DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FREEDOM OF INFORMATION/PRIVACY OFFICE
FORT GEORGE G. MEADE, MARYLAND 20755-5995

Freedom of Information/
Privacy Office

NOV 18 2019

Mr. Steven Aftergood
Federation of American Scientists
1725 DeSales Street NW, Suite 600
Washington, DC 20036

Dear Mr. Aftergood:

This is in reponse to your Freedom of Information Act (FOIA) request of July 5, 2017, to the U.S. Army Installation Management Command (IMCOM), United States Army Garrison, Fort Huachuca, for copies of ATP 2-22.9, Open-Source Intelligence, Intelligence Center of Excellence (Huachuca), 30 June 2017. On January 8, 2019, IMCOM forwarded your request and records to the U.S. Army Training and Doctrine Command (TRADOC). On November 5, 2019, TRADOC forwarded your request and records to this office and they were received on November 6, 2019.

Coordination with another element of our command has been completed and records have been returned to this office for final disposition and direct reply to you. The records have been determined to be partially releasable and are enclosed.

Information has been sanitized that would result in an unwarranted invasion of the privacy rights of the individuals concerned. This information is exempt from the public disclosure provisions of the FOIA per Title 5 U.S. Code 552 (b)(6).

Information also has been withheld pursuant to Title 5 U.S.C. 552(b)(3) of the FOIA. Exemption (b)(3) pertains to information that is exempt by statute. The applicable statute is 50 U.S.C. § 3024(i), which protects intelligence sources and methods.

The withholding of the information described above is a partial denial of your request. This denial is made on behalf of Major General Gary W. Johnston, Commanding, U.S. Army Intelligence and Security Command, who is the Initial Denial Authority for Army intelligence investigative and security records under the FOIA. You have the right to appeal this decision to the Secretary of the Army. Your appeal must be postmarked no later than 90 calendar days from the date of this letter. After the 90-day period, the case may be considered closed; however, such closure does not preclude you from filing litigation in the courts. You should state the basis of your disagreement with the response and provide justification for a reconsideration of the denial. An appeal may not serve as a request for additional or new information. An appeal may only address information denied in this response. Your appeal is to be made to this office, for forwarding, as appropriate to the Secretary of the Army, Office of the General Counsel.

There are no assessable FOIA fees.

If you have any questions regarding this action, feel free to contact this office at 1-866-548-5651, or email the INSCOM FOIA office at: usarmy.meade.902-mi-grp.mbx.inscom-foia-service-center@mail.mil and refer to case #0065F-20. Please note that you now have the ability to check the status of your request online via the U.S. Army Records Management and Declassification Agency (RMDA) website: https://www.foia.army.mil/FACTS/CaseStatus.aspx. Please refer to FOIA Control Number: FP-20-003201. You may also contact the INSCOM FOIA Public Liaison, Mrs. Joanne Benear, for any further assistance and to discuss any aspect of your request at 301-677-7856. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; email at ogis@nara.gov; telephone at 202-741-5770; toll tree at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,

Michael T. Heaton
Director
Freedom of Information/Privacy Office
Investigative Records Repository

Enclosure

ATP 2-22.9
MCRP 2-10A.3

Open-Source Intelligence (U)

JUNE 2017

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies only because it requires protection in accordance with AR 380-5, AR 530-1, and U.S. Army Directive 2016-37, 22 November 2016. This determination was made on 10 February 2017. Contractor and other requests must be referred to ATTN: ATZS-CDI-D, U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ 85613-7017, or via e-mail at usarmy.huachuca.icoe.mbx.doctrine@mail.mil. Requests to release this document to foreign entities must be referred to the requestor's supporting foreign disclosure office.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document in accordance with AR 380-5.

This publication supersedes ATP 2-22.9 dated 10 July 2012.

Headquarters, Department of the Army
Headquarters, United States Marine Corps

~~**FOR OFFICIAL USE ONLY**~~

(U) This publication is available at the Army Publishing Directorate site (http://www.apd.army.mil), and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

(U) *This publication is available at the U.S. Marine Corps Doctrine website (https://doctrine.usmc.mil).*

***ATP 2-22.9**
MCRP 2-10A.3

Army Techniques Publication
No. 2-22.9
Marine Corps Reference Publication
No. 2-10A.3

Headquarters
Department of the Army
Washington, DC

Headquarters
United States Marine Corps
Deputy Commandant
Combat Development &
Integration Quantico, Virginia

30 June 2017

Open-Source Intelligence (U)

Contents (U)

DISTRIBUTION RESTRICTION: Distribution authorized to U.S. Government agencies only because it requires protection in accordance with AR 380-5, AR 530-1, and U.S. Army Directive 2016-37, 22 November 2016. This determination was made on 10 February 2017. Contractor and other requests must be referred to ATTN: ATZS-CDI-D, U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ 85613-7017, or via e-mail at usarmy.huachuca.icoe.mbx.doctrine@mail.mil. Requests to release this document to foreign entities must be referred to the requestor's supporting foreign disclosure office.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document in accordance with AR 380-5.

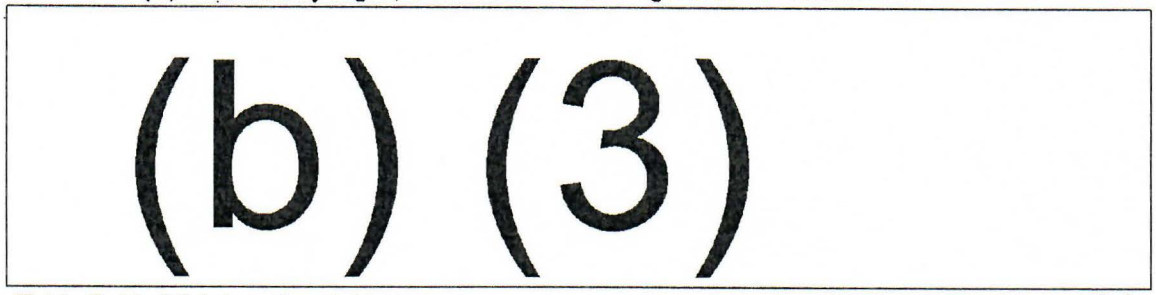
*This publication supersedes ATP 2-22.9 dated 10 July 2012.

~~FOR OFFICIAL USE ONLY~~

3

Figures (U)

Tables (U)



~~FOR OFFICIAL USE ONLY~~

This page intentionally left blank.

Preface (U)

(U) ATP 2-22.9/*MCRP 2-10A.3* establishes a common framework, foundational concepts, and methods of use for Army and *Marine Corps* open-source intelligence (OSINT) activities. It highlights the fundamentals of OSINT as an intelligence discipline and discusses the role it plays in the intelligence process. This publication addresses only open-source information.

(U) ATP 2-22.9/*MCRP 2-10A.3*—

- Establishes a common foundation for understanding OSINT.
- Provides fundamental principles and terminology for Army elements and *Marine Corps organizations* conducting OSINT activities.
- Emphasizes the value of open-source information.
- Describes systematic approaches to plan, prepare, collect, and produce intelligence from open-source information.

(U) The principal audience for ATP 2-22.9/*MCRP 2-10A.3* is—

- Army or *Marine Corps* intelligence staffs at battalion, brigade/*Marine air-ground task force*, division, corps, and theater army/*Marine expeditionary force* that collect open-source information or use OSINT to aid intelligence analysis or support the military decision-making process/*Marine Corps planning process*.
- Army intelligence personnel (military, civilians, and contractors) assigned, attached, detailed to, or supporting Army intelligence organizations, units, or elements with an authorized OSINT mission.
- Army intelligence elements or *Marine Corps organizations* conducting OSINT activities.
- Strategic, operational, and tactical commanders who require OSINT to address specific intelligence requirements to support planning and operations.

(b) (3)

(U) **Cyberspace** is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 3-12[R]).

(U) Commanders and staffs of Army/*Marine Corps* headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army/*Marine Corps* also use this publication.

(U) Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States (U.S.), international, and, in some cases, host-nation laws and regulations. Commanders at all levels must ensure their Soldiers/*Marines* operate in accordance with the law of war and the rules of engagement. (See FM 27-10.)

