIDERATIONS

C-31. When conducting Internet basic and advanced searches, technique areas that should be considered are—

- **COTS software.** When utilizing COTS tools and software, OSINT personnel must consider the tools and software utilized in accordance with unit SOPs, guidelines and policies.
- **Cataloging and archiving.** Due to the nature of Internet Web sites and the lack of control restrictions, Web sites can be removed from the WWW without prior notice.
- **Authorship.** Open-source products can oftentimes be authored through anonymity.
- **Identified Web sites and portals.** Familiarization of publicly available information generally results in standardized Web sites and portals used for research. Web sites and portals are subjective in nature due to the biases and perceptions of the Web site administrator or designer.
- **Off-line browsers.** Due to the volatile and unpredictability of Web sites, effective use of off-line browsers can enhance Internet research.

INTERNET AND OPERATIONS SECURITY VULNERABILITIES

C-32. The intent of OSINT is to exploit publicly available information and open sources without revealing user or organizational identities. Exploiting publicly available information and open sources is typically anonymous and conducted with a low risk of potential OPSEC compromise. There are inherent threats when conducting research on the WWW and Deep Web. Open-source research can compromise OPSEC and reveal user identification and the location of the computer systems through IP addresses. Any number of system disruption tools can render open-source collection activities ineffective. These include but are not limited to—

- **Viruses.** Computer codes that attach to computer programs. Once attached, viruses infect other computer systems through replication.
- **Trojan horses.** Computer programs that prevent user-activated commands.
- **Worms.** Self-contained computer programs that infect computers through replication. Worms create traffic on Web sites with the objective of decreasing visibility by conducting denial of service attacks.

Note. OSINT personnel should consult with organic unit’s S-6/G-6 and information assurance personnel for current threats and guidelines to ensure that operating systems and browsers are using the most current security patches, antivirus, and antispyware protection software.

Appendix D

OSINT Contributions

The vignettes and discussions in this appendix illustrate how integrated OSINT supports or contributes to—

- Unified land operations and associated missions and tasks.
- Other intelligence disciplines.
- Other functions, such as site exploitation (SE) and source vetting.

The examples provided do not constitute a comprehensive list.

SUPPORT TO TARGETING, COUNTERINSURGENCY, AND IMPROVISED EXPLOSIVE DEVICE DEFEAT OPERATIONS

D-1. As a result of target development, OSINT contributes to the products such as target lists, target folders, target briefs, and exploitation requirements. The following vignette describes one situation where OSINT contributes to targeting. (For more information on targeting see FM 3-60.)

Example of OSINT Contributions to Targeting

The United States is going to war against Country X. The United States has an objective to limit the counterstrike capabilities of Country X. There is a significant military stockpile that Country X purposely collocated by a religious center. Should the United States destroy the stockpile knowing there is a great chance that the symbolic religious center will be destroyed as collateral damage?

OSINT can support this objective by providing information such as—

- What is the religious background of the population living near the religious center?
- Is the religious center culturally significant?
- Is it an historical landmark?
- What is the makeup of the congregation?
- What are the normal times that people congregate?
- What are the technical descriptions of the equipment in the stockpile?

D-2. In support of counterinsurgency operations, publicly available information is valuable for understanding the operational environment. It is often more useful than any other discipline for understanding public attitudes and public support during counterinsurgency operations. Publicly available information is also an important means of determining the effectiveness of inform and influence activities among the local populace. Monitoring public media benefits counterinsurgency operations. If possible, monitoring should occur at every echelon in support of PIRs. Each echelon should monitor the media that contain information relevant to operations at that echelon. For instance, at the corps level, major news networks should be monitored; in contrast, at the tactical level, local newspapers or radio stations may be more important. (For additional information on counterinsurgency operations, see FM 3-24.)

D-3. In support of improvised explosive device (IED) defeat operations, publicly available information can be used to—

- Collect and monitor IED-related information discussed during events that are open to the public or occur in public areas.
- Collect and monitor IED-related information that is located in any recorded public document (such as newspapers, magazines, leaflets, brochures, posters).
- Collect and monitor IED-related information that is broadcast for general public consumption to all receivers or terminals within a computer, radio, or television network.
- Monitor threat or IED-related Internet Web sites that may provide indications and warning of threat intentions, capabilities, activities, and responsible entities for a specific incident.

D-4. See FM 3-90.119 for more information on combined arms IED defeat operations.

SUPPORT TO OTHER INTELLIGENCE DISCIPLINES

D-5. Publicly available information and open sources developed as finalized OSINT can also support other intelligence disciplines.