~~FOR OFFICIAL USE ONLY~~

(U) ATP 2-22.9/*MCRP 2-10A.3* uses joint terms where applicable. Selected joint, Army, and *Marine Corps* terms and definitions appear in both the glossary and the text. This publication is not the proponent for any Army/*Marine Corps* terms. (See the page vii for style conventions used to identify terms in this publication.)

(U) The use or mention of the name of any commercial or private organization or its associated trademark or services by the Army/*Marine Corps* does not express or imply an endorsement of the sponsor or its products and services by the Army/*Marine Corps*.

(U) ATP 2-22.9/*MCRP 2-10A.3* applies to the Active Army and *Marine Corps*, the Army National Guard/Army National Guard of the United States, the U.S. Army Reserve, and the *U.S. Marine Corps Reserve*, unless otherwise stated.

(U) The proponent of ATP 2-22.9/*MCRP 2-10A.3* is the U.S. Army Intelligence Center of Excellence. The preparing agency is the Capabilities Development and Integration Directorate, U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ. Send comments and recommendations on a DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, U.S. Army Intelligence Center of Excellence, ATTN: ATZS-CDI-D (ATP 2-22.9), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017; by e-mail to usarmy.huachuca.icoe.mbx.doctrine@mail.mil; or submit an electronic DA Form 2028.

(U) U.S. Marine Corps readers of this publication are encouraged to submit suggestions and changes through the Universal Need Statement (UNS) process. The UNS submission process is delineated in MCO 3900.20, which can be obtained from the Marine Corps Publications Electronic Library online.

(U) The UNS recommendation should include the following information:

- *Location of change.*
- *Publication number and title.*
- *Current page number.*
- *Paragraph number (if applicable).*
- *Line number.*
- *Figure or table number (if applicable).*
- *Nature of change.*
- *Addition or deletion of text.*
- *Proposed new text.*

~~FOR OFFICIAL USE ONLY~~

Introduction (U)

OPEN-SOURCE INTELLIGENCE AND CURRENT OPERATIONS (U)

(U) Circumstances have never been more favorable for using open-source information in developing intelligence to support operations. OSINT activities offer the following advantages:

- Least intrusive.
- Cost-effective.
- Abundant sources of data and information.

(U) The increasing volume of potentially detailed information worldwide on the internet provides compelling reasons to use open-source information to defend the Nation. Despite the recent recognition of OSINT as an intelligence discipline, OSINT is arguably one of the oldest forms of intelligence. Before the advent of satellites and other advanced technological means of collecting information, military professionals developed intelligence from open-source information to gain knowledge and understanding of foreign lands, peoples, potential threats, and armies. However, the world is reinventing itself on the internet, posting unprecedented amounts of information that become immediately available to the public. New techniques, technologies, data sources, and emerging practices to develop OSINT products evolve at a substantial rate to meet the growth of open-source information worldwide. ATP 2-22.9/*MCRP 2-10A.3* explains OSINT fundamentals, and how to organize for and conduct OSINT assets while leveraging joint force and Department of Defense (DOD) enterprise capabilities.

(U) OSINT may only be conducted by intelligence professionals due to the authorities and restrictions placed upon intelligence personnel in Executive Order 12333 as amended, DODM 5240.01, DOD 5240.1-R, AR 381-10, and *MCO 3800.2B*. Commanders must ensure the activities of other warfighting domains operating in the cyberspace environment are de-conflicted with intelligence operations, and intelligence collection activities are levied on intelligence elements.

(U) Further, for the Army, the Deputy Chief of Staff, G-2; the Commander, U.S. Army Intelligence and Security Command (INSCOM); the Commanders of Army Commands and Army Service Component Commands; and the Commander, 650th Military Intelligence Group or their designees may grant, in writing, to assigned, attached, aligned, or detailed Army intelligence organizations, units, or elements the authority to conduct OSINT activities to support their intelligence missions.

Note. (U) Intelligence officers have a responsibility to advise the commander on the best ethical use of OSINT.

(U) Open sources possess much of the information needed to understand the physical and human factors of an operational environment. Many information and intelligence requirements can be satisfied with open-source information. Open-source information may increase situational awareness and can provide confirmation of information obtained through non-OSINT-related technical or classified resources.

(U) Access to the massive amounts of open-source information, including publically available information, is reshaping how people perceive the world. People can use open-source information to pursue a broad spectrum of objectives. The significance and relevance of OSINT provides an additional leverage capability and can cue technical or classified assets to refine and validate both information and intelligence.

~~FOR OFFICIAL USE ONLY~~

OVERSIGHT OF OPEN-SOURCE INTELLIGENCE (U)

(U) Only intelligence personnel perform the collection and exploitation of open-source information for the purposes of answering intelligence requirements. This publication applies to the military intelligence/*Marine Corps intelligence, surveillance, and reconnaissance enterprise* use of open-source information; it does not address the use of open-source information by other branches and specialties. Activities conducted by others (such as information operations, civil affairs, cyberspace operations, law enforcement, operations staff planners, security) fall under the purview of their respective centers of excellence or *Marine Corps commands*. Nonetheless, all warfighting functions are subject to restrictions on the collection and storage of non-DOD-affiliated U.S. person information. Although intelligence is the only warfighting function subject to intelligence oversight, all warfighting functions are required to comply with law.

Note. (U) Collection of information on U.S. persons is regulated by law and regulation. (See appendix A.)

STYLE CONVENTIONS (U)

(U) "OSINT practitioners" indicate intelligence personnel in the Active Army and *Marine Corps*, the Army National Guard/Army National Guard of the United States, U.S. Army Reserve, the *U.S. Marine Corps Reserve*, the Army Civilian Corps, *Civil Marines*, and contracted intelligence analysts who engage in authorized missions involving open-source information.

(U) In doctrinal publications, the normal convention for identifying terms is through the use of italics. Since this is a dual-designated Army and *Marine Corps* publication, the following protocol is used to distinguish proponency (authority) for information and terms:

- Terms in bold italics and phrasing in italics—Marine Corps.
- Terms in bold and definitions in plain text—joint and Army terms with the proponent publications in parentheses.

SUMMARY OF CHANGES (U)

(U) ATP 2-22.9/*MCRP 2-10A.3* updates the following Army/*Marine Corps* doctrine on OSINT:

- Chapter 1—
  - Incorporates the definition of OSINT established by Public Law 109-163.
  - Adds the definitions of open-source information, publicly available information, and collection.
- Chapter 2 provides information concerning organizations that conduct OSINT.
- Chapters 3 through 6 are reorganized to follow the construct of the intelligence process.
- Appendix A provides legal guidance on the collection of open-source information and OSINT.
- Appendix B provides information on security awareness.
- Appendix C provides a discussion on internet research techniques.
- Appendix D provides a list of open-source resources.

~~FOR OFFICIAL USE ONLY~~

PART ONE

Fundamentals (U)

(U) The passage of legislation has affected the United States (U.S.) intelligence community and its application of open-source information. The National Security Act of 1992 began the reformation of the U.S. intelligence community. This resulted in the establishment of the Open-Source Office in 1992, the Director of National Intelligence Open Source Center in 2005, and the Open Source Enterprise in 2015. Part one describes the fundamentals of open-source intelligence (OSINT).

Chapter 1

Open-Source Intelligence (OSINT) Overview (U)

(U) Chapter 1 discusses the role, characteristics, considerations, and employment of OSINT. OSINT is a discipline within the intelligence warfighting function; as such, it provides timely, relevant, accurate, predictive, and tailored intelligence that focuses missions and operations. OSINT involves the collection, analysis, evaluation, synthesis, and processing, exploitation, and dissemination (PED) of information to answer intelligence requirements.

Note. (U) This publication applies to the collection, exploitation, and analysis of open-source information, including publicly available information (PAI), for the purposes of answering intelligence requirements. Only intelligence personnel perform this task. Only intelligence professionals may conduct OSINT activities due to the authorities and restrictions placed upon them in Executive Order (EO) 12333 as amended, DODM 5240.01, DOD 5240.1-R, DODI 3115.12, JP 2-0, AR 381-10, and *MCO 3800.2B*. This publication does not apply to any of the other warfighting functions.