HUMAN INTELLIGENCE

D-6. OSINT supports HUMINT collection operations by providing open-source materials to the appropriate J/G/S-2X and intelligence community agencies and liaison officers. These materials include but are not limited to—

- Maps.
- Charts.
- Phone directories.
- Business directories.
- Newspapers.
- Video and audio media (including tapes and CDs).

D-7. For further information on HUMINT collector operations see FM 2-22.3.

SIGNALS INTELLIGENCE AND GEOSPATIAL INTELLIGENCE

D-8. The following vignette describes a specific situation where OSINT directly contributes to signals intelligence (SIGINT) and geospatial intelligence (GEOINT).

Example of OSINT Contributions to SIGINT

The signals officer for Unit C is preparing an assessment based on an upcoming operation. The signals officer does not have access to classified systems. Unit C is preparing to conduct operations in an area where the media is state-controlled by a totalitarian government.

OSINT can support the signals officer by providing information such as—

- The identification of locally televised channels along with supporting components and systems.
- Web sites used to communicate to the local populace.

Example of OSINT Contributions to GEOINT

During mission planning, Engineer D is observing the potential effects of building a new rail system. The rail system will bisect an agricultural community located along a primary irrigation path. There is an increased potential that the rail system will disrupt and cause damage to the irrigation canals. There are time constraints preventing the request of satellite imagery in order to provide an overhead view of the area for assessment. If the rail system damages the irrigation canals, the results will more than likely destroy relationships established between unit leadership and tribal leaders.

OSINT can support imagery intelligence (IMINT) by providing information such as Google Earth and other COTS imagery to identify alternative waterways, future irrigation draining areas, and water paths in the event of flooding.

TECHNICAL INTELLIGENCE AND COUNTERINTELLIGENCE

D-9. Publicly available information supports technical intelligence (TECHINT) efforts in significant ways. Although adversaries and potential threats attempt to closely protect capabilities and vulnerabilities as well as intent, the inevitable results of technological advances, such as the Internet and Google Earth, provide exploitation opportunities into even the most secretive nations and organizations. (For further information on TECHINT, see TC 2-22.4.)

D-10. In support of CI, publicly available information can be used to obtain information that satisfies PIRs or other standing CI collection requirements. The collectors of Army OSINT are the military intelligence brigades. Military intelligence Soldiers receive OSINT training at their schools, as applicable. Upon arrival at permanent duty stations, unit training should include OSINT training relevant to duty assignments. (For more information on CI, see FM 2-22.2.)

Appendix E

OSINT Organizations

OSINT expands the entire breath of the intelligence community from the national level to the tactical level of operations. U.S. Government organizations, such as DOD, law enforcement agencies, and others that collect, acquire, exploit, analyze, disseminate, or utilize OSINT as a customer include—

- Defense Open Source Council (DOSC).
- INSCOM.
- DA IIS.
- DNI OSC.
- Open Source Academy.
- ASD.
- FBI.
- Federal Research Division (FRD), Library of Congress.

DEFENSE OPEN SOURCE COUNCIL

E-1. The DOSC is the primary governance mechanism for DOD OSINT. It serves as a forum for the coordination and facilitation of OSINT activities and programs for all Services and combatant commands. The DOSC advices and reports to the Under Secretary of Defense for Intelligence (USD[I]) on OSINT issues and recommends initiatives to improve the effectiveness and efficiency of OSINT programs, activities, and systems of the DOD. The responsibilities of the DOSC include but are not limited to—

- The coordination of activities and the resolution of OSINT programs and activities.
- The prioritization of OSINT requirements.

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

E-2. INSCOM conducts multidiscipline and all-source intelligence operations to include collection, analysis, production, and dissemination; knowledge management for the Army intelligence enterprise; as well as delivers specialized quick reaction capabilities, advanced skills training, and linguist support for deploying forces to enable battle command to support unified land operations.

E-3. INSCOM regionally supports each of the geographic combatant commands through subordinate regionally focused multifunctional military intelligence brigades. Each brigade manages intelligence requirements (to include OSINT) and provides support to Army tactical units deploying to or operating within a unified combatant command's area of responsibility or operational environment. Each multifunctional brigade has the capability to produce OSINT, generate requests to higher agencies, and answer collection requirements submitted by subordinate units at the tactical level through OSCAR-MS.