DEFINING OSINT (U)

1-1. (U) The definitions in this section are important in any open-source activity. They assist leaders and practitioners in understanding open-source activities and the authorities under which intelligence components conduct these activities.

1-2. (U) **Open-source intelligence** is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement (Public Law 109-163). The term also applies to the activity itself. OSINT activities are integral to the intelligence warfighting function (see ADRP 2-0 and *MCDP 2*) and are conducted using the PED process, contributing to all-source analysis, tipping and cueing from other intelligence activities, and support to targeting activities.

~~FOR OFFICIAL USE ONLY~~

1-3. (U) The intelligence resulting from open sources is produced by intelligence professionals, incorporating tips and cues from other disciplines, and is integrated into all-source analysis. The following terms are fundamental to understanding OSINT:

- **Open-source information:** Information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access (JP 2-0).
- **Publicly available information:** Information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public (DODM 5240.01).
- **Collection:** Information is collected when it is received by a Defense Intelligence Component, whether or not it is retained by the Component for intelligence purposes or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the Component. Collected information does not include: information that only momentarily passes through a computer system of the Component; information on the internet or in an electronic forum or repository outside the Component that is simply viewed or accessed by a Component employee but is not copied, saved, supplemented, or used in some manner; information disseminated by other Components or elements of the Intelligence Community; or information that is maintained on behalf of another U.S. Government agency and to which the Component does not have access for intelligence purposes (DODM 5240.01).

1-4. (U) OSINT production contributes to all-source intelligence and the continuing activities of the intelligence process (analyze and assess), as described in ADRP 2-0 and *MCDP 2*. Like other intelligence disciplines, OSINT is developed based on intelligence requirements and can be used to cue or support other intelligence disciplines.

OPERATIONS SECURITY AND PUBLICLY AVAILABLE INFORMATION (U)

1-5. (U) When using open-source information, operations security (OPSEC) is a major concern. Denying the adversary clues to the Nation's plans and interests are of the upmost importance. (See chapter 3 and appendix B for more information on OPSEC.)

1-6. (U) PAI comes from many different venues such as broadcasting, publishing, and the internet. When accessing these venues, the user must practice good OPSEC procedures and obtain the information in the least intrusive way. With leaks of classified information to the internet, users must know that some open-source information has not been downgraded and collection may cause data spillage on a Department of Defense (DOD) Nonsecure Internet Protocol Router Network (NIPRNET) system.

OSINT CHARACTERISTICS (U)

1-7. (U) The following characteristics frame the role of OSINT in Army and *Marine Corps* operations:

- **OSINT provides the foundation.** Open-source information provides foundation information and real-time ongoing information updates to assist in developing and enhancing intelligence products and the intelligence disciplines. There is much information about the political, military, economic, social, and infrastructure of a region or local area obtainable from open-source information and readily changed to OSINT products. This foundation information and intelligence products can be essential to generating a clear picture for the commander. The variety of foundational websites associated with social structures, education systems, and news services provides a foundational perspective for intelligence knowledge.

~~FOR OFFICIAL USE ONLY~~

- **OSINT addresses requirements.** The availability, depth, and range of open-source information enable intelligence professionals to satisfy many priority intelligence requirements (PIRs) and information requirements without using specialized human or technical collection means.
- **OSINT enhances collection.** Open-source information supports other requirements and provides information that optimizes the employment and performance of sensitive human and technical collection means. Examples of this type of information include biographies, cultural information, geospatial information, and technical data.
- **OSINT enhances production.** As part of single-source and all-source intelligence production, the use and integration of OSINT ensure commanders have the benefit of all sources of available information.

1-8. (U) OSINT supports the development and refinement of the collection plan to satisfy intelligence requirements, and may quickly fill information gaps to optimize the use of low-density collection assets. OSINT supports situational understanding by-

- Developing an understanding of complex situations by integrating intelligence and operations.
- Supporting fused all-source analysis.
- Providing tips and cues from other intelligence activities.
- Supporting intelligence operations and activities in other intelligence disciplines.

THE INTELLIGENCE WARFIGHTING FUNCTION (U)

1-9. (U) **Intelligence warfighting function** is the related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment (ADRP 3-0). **Intelligence** is 1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities (JP 2-0). *The Marine Corps amplifies the JP 2-0 definition. **Intelligence** is knowledge about the enemy or the surrounding environment needed to support decision making. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. Intelligence is one of the six warfighting functions (MCRP 1-10.2).*

1-10. (U) The intelligence warfighting function includes understanding threats (enemies and adversaries) and weather. It synchronizes information collection with the Army tactical tasks of reconnaissance, surveillance, security, and intelligence operations. Intelligence is driven by commanders-it is more than just collection. Developing intelligence is a continuous process that involves analyzing information from all sources and conducting operations to develop the situation. (See ADRP 2-0 and *MCDP 2* for fundamental intelligence doctrine. See FM 2-0 for doctrine on intelligence operations. See ADRP 3-90, FM 3-90-2, and *MCRP 2-10A.8* for doctrine on reconnaissance and security. See FM 3-55 and *MCRP 2-10A.8* for doctrine on surveillance.)

1-11. (U) The intelligence warfighting function facilitates support to the commander and staff through a broad range of Army tactical tasks. (See ADRP 1-03 and *MCO 3500.26A*.) The Army intelligence warfighting function tasks include-

- Provide intelligence support to force generation.
- Provide intelligence support to situational understanding.
- Conduct information collection.
- Provide intelligence support to targeting and information capabilities.

~~FOR OFFICIAL USE ONLY~~

1-12. *(U) The Marine Corps intelligence functional tasks per MCO 3500.26A include—*

- *Provide support to the commander's estimate.*
- *Provide intelligence to develop the situation.*
- *Provide indications and warning of threat.*
- *Provide intelligence support to force protection.*
- *Provide intelligence support to targeting.*
- *Provide intelligence support to combat assessment.*

1-13. (U) The intelligence warfighting function receives information from a wide variety of sources. OSINT, as an intelligence discipline, is produced from open-source information. PAI can be used to—

- Support situational understanding of the threat and operational environment.
- Develop intelligence about the enemy, terrain, weather, and civil considerations.
- Generate intelligence knowledge before receipt of mission to provide relevant knowledge of the operational environment.
- Contribute to satisfying intelligence requirements.
- Develop a baseline of knowledge and understanding about potential threat actions or intentions to support answering ongoing intelligence requirements.
- Generate intelligence products as the basis for Army/*Marine Corps* integrating functions such as intelligence preparation of the battlefield/*battlespace* (IPB). IPB is designed to support running estimates and the military decision-making process (MDMP)/*Marine Corps planning process (MCPP)*. Many intelligence requirements are generated because of IPB and its interrelation with the MDMP/*MCPP*.
- 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 area of operations before and during operations. (See ADRP 1-03.) Situation development-
  - Assists the intelligence staff in determining threat intentions and objectives.
  - Assists in confirming or denying courses of action (COAs).
  - Provides an estimate of threat combat effectiveness.
- Support plan requirements and assess collection by contributing to the analysis of information requirements, the identification of intelligence gaps, and the determination of assets to satisfy the requirements. (See ATP 2-01 and *MCTP 2-10A*.)

OSINT WITHIN THE INTELLIGENCE ENTERPRISE (U)

1-14. (U) The intelligence enterprise is the sum of the intelligence efforts of the U.S. intelligence community. (See ADRP 2-0 and *MCDP 2*.) The intelligence warfighting function is the Army's contribution to the intelligence enterprise. The intelligence enterprise comprises all U.S. intelligence professionals, sensors, systems, federated organizations, information, and processes supported by a network-enabled architecture. The most important element of the intelligence enterprise is the people who make it work.

1-15. (U) OSINT contributes to the intelligence enterprise by providing information of intelligence value that answers or assists in answering intelligence requirements. Members of the OSINT regional communities of interest may provide support through intelligence reach, granting access, and information sharing.