DEPARTMENT OF THE ARMY INTELLIGENCE INFORMATION SERVICE

E-4. DA IIS provides a broad spectrum of intelligence support functions to Army and intelligence community customers. DA IIS is the primary OSINT information and dissemination proponent for the Army. DA IIS is an element of Army G-2, Intelligence Information Management Directorate (DAMI-IM) and operational control is assigned to the INSCOM G-3. DA IIS is the primary intelligence information dissemination office for the Army. DA IIS provides a broad spectrum of intelligence support functions to Army and intelligence community customers, including Army Open-Source Collections Requirements Management.

E-5. The mission of the DA IIS is to coordinate, disseminate, and validate the strategic-level requests for open-source requirements Army-wide under the direction of the Army G-2. This is done by providing information sharing services across the intelligence community. The DA IIS is a voting member of the Office of the Director of National Intelligence (ODNI) NOSC Collection Requirements Management (CRM) subcommittee. DA IIS is the Army proponent office for OSINT. As such it addresses all aspects of OSINT policy, training, operational support, collection, production, analysis, and dissemination.

DIRECTOR OF NATIONAL INTELLIGENCE OPEN SOURCE CENTER

E-6. The DNI OSC supports the NOSE as directed by the ADDNI/OS. The OSC is an organization within the intelligence community, U.S. Government, private sector, and academia.

E-7. The operations of the OSC are driven by standing open-source requirements contained in the OSC's annually reviewed and approved information collection plans. The OSC maintains a worldwide network of multilingual regional experts that respond to intelligence and information requirements using publicly available information and open sources such as 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 DOD, U.S. government agencies, and local law enforcement departments.

E-8. OSC services and tools facilitate OSINT efforts of agencies and offices throughout the U.S. Government and intelligence community by enabling the creation, management, and dissemination of unclassified products. The effectiveness and adaptability of OSC tools are—

- Highly developed for open-source exploitation and product creation.
- Designed to support and provide resources to a decentralized customer-base mainly through the Internet and readily available, purchased COTS content.
- Consistent with intelligence community security, technical, and metadata standards.

E-9. The OSC analyzes the content and behavior of media and Internet Web sites of nations and other international actors of significant policy interest to the U.S. Government.

OPEN SOURCE ACADEMY

E-10. The Open Source Academy is a leading provider of open-source tradecraft training. As intelligence consumers place a greater value on OSINT, open-source specialists throughout the U.S. Government are turning to Open Source Academy courses (see table E-1) to build open-source skills and to stay abreast of evolving OSINT technologies. The Open Source Academy is building relationships with community leaders across the intelligence community to develop a comprehensive approach to instilling open-source tradecraft skills. The academy hosts participants expanding across DOD, federal agencies, as well as local law enforcement departments.

Table E-1. Open Source Academy curriculum

• Introduction to the Field • Library Resources and Research Techniques • Media Analysis	• Visual Persuasion Methodology Advanced Googling • Audience Resonance Methodology

- Newcomer’s Basic Desktop
- Open-source Research and Analysis
- Orientation to the Open Source Center
- OS 101: Open-source Fundamentals
- OS 201: Open-source 201
- Open-source Intelligence (OSINT) and the Other Intelligences
- Overview of the Open Source Center Collection Requirements Process
- Security and Privacy Issues for Internet Users
- Smart Research—Partnering with the Library
- Temporary Duty Workshop
- Tools and Data Sources
- Classification Workshop
- Community Digital Audio Video Enterprise (DAVE) System
- Creating Multi-media Products
- DAVE Executive Overview
- Disseminations
- Essentials of Open-source Analysis
- Field Management
- Fundamentals of Open Source Center Textual Production and Operations (PROPS)
- Geospatial Analysis: An Introduction
- Hidden Universes of Information on the Internet
- High-end Workstation Block II 101
- High-end Workstation Block II 201

U.S. ARMY ASIAN STUDIES DETACHMENT

E-11. The ASD is the oldest, largest, and one of the most well-established OSINT activities in DOD that demonstrates the characteristics of sustained OSINT exploitation. The ASD collects, analyzes, exploits, processes, and reports short-to-mid-term analyses of publicly available information on military capabilities, force protection threats, and other operational-level intelligence information on countries, forces, and nonstate actors of interest in the USPACOM area of responsibility. Such requirements include the capabilities, disposition, and readiness of military forces in China, North Korea, and the Russian Far East, as well as defense-related topics throughout South and Southeast Asia. The ASD serves as a model for combatant command-level OSINT exploitation. The ASD workforce consists of Department of the Army Civilians and Army Reserve and National Guard Soldiers who serve as mission managers and editorial staff and Government of Japan-funded foreign nationals who perform all of the collection, analysis, translation, reporting, library, and graphics support functions.