INTELLIGENCE REACH (U)

1-16. (U) **Intelligence reach** is the activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command (ADRP 2-0). Units should understand all available intelligence reach options before deployment. (See figure 1-1/*figure 1-2 on page 1-6*.) They can coordinate this through supporting regionally aligned military intelligence (MI) brigades (theater)/*Marine air-ground task force*

~~FOR OFFICIAL USE ONLY~~

(MAGTF) intelligence centers (MICs) or combatant commands. The following includes other sources of information:

- Supporting and supported combatant commands' joint intelligence operations centers.
- Theater army/*Marine expeditionary force (known as MEF)* intelligence staffs.
- National Ground Intelligence Center or the *Marine Corps Intelligence Activity (MCIA)*.
- Other intelligence community members described in chapter 2.

Note. (U) Higher echelon units that provide reach support should maintain an understanding of those units moving into and out of the supported combatant command's area of responsibility, and engage them, as necessary, to provide OSINT reach support.

1-17. (U) Figure 1-1 illustrates intelligence reach relationships among regional communities of interest. Forces regionally aligned with a given combatant command reach forward to projected receiving combatant commands and back to national-level agencies. Regional communities of interest include—

- Regional combatant commands, their associated theater armies, and regionally aligned MI brigades (theater).
- The national-level intelligence community, which provides support through the—
  - Open Source Enterprise.
  - National Ground Intelligence Center.
  - National Geospatial-Intelligence Agency.
  - Defense Intelligence Agency (DIA).
  - National Security Agency.
- Special operations community personnel who collect open-source information through the appropriate authorities.

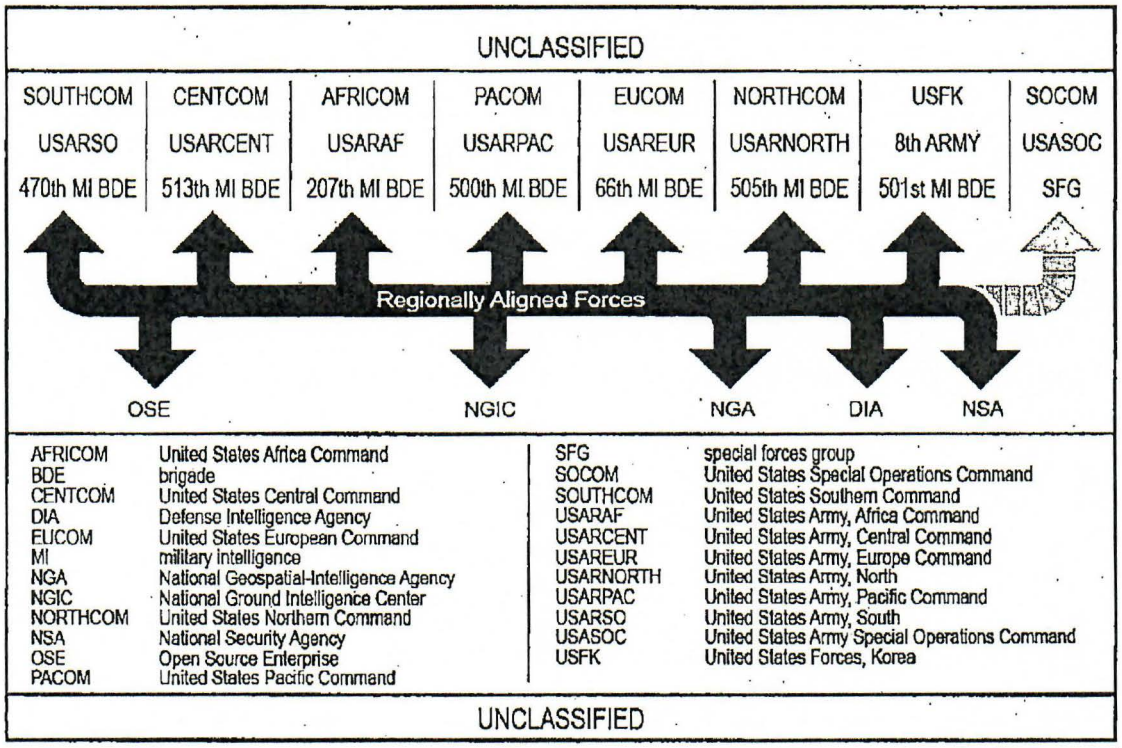


Figure 1-1. (U) Intelligence relationships among regional communities of interest

~~FOR OFFICIAL USE ONLY~~

1-18. *(U) Figure 1-2 illustrates internal and external Marine Corps intelligence relationships:*

- *Marine expeditionary forces and MICs.*
- *Regional combatant commands and their associated Marine Corps Service component commands.*
- *The national-level intelligence community, which provides support through DIA and MCIA.*

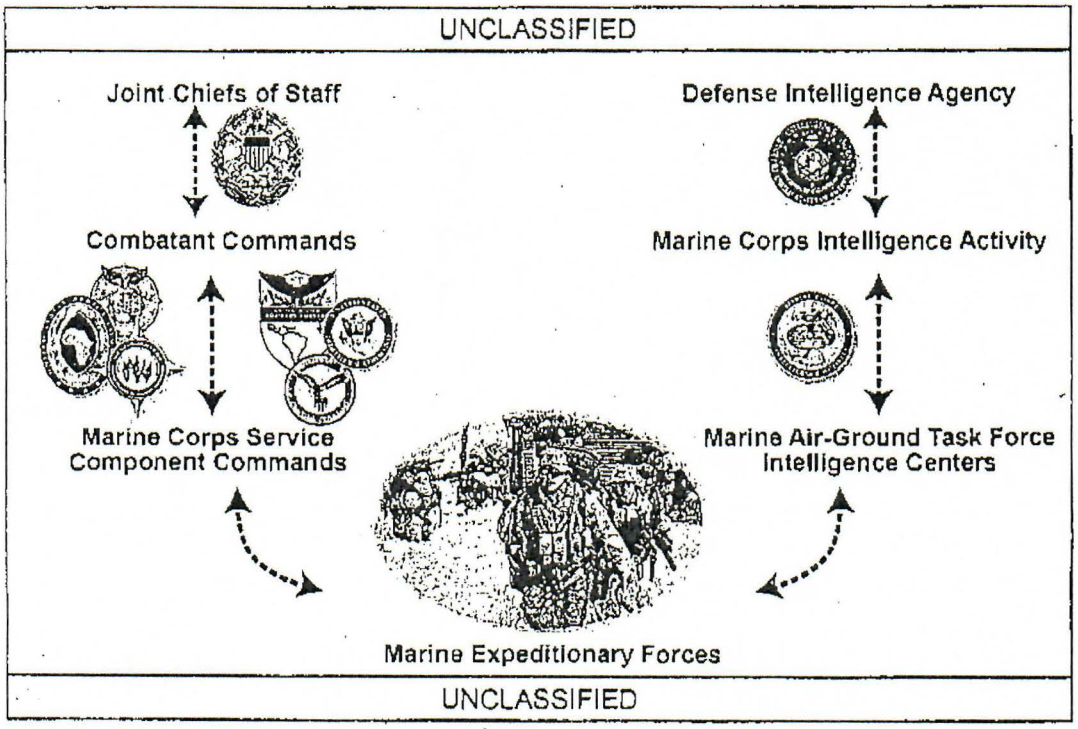


Figure 1-2. (U) *Marine Corps intelligence relationships*

GRANTING ACCESS (U)

1-19. (U) The proper management of access to databases, information, and intelligence assists in ensuring personnel, units, and organizations obtain needed information. Digitized open-source information resides in classified and unclassified data repositories. While there is an abundance of information and tools available on the internet and DOD information networks, units should contact the Army Open-Source Intelligence Office (AOO) or *MCIA* and *MICs* to receive information about accessing specific open-source tools and services. The AOO provides information and support about access to open-source tools and data and provides training and account management for Army intelligence elements.