E-12. The mission of the ASD is to collect, analyze, exploit, and report foreign OSINT in response to USPACOM and U.S. Army Pacific taskings and other national-level intelligence requirements. ASD’s OSINT collectors, analysts, and reporters accomplish their wide-scope mission through the exploitation of print and Internet media materials.

E-13. ASD personnel extract and compile information into analytical products answering specific taskings received via the OSCAR-MS. The ASD synthesizes and cites open-source references in open-source intelligence report format similar to research papers or essays. ASD’s current operations section provides a suite of daily media summary products containing press articles responding to more immediate and time-sensitive requirements for foreign media reflections of U.S. activities and other topics of interest. The services and tools that the ASD provide include but are not limited to—

- OSINT products responding to OSCAR-MS requirements.
- Analytical open-source intelligence reports.
- Daily force protection/situational awareness reports (FPSARs).
- Daily area surrounding Japan open-source intelligence reports (ASJORs).
- Daily situational reports (SITREPs).
- Weekly China and Taiwan Military photos reports.
- Ad hoc reporting as requested by customer in OSCAR-MS.
- OSINT product distribution on NIPRNET, SIPRNET, and JWICS.
- Map collection.
- Media summary reports.

FEDERAL BUREAU OF INVESTIGATION

E-14. The FBI is an agency of the Department of Justice that serves as both a federal criminal investigative body and an internal intelligence agency. The FBI has investigative jurisdiction over violations of more than 200 categories of federal crime.

E-15. The main missions of the FBI are to protect and defend the United States against terrorist and foreign intelligence threats and to uphold and enforce criminal laws. This is done by focusing on specific categories that include but are not limited to—

- Bank robbery.
- Robbery and extortion affecting interstate commerce.
- Drugs.
- Conspiracy.
- Sexual exploitation of minors.
- Mail fraud.
- Bank fraud.
- Fraud by wire, radio, or television.
- Illegal gambling businesses.

E-16. The FBI uses publicly available information through open sources in the areas of counterterrorism, CI, cybercrime, information technology, and forensics. Within the mission scope of the FBI, the services and tools provided include but are not limited to—

- Law enforcement bulletins.
- Crime mapping.
- Statistics (cybercrime, white-collar crime, and violent crime).

FEDERAL RESEARCH DIVISION, LIBRARY OF CONGRESS

E-17. The FRD was organized during World War II to collect and conduct research on captured aeronautical and technical reports on German and Japanese forces. These collections provided insight to future U.S. defensive posture developments and subsequently assisted in the intelligence effort leading to the defeat of the Axis powers.

E-18. The mission of the FRD is to provide directed research and analysis on domestic and international subjects to agencies of the U.S. Government, the District of Columbia, and authorized federal contractors. The FRD conducts open-source research for the U.S. Library of Congress. The services and tools that the FRD provide include but are not limited to—

- Primary research material, including document delivery.
- Foreign language abstracting and translation.
- Annotated bibliographies.
- Organizational and legislative histories.
- Studies and reports.
- Books.
- Military legal resources.
- Country studies.
- Country profiles.
- Terrorism and criminal studies and assessments.

Appendix F

Open-Source Resources

Intelligence personnel have access to vast amounts of information during research. Understanding and awareness of where to begin to look for specific information can be the largest obstacle analysts encounter. The tables in this appendix list some starting reference points for obtaining information that can be developed and produced into finalized OSINT. Table F-1 lists open-source training and resources that are specifically military.

Table F-1. Military open-source training and resources

Intelligence Knowledge Network (IKN):
IKN is a knowledge management tool that enables intelligence Soldiers worldwide to communicate, collaborate, and investigate. IKN— • Hosts discussion forums. • Serves as a single point of entry to get to U.S. Army Intelligence Center of Excellence (USAICoE) and other intelligence community Web sites. • Hosts a variety of public and private Web applications that support the intelligence community.
University of Military Intelligence (UMI):
UMI is the distance learning arm of the military intelligence schoolhouse. From the UMI Web site, military intelligence professionals can access— • Self-paced and reachback training. • The Cultural, Foreign Language Integration Center. • Military intelligence training resources.
Army Knowledge Online (AKO) Intelligence:
AKO Intelligence features— • The Intelligence Collaboration Center. • Knowledge Center (documents, FMs, TCs, ATTPs, and others). • Training, agencies, policy, doctrine, and links to other intelligence-related Web sites.
AKO Open-Source Program:
AKO Army Open-Source Program features Open-Source— • Events. • Discussion forums. • Links of interest. • Intelligence products. • Handbooks.
Military Intelligence Library: ***Available via the IKN and Warfighter Forum homepage***
Military Intelligence Library Reference Center includes many databases and resources, such as— • Journals and magazines. • Forms and publications. • Resource guide. • Historical documents. • Cultural field readings. • Military Intelligence Foreign Language Training Center (MIFLTC).