INFORMATION SHARING (U)

(b) (3)

(b) (3)

PROCESSING, EXPLOITATION, AND DISSEMINATION (U)

1-22. (U) Executing effective OSINT requires resourcing, planning for, and preparing specific OSINT PED capabilities. OSINT PED capabilities can be organic to the intelligence unit, task-organized or attached to a supported unit, or distributed from a centralized location through the network as required. Units can execute PED using expeditionary and reach techniques. At the basic level, the intelligence warfighting function observes details about the threat and relevant aspects of the operational environment. It collects data—processed and exploited into useable information—for analysis and production that results in intelligence. Army doctrine has long recognized the functions of processing, initial analysis, and reporting, as well as the requirement to provide combat information.

1-23. (U) Expeditionary PED is the deployment of tailored formations of tactical, operational, and/or strategic intelligence Soldiers/*Marines* and enablers to support commanders. Expeditionary PED may be necessary when—

- Infrastructure is underdeveloped.
- Emerging technologies are employed.
- Continuity of operation plans is required.
- Reach capabilities cannot support high-priority, time-sensitive requirements.

1-24. (U) Reach PED is conducted from sanctuary locations. It leverages a robust communications infrastructure and pooled resources to provide multidiscipline intelligence PED support to deployed commanders. Reach PED reduces the number of forward-deployed Soldiers/*Marines* by shifting PED functions to dedicated centers within the United States or other theater locations. Reach PED depends on assured communications to maintain uninterrupted mission support.

1-25. (U) OSINT PED includes the activities necessary to process information into a useable form for ingestion into the intelligence process or for dissemination as combat information. For example, OSINT PED may include the translation of foreign language material into English (a useable form) for use during IPB. Advanced processing may involve digitizing, transcribing, and translating non-English graphics, recordings, and text documents into English-language text format. Language-based processing activities require procedures and management to ensure transcripts and translations are timely, accurate, complete, and free of bias. Continuity of operation plans, commanders' requirements, and architecture limitations may require simultaneous employment of expeditionary and reach PED elements. For example, geospatial intelligence PED may be conducted through expeditionary means, while OSINT PED may be conducted through reach to the MI brigade (theater) or DIA.

THE MILITARY DECISION-MAKING PROCESS/*MARINE CORPS PLANNING PROCESS* (U)

1-26. (U) The **military decision-making process** is an interactive planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). The MDMP is the Army's seven-step analytical approach to visualizing the operational environment, the threat, and future operations. It results in an improved understanding and a plan or order guiding the force through preparation and execution. (See ADRP 5-0 for more information on the MDMP.)

1-27. *(U) The **Marine Corps planning process** is a six-step methodology which helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the mission and the threat and is based on the Marine Corps philosophy of maneuver warfare. It*

~~FOR OFFICIAL USE ONLY~~

capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of problem framing, course of action development, course of action war game, course of action comparison and decision, orders development, and transition (MCRP 1-10.2).

Note. (U) Tenets of the MCPP include top-down planning, single-battle concept, and integrated planning. (See MCWP 5-10 for more information on the MCPP.)

1-28. (U) Upon receipt of the mission or in anticipation of a new mission, commanders and staffs begin the MDMP. During step 1, OSINT is used to generate intelligence knowledge and assist in identifying gaps addressable by open-source information. Immediately following receipt of the mission, the commander and staff begin mission analysis/*problem framing*, the second step/*first step* of the MDMP/*MCPP*. Commanders and staffs analyze the relationships among the mission variables (mission, enemy, terrain and weather, troops and support available-time available and civil considerations [METT-TC]/*mission, enemy, terrain and weather, troops and support available-time available [METT-T]*), seeking to gain a greater understanding of the—

- Operational environment, the threat, and operational variables (political, military, economic, social, information, infrastructure, physical environment, and time [PMESII-PT]/*political, military, economic, social, information, and infrastructure [PMESII]*).
- Higher commander's desired end state.
- Mission and how it is nested with the higher headquarters' mission.
- Forces and resources available to accomplish the mission and associated tasks.

1-29. (U) Throughout the MDMP/*MCPP*, various staff elements use open-source information to perform open-source research to support nonintelligence activities (for example, to prepare functional area-specific running estimates, papers, briefings, plans, and orders). Intelligence analysts use open-source information to collect intelligence in order to produce products that assist the staff in updating its running estimates and producing initial assessments. The intelligence staff also conducts OSINT activities to answer specific intelligence requirements. Major intelligence contributions to mission analysis occur as part of IPB.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD/*BATTLESPACE* (U)

1-30. (U) **Intelligence preparation of the battlefield** is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations (ATP 2-01.3). ***Intelligence preparation of the battlespace is the systematic, continuous process of analyzing the threat and environment in a specific geographic area (MCRP 2-10B.1).*** IPB is a four-step process, used to enhance situational understanding and awareness of the operational environment. By applying the IPB process, commanders gain insight to selectively apply combat power and maximize operational effectiveness at critical points in time and space. (See ATP 2-01.3/*MCRP 2-10B.1* for IPB techniques.)

1-31. (U) During IPB, OSINT makes significant and integral contributions to generating intelligence knowledge and satisfying intelligence and information requirements identified during the MDMP/*MCPP*. Mission variables (METT-TC/*METT-T*), operational variables (PMESII-PT/*PMESII*), and civil considerations (areas, structures, capabilities, organizations, people, and events [known as ASCOPE]) are tools used to collect essential information and intelligence, identify information and intelligence gaps, and organize information and intelligence into functional categories. OSINT often identifies information gaps that require additional collection and analysis.

FOR OFFICIAL USE ONLY

Chapter 2

OSINT Structures (U)

(U) This chapter describes the framework for the organization of OSINT assets to enable commanders and staffs to leverage OSINT capabilities to address specific intelligence requirements.

OSINT CAPABILITIES (U)

2-1. (U) Currently, the Army and *Marine Corps* lack a military occupational specialty for OSINT practitioners. The commander or Army intelligence staff section (G-2/S-2/R-2) may organize OSINT assets, as necessary, to meet mission requirements. The intelligence staff must balance additional requirements for OSINT against requirements from other intelligence disciplines and complementary intelligence capabilities. Any formation of an OSINT cell diverts personnel from other intelligence tasks and requirements.

2-2. (U) Generally, DOD and the intelligence community support OSINT collaboratively. The AOO collaborates with all Army intelligence elements to operationalize the use of open-source data in all-source analysis.

2-3. (U) Options available for organizing an OSINT capability include—

- Forming a dedicated cell of OSINT analysts.
- Training selected analysts throughout the intelligence element to leverage OSINT to satisfy intelligence requirements.

2-4. (U) **Reach.** The MI brigade (theater) should be leveraged for reach OSINT, regardless of the size or type of OSINT organization, the same way it provides reach support for other intelligence capabilities. **Contract support.** Contract support can augment the organization, especially to provide continuity in subject matter expertise and to coach newly trained OSINT practitioners.

OSINT—BRIGADE COMBAT TEAM AND BELOW AND *MARINE AIR-GROUND TASK FORCE* (U)

2-5. (U) Tactical commanders create OSINT cells from organic or reinforcing intelligence personnel (including the PED platoon from the expeditionary MI brigade) when required to satisfy intelligence requirements.

Note. (U) Neither brigade combat teams (BCTs)/*MAGTFs* nor battalions have assigned OSINT positions. Positions assigned to a task-organized OSINT cell come from those within the unit.

BRIGADE COMBAT TEAM AND BELOW (U)

2-6. (U) Figure 2-1 on page 2-2 illustrates a BCT OSINT cell formed from organic personnel. Positions might include—

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

~~FOR OFFICIAL USE ONLY~~

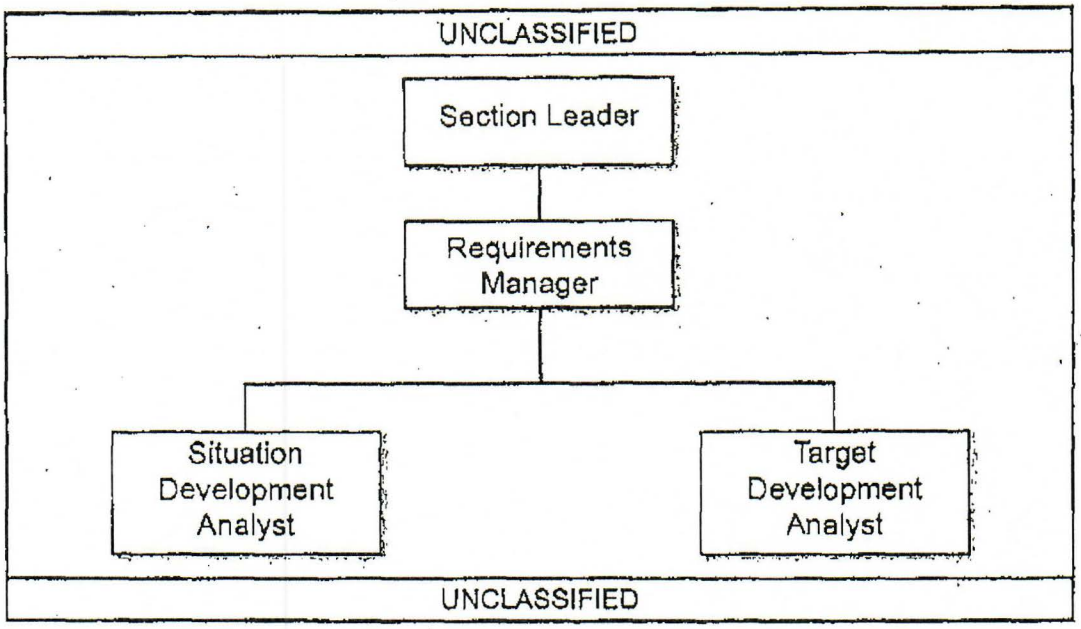


Figure 2-1. (U) Brigade combat team OSINT cell example

Section Leader (U)

2-7. (U) The section leader—

- Serves as the primary liaison and coordinator with the BCT intelligence staff.
- Oversees the BCT OSINT cell.
- Prioritizes tasks based on intelligence requirements.
- Monitors ongoing intelligence support required by the BCT intelligence staff.
- Ensures the inclusion of all OSINT products in the planning of current and future operations.

Requirements Manager (U)

2-8. (U) The requirements manager—

- Ensures situation development and target development to support the intelligence staff's efforts.
- Verifies the availability of collection assets.
- Checks for similar requirements and finished products.
- Performs quality control for situation development and target development products.
- Supervises the receipt, integration, and dissemination of OSINT products.

Situation Development Analyst (U)

2-9. (U) The situation development analyst—

- Monitors open-source information for information relevant to situation development.

(b) (3)

- Integrates information received on threat intentions, objectives, combat effectiveness, and potential missions.

~~FOR OFFICIAL USE ONLY~~

- Confirms or denies threat COAs based on open-source information.

(b) (3)

Target Development Analyst (U)

(b) (3)

MARINE AIR-GROUND TASK FORCE (U)

2-11. *(U) Figure 2-2 illustrates a MIC OSINT cell formed from organic personnel. Positions might include—*

- *OSINT officer in charge.*
- *OSINT subject matter expert.*
- *OSINT chief.*
- *OSINT analyst.*
- *OSINT collector.*

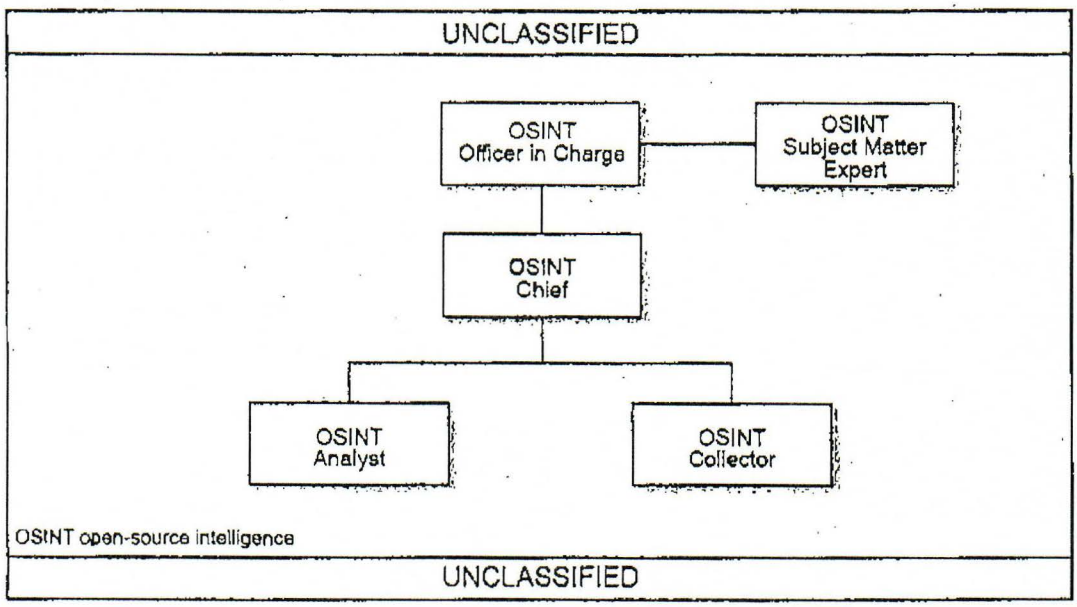


Figure 2-2. (U) ***Marine-air ground task force intelligence center OSINT cell example***

OSINT Officer in Charge (U)

2-12. *(U) The OSINT officer in charge—*

- *Serves as the primary liaison and coordinator with the MIC OSINT staff.*
- *Provides supervisory and managerial capacity oversight.*
- *Prioritizes tasks based on intelligence requirements.*
- *Ensures the inclusion of all OSINT products in the planning of current and future operations.*

OSINT Subject Matter Expert (U)

2-13. *(U) The OSINT subject matter expert—*

- *Captures open-source tradecraft.*
- *Performs the quality control of situation development and target development products.*
- *Serves as the OSINT Community of Practice representative.*

OSINT Chief (U)

2-14. *(U) The OSINT chief—*

- *Monitors ongoing intelligence support required by the MIC staff.*
- *Supervises the receipt, integration, and dissemination of OSINT products.*
- *Manages OSINT requirements and provides the estimate of supportability.*

OSINT Analyst (U)

2-15. *(U) The OSINT analyst—*

- *Monitors open-source information for information relevant to situation development.*
- *Confirms or denies threat COAs based on open-source information.*
- *Analyzes information and produces current intelligence about the enemy, weather and terrain, and civil considerations before and during operations.*

OSINT Collector (U)

2-16. *(U) The OSINT collector-*

- *Validates open-source information sourcing.*
- *Verifies the availability of collection assets.*
- *Provides open-source information on threat capabilities and limitations.*

OSINT—DIVISION AND ABOVE (U)

2-17. (U) Each theater army or *Marine expeditionary force* may have a task-organized OSINT element in scope and personnel within itself or within a *major subordinate command (MSC)*. At the division and above/MSC level, it is common for commanders to create OSINT cells from organic intelligence personnel.

2-18. (U) At the division and above/*MSC* level, OSINT cells are task-organized within the echelon intelligence staff. These cells exploit open-source information from all available sources. Any task-organized OSINT cell at the division and above/*MSC* level should support intelligence staffs at the BCT and below/*MAGTF* level by providing analytical products specific to the area of operations.

2-19. (U) While division and above/*MSC* organizations task-organize personnel to fill OSINT cells based on requirements, typically the organization of the cell is based on operational variables (PMESII-PT/*PMESII*). Although intelligence staffs may have the requirement to provide intelligence for multiple areas, using the analytical construct of the operational variables provides the focus for collection and analysis. OSINT practitioners should leverage foreign area officers, the civil affairs staff, and other staff elements who use open-source information.

RESOURCE REQUIREMENTS (U)

2-20. (~~FOUO~~) OSINT practitioners should have access to unclassified and classified networks in the same space in order to collect information, contribute to fused all-source analysis, tip or cue assets to act on time-sensitive targeting information, and perform processing, exploitation, and analysis. There is no requirement to locate the OSINT cell inside the sensitive compartmented information facility if the unit mission only requires access to open-source information.