Table F-1. Military open-source training and resources (continued)

DA IIS Country Research Portal: ***Available via the DA IIS portal from the AKO homepage***
The Department of the Army Intelligence Information Service (DA IIS) Country Research portal has road-mapped and data-mined networks resulting in a one-stop-shop for intelligence information. Some of the links on this Web site include— • Open-source documents such as Early Bird, Terrorism Daily Update, Baghdad Mosquito, Basra Bugle, and others. • Intelligence community. • Analyst references. • Combatant commands. • Foundry program. ***Note.*** Data is accessible through multiple networks to ensure that intelligence consumers have all required information necessary for mission success.
Intelink-U:
Intelink-U is the designated network of the Department of National Intelligence (DNI) for intelligence collaboration. The Intelink-U is— • Managed by the Intelink Management Office. • A joint-use, remotely accessed, and operationally-implemented information service that is used to access and process unclassified, publicly accessible information only. • Provides a protected environment to exchange authorized unclassified, unclassified for official use only, and sensitive but unclassified information among personnel of the DOD. ***Note.*** Access to Intelink-U services is implemented through multiple virtual private networks.
Joint Military Intelligence Training Center:
Armies of the World
Armed Forces of the World ***Note.*** Requires account log in to access the page. Combined Arms Research Library
Center for Army Lessons Learned (CALL)
CALL
Military Operations in Urban Terrain (MOUT)
MOUT
Military Service Intelligence Organizations
U.S. Army Intelligence and Security Command (INSCOM) Office of Naval Intelligence Air Force Intelligence, Surveillance, and Reconnaissance (ISR) Agency Marine Corps Intelligence Activity
Unified Command Intelligence Organizations
U.S. Central Command U.S. European Command U.S. Pacific Command U.S. Southern Command U.S. Africa Command U.S. Air Force Space Command U.S. Special Operations Command U.S. Strategic Command U.S. Transportation Command

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

2X	human intelligence and counterintelligence staff element
ADDNI/OS	assistant deputy to the Director of National Intelligence for Open-source
AM	amplitude modulation
AO	area of operations
AR	Army regulation
ART	Army tactical tasks
ATP	Army techniques publication
ATTP	Army tactics, techniques, and procedures
BCT	brigade combat team
CCIR	commander's critical information requirement
CI	counterintelligence
CIA	Central Intelligence Agency
COA	course of action
CONUS	continental United States
COTS	commercial-off-the-shelf
CRM	collection requirements management
DA	Department of the Army
DA IIS	Department of the Army Intelligence Information Service
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOSC	Defense Open Source Council
DVD	digital video device
EO	executive order
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FFIR	friendly force information requirement
FM	field manual
FMI	field manual interim
FRD	Federal Research Division
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal

G-7	assistant chief of staff, inform and influence activities
G-9	assistant chief of staff, civil affairs operations
GEOINT	geospatial intelligence
HVT	high-value target
ICD	intelligence community directive
IED	improvised explosive device
IIR	intelligence information report
ILR	Interagency Language Roundtable
INSCOM	United States Army Intelligence and Security Command
IO	information operations
IP	Internet protocol
IPB	intelligence preparation of the battlefield
ISP	Internet service provider
JP	joint publication
JWICS	Joint Worldwide Intelligence Communcations System
MDMP	military decisionmaking process
METT-TC	mission, threat, terrain and weather, troops and support available, time available, and civil considerations (mission variables)
MFLT	machine foreign language translation
mm	millimeter
NIPRNET	Nonsecure Internet Protocol Router Network
NOSC	National Open Source Committee
NOSE	National Open Source Enterprise
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OPSEC	operations security
OSC	Open Source Center
OSCAR-MS	open-source collection acquisition requirement management system
OSINT	open-source intelligence
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time (operational variables)
S-2	intelligence staff officer
S-3	operations staff officer
S-6	signal staff officer
S-7	inform and influence activities staff officer
S-9	civil affairs operations staff officer
SCI	sensitive compartmented information
SIPRNET	SECRET Internet Protocol Router Network
SOP	standard operating procedure
TCP/IP	transmission control protocol/Internet protocol

TTP	tactics, techniques, and procedures
URL	uniform resource locator
U.S.	United States
USC	United States Code
WWW	World Wide Web

SECTION II – TERMS

esoteric communications

Public statements whose surface meaning (manifest content) does not reveal the real purpose, meaning, or significance (latent content) of the author.

media source analysis

The systematic comparison of the content, behavior, patterns, and trends of organic media organizations and sources of a country.

open source

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

open-source intelligence

The discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (FM 2-0)

private information

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

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.

References

REQUIRED PUBLICATIONS

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

FM 1-02. *Operational Terms and Graphics.* 21 September 2004.

RELATED PUBLICATIONS

These sources contain relevant supplemental information.

AR 11-6. *Army Foreign Language Program*. 31 August 2009.

AR 25-400-2. *The Army Records Information Management System (ARIMS).* 2 October 2007.

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

AR 190-13. *The Army Physical Security Program*. 25 February 2011.

AR 380-5. *Department of the Army Information Security Program*. 29 September 2000.

AR 380-67. *Department of the Army Personnel Security Program*. 9 September 1988.

AR 381-10. *U.S. Army Intelligence Activities*. 3 May 2007.

AR 530-1. *Operations Security (OPSEC).* 19 April 2007.

ATTP 2-91.6. *Tactics, Techniques, and Procedures for Intelligence Support to Site Exploitation.* 27 December 2010.

Carnegie Mellon Software Engineering Institute.

Chatham House.

Department of the Army Intelligence Information Services.

DOD 5240.1-R. *DoD Intelligence Activities.* 1 December 1982.

DODD 5100.20. *National Security Agency/Central Security Service (NSA/CSS).* 26 January 2010.

DODD 3115.12. *Open Source Intelligence (OSINT).* 24 August 2010.

EO 12333. *United States Intelligence Activities.* 4 December 1981.

FM 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace.* 15 October 2009.

FM 2-19.4. *Brigade Combat Team Intelligence Operations*. 25 November 2008.

FM 2-22.2. *Counterintelligence.* 21 October 2010.

FM 2-22.3. *Human Intelligence Collector Operations*. 6 September 2006.

FM 3-24. *Counterinsurgency*. 15 December 2006.

FM 3-55. *Information Collection*. 14 December 2011.

FM 3-60. *The Targeting Process.* 26 November 2010.

FM 3-90.119. *Combined Arms Improvised Explosive Device Defeat Operations.* 21 September 2007.

FM 5-0. *The Operations Process*. 26 March 2010.

FM 6-0. *Mission Command.* 13 September 2011.

FM 7-0. *Training Units and Developing Leaders for Full Spectrum Operations*. 23 February 2011.

FM 7-15. *The Army Universal Task List.* 27 February 2009.

JP 1-02. *Department of Defense Dictionary of Associated Terms*. 8 November 2010.

JP 2-0. *Joint Intelligence.* 22 June 2007.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 7 October 2004.

JP 3-0. *Joint Operations.* 17 September 2006.

JP 3-35. *Deployment and Redeployment Operations*. 7 May 2007.

JP 3-59. *Meteorological and Oceanic Operations*. 24 September 2008.

JP 3-60. *Joint Targeting*. 13 April 2007.

JP 4-0. *Joint Logistics.* 18 July 2008.

JP 5-0. *Doctrine for Planning Joint Operations*. 20 January 2005.

Lanicci, John M. "Integrating Weather Exploitation into Air and Space Power Doctrine." *Air Power 12, No. 2*. Summer 1998: 52-63.

Library of Congress, Federal Research Division.

Open Source Center.

TC 2-22.4. *Technical Intelligence.* 19 November 2009.

TC 2-33.4. *Intelligence Analysis*. 1 July 2009.

TC 2-91.8. *Document and Media Exploitation.* 6 August 2010.

U.S. Computer Security Readiness Team.

Title 17 USC. *Copyrights*.

Title 18 USC. *Crimes and Criminal Procedure*.

PRESCRIBED FORMS

None.

REFERENCED FORMS

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

Index

Entries are by paragraph number.

Entries are by paragraph number.

ATP 2-22.9
10 July 2012

By order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

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

DISTRIBUTION:

Unlimited Distribution; Not to be distributed; electronic media only.