~~FOR OFFICIAL USE ONLY~~

2-21. ~~(FOUO)~~ The number of OSINT practitioners is based on intelligence requirements, the mission, and the federation of OSINT requirements or level of support provided through reach (such as the MI brigade [theater]). The OSINT collection activity requires the unit to have the following:

- Required intelligence oversight mechanisms.
- An OSINT training and tradecraft strategy.
- Appropriate security classification guides.
- Risk assessment, OPSEC assessment, or both.
- Collection plan.

PERSONNEL DUTIES (U)

2-22. (U) Figure 2-3 illustrates a task-organized OSINT cell at the division and above/*MSC* level. The cell might include—

- Team lead and requirements collection manager.
- Situation development and production analyst.
- Two target development and production analysts.
- Two linguists.

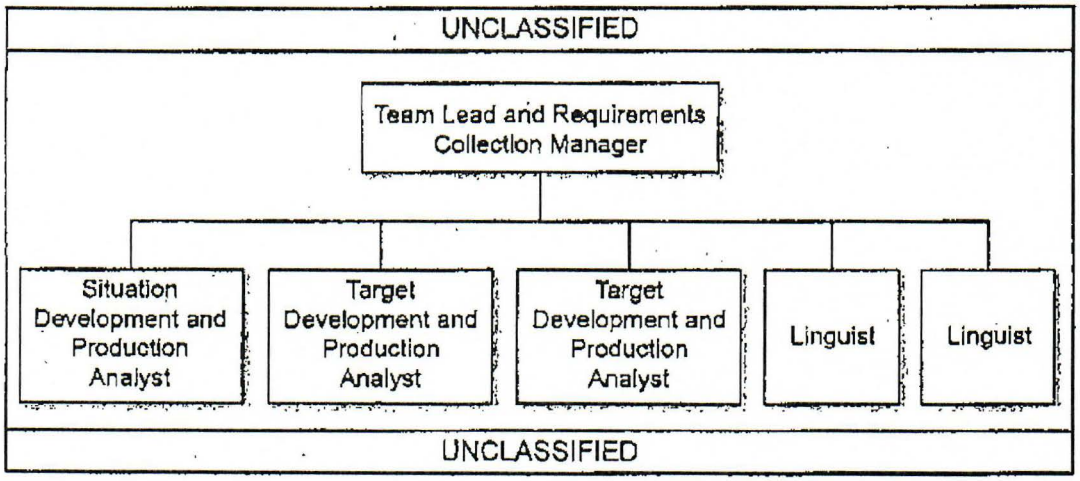


Figure 2-3. (U) Division and above/*Major subordinate command* OSINT cell example

Team Lead and Requirements Collection Manager (U)

2-23. (U) The team lead and requirements collection manager—

- Serves as the liaison with the MI brigade (theater).
- Provides cell-level intelligence oversight.
- Ensures the cell has the appropriate access to tools and data from the supporting MI brigade (theater)/*MIC* or higher headquarters.
- Trains the cell.
- Prioritizes tasks based on intelligence requirements.
- Ensures a survey of the internet environment is performed for the area of operations (for example, determines the percentage of the population using the internet and the types of usage).
- Inputs the unit's commercial content requirements into (b) (3) if required, and monitors community responses.
- Inputs the unit's information requirements into (b) (3) and monitors community responses.
- Performs cell production quality control and supervises dissemination.
- Ensures the inclusion of relevant products in the planning of current and future operations.

Situation Development and Production Analyst (U)

2-24. (U) The situation development and production analyst—

- Monitors OSINT products from the MI brigade (theater)/*MIC* and other OSINT producers.
- Collects and analyzes open-source information based on intelligence requirements.
- Tips or cues other intelligence disciplines.
- Alerts the intelligence noncommissioned officer in charge or OSINT technician of mission-critical information.
- Produces current intelligence about the threat, terrain, and civil considerations.

Target Development and Production Analysts (U)

2-25. (U) The target development and production analysts—

- Monitor OSINT products from the MI brigade (theater)/*MIC* and other OSINT producers.
- Collect and analyze open-source information based on intelligence requirements.
- Tip or cue other intelligence disciplines.
- Alert the intelligence noncommissioned officer in charge or intelligence technician of mission-critical information.

(b) (3)

Linguists (U)

2-26. (U) Linguists perform translation, transcription, and interpretation tasks. (See paragraphs 3-39 through 3-42 and paragraphs 5-5 through 5-8 for additional information on language support.)

SERVICE ORGANIZATIONS (U)

2-27. (U) OSINT activities are conducted throughout the national and defense intelligence enterprise. The National Open-Source Committee (NOSC) is the body of representatives that meet to collaborate on OSINT issues and requirements and reports to the Board of Governors. The Defense Open-Source Council (DOSC) represents OSINT communities of interest in the defense intelligence enterprise.

ARMY CHIEF INFORMATION OFFICER/G-6 (U)

2-28. (~~FOUO~~) The Army Chief Information Officer/G-6 provides—

- Guidance and resource planning for OSINT-unique network and technical requirements.
- Guidance to Army commands regarding commercial circuit connections to the internet in support of Army open-source activities.

ARMY DEPUTY CHIEF OF STAFF, G-2 (U)

2-29. (U) The Army Deputy Chief of Staff, G-2—

- Serves as the functional proponent for U.S. Army OSINT policy, strategic planning, and programming.
- Represents the Army at the NOSC and DOSC and coordinates Army OSINT programs and activities through them.
- Provides strategic planning for OSINT activities and resource planning for OSINT operations, as authorized and directed by the Director of National Intelligence and the Secretary or Deputy Secretary of Defense or the Under Secretary of Defense for Intelligence; coordinates U.S. Army OSINT functional requirements during military and national intelligence programmatic processes.

- Coordinates with the Army Chief Information Officer/Deputy Chief of Staff, G-6 for unique network requirements to support OSINT activities.
- Ensures U.S. Army intelligence elements conduct OSINT activities in compliance with U.S. law, the Director of National Intelligence, DOD, and Army policies, guidelines, and restrictions, particularly those regarding intelligence oversight rules and procedures.

U.S. Army Intelligence and Security Command, Army OSINT Office (U)

2-30. (~~FOUO~~) INSCOM is the Army operational proponent for OSINT and the capabilities requirements manager for the Army OSINT program. INSCOM manages the Army OSINT program though the AOO, which oversees the program. (b) (3) (b) (3) (b) (3) Army units that want to establish an OSINT capability should consult the AOO.

2-31. (~~FOUO~~) For the Army, the AOO—

- Serves as a start point for units interested in OSINT capabilities.

(b) (3)

- Trains, certifies, and provisions Army intelligence professionals.

(b) (3)

- Provisions Army intelligence professionals based on the Army's operational priorities.
- Enables operational OSINT activities for Army intelligence elements.

2-32. (~~FOUO~~) INSCOM supports each geographic combatant command through its subordinate, regionally focused MI brigades (theater). Each MI brigade (theater) addresses intelligence requirements and provides support to Army tactical units deploying to or operating within the supported combatant command's area of responsibility. The reach support provided by MI brigades (theater) includes OSINT.

Marine Corps Intelligence Activity (U)

2-33. *(U) The MCIA's Center for Marine Expeditionary Intelligence Knowledge OSINT Cell is the OSINT hub for the Marine Corps intelligence, surveillance, and reconnaissance enterprise. MCIA OSINT pursues professionalization and development of the OSINT discipline in the enterprise through the development and maintenance of the OSINT Community of Practice, doctrine, policy, and the development of innovative OSINT practices and tradecraft.*

Department of the Army Intelligence Information Service (U)

2-34. (U) DA IIS provides a broad spectrum of intelligence support functions to Army intelligence components and international intelligence community partners. It is the primary dissemination proponent for the Army. DA IIS is an operational element of the Army MI, Intelligence Community Information Management Directorate and administratively assigned to Headquarters, INSCOM.

2-35. (U) DA IIS provides OSINT support to partners conducting foreign intelligence collection, analysis, and production missions. It is the Army's open-source requirements manager for validating information requirements and managing Army accounts within (b) (3) and other intelligence community and DOD capabilities. (b) (3) (b) (3)

(b) (3)

U.S. ARMY INTELLIGENCE COMPONENTS (U)

2-37. (U) All commanders of intelligence components authorized to conduct OSINT will, when conducting OSINT activities:

- (~~FOUO~~) Ensure that risk assessments are conducted to support OSINT collection by command and subordinate units; that intelligence personnel receive specific OSINT OPSEC training; and, when conducting risk management level 1 activities, that intelligence personnel are trained in the use of managed attribution.
- (U) Ensure annual intelligence oversight training specific to OSINT, including the use of social media, is conducted and oversight of OSINT collection activities occurs.

(b) (3)

- (U) Submit requests for OSINT information through (b) (3) to deconflict existing requirements and products and post new unit requests as needed. Army commands with available intelligence analysis capacity and a mission to conduct analysis activities in support of the intelligence community, DOD, or other Army intelligence requirements are encouraged to routinely review (b) (3) and provide answers where possible. The (b) (3) and Headquarters, INSCOM manages Army accounts.

U.S ARMY CYBER COMMAND (U)

(b) (3)

PART TWO

OSINT and the Intelligence Process (U)

(U) Part two discusses OSINT within the intelligence process. The Army views the intelligence process as a model that describes how the intelligence warfighting function develops intelligence that facilitates situational understanding and supports decision making. The steps of the intelligence process are **plan and direct**, **collect**, **produce**, and **disseminate**. **Analyze** and **assess** are the two continuing activities that occur continually throughout the process. Chapters 3 through 6 each address an intelligence process step. Since the continuing activities occur during all steps, each chapter incorporates discussions of these activities, placing them in the various contexts in which they occur.

Chapter 3

Plan and Direct (U)

(U) The plan and direct step of the intelligence process closely corresponds with the plan activity of the operations process. The plan and direct step starts well in advance of detailed planning. It includes activities such as open-source collection, intelligence reach, and analysis. These activities produce the initial intelligence knowledge about the operational environment. After receipt of mission, intelligence analysts prepare planning products for the commander and staff for orders production and execution of operations. OSINT products support the plan and direct step by attempting to provide a context for understanding classified information. OSINT products may also reduce large target sets by quickly filling information gaps and allowing the efficient use of low-density intelligence collection assets.

INFORMATION COLLECTION AND OSINT (U)

3-1. (U) Information collection activities provide data and information about the threat and relevant aspects of the operational environment needed to develop the detailed and timely intelligence that commanders require to gain situational understanding. Information collection is an integrated intelligence and operations function and a combined arms operation. At the tactical level, commanders use surveillance, reconnaissance, security, and intelligence operations to collect information that answers the commander's critical information requirements (CCIRs). (For more information on surveillance, reconnaissance, security, intelligence operations, see FM 3-55 and *MCTP 2-10A*; FM 3-90-2, *MCRP 2-10A.6*, and *MCTP 3-20G*; FM 3-90-2, *MCTP 2 10A*, and *MCTP 3-20G*; and FM 2-0, respectively.)

3-2. (U) During planning, staffs recommend information requirements for commanders to designate as CCIRs. Commanders drive the intelligence process by providing guidance and approving CCIRs. The commander's guidance—

~~FOR OFFICIAL USE ONLY~~

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

3-3. (U) **Commander's critical information requirement** is an information requirement identified by the commander as being critical to facilitating timely decision making (JP 3-0). CCIRs comprise two types of requirements:

- **Priority intelligence requirement** is an intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or other aspects of the operational environment (JP 2-01).
- **Friendly force information requirement** is information the commander and staff need to understand the status of friendly force and supporting capabilities (JP 3-0).

3-4. (U) Open-source information is used to answer specific information requirements developed during planning requirements and assessing collection (see ATP 2-01 and *MCTP 2-10A*) and IPB (see ATP 2 01.3/*MCRP 2-10B.1*). The collection of open-source information is a means to analyze mission variables (METT-TC/*METT-T*) and operational variables (PMESII-PT/*PMESII*).

INTELLIGENCE MISSIONS AND INFORMATION REQUIREMENTS (U)

3-5. (U) To conduct OSINT activities, the commander or designated authority (for example, the G-2/S-2/R-2, analysis and control element chief, collection manager) must ensure the following:

- The command, organization, or element has obtained authority to conduct OSINT activities.
- Forward-stationed or forward-deployed units establish an OSINT collection plan aligned to the supported combatant command. This plan is retained for unit leaders and intelligence oversight officials to review annually.
- Continental U.S.-based global response forces, regionally aligned forces, reachback elements, and other continental U.S.-based support elements planning to conduct OSINT activities must align their mission to a supported combatant command's intelligence mission, and document the mission in an established collection plan that is retained for unit leaders and intelligence oversight officials to review periodically, per DODM 5240.01.
- The OSINT collection plan must also identify and document information requirements reviewed from the national intelligence priorities framework, integrated defense intelligence priorities, theater operation plans, or the commander's PIRs.

PLANNING FOR OSINT ACTIVITIES (U)

3-6. (U) During the plan and direct step, commanders and staffs consider the following activities, as shown in figure 3-1, regarding open-source information and OSINT:

- Identify information and intelligence requirements.
- Categorize information and intelligence requirements by type.
- Identify assets to collect information.
- Determine collection techniques.

~~FOR OFFICIAL USE ONLY~~

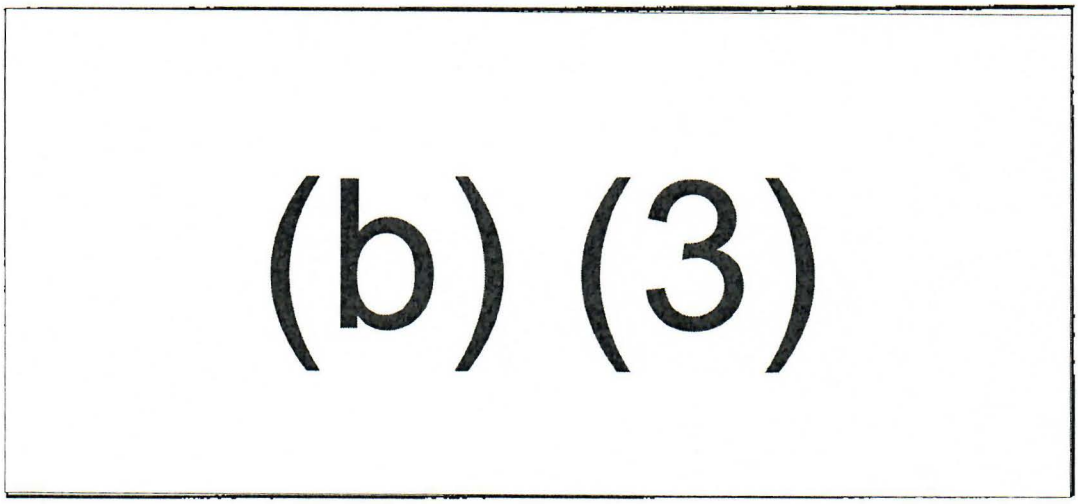


Figure 3-1. (U) Planning for OSINT activities

IDENTIFY INFORMATION AND INTELLIGENCE REQUIREMENTS (U)

3-7. (U) Intelligence and information gaps are identified during IPB. These gaps should be developed and framed in terms of the mission and operational variables to ensure the commander receives the information required to support all lines of operations or lines of effort. Upon receipt of open-source information, OSINT practitioners update IPB products and inform the commander of any relevant changes. Those responsible for producing OSINT require clearly stated information and intelligence requirements to focus collection and production effectively. These requirements should be incorporated into collection plans.

Note. (U) OSINT cannot eliminate all unknown aspects or uncertainties that concern commanders and staffs. During planning, the intelligence staff fills gaps with reasonable assumptions. Upon filling gaps with collected information, the intelligence staff develops databases at the unit level to make the information readily available. Analysts should routinely review requirements through (b) (3) since information to answer their requirements may exist. This reduces the number of new requests for information (RFIs) from subordinate units or organizations.

CATEGORIZE INFORMATION AND INTELLIGENCE REQUIREMENTS BY TYPE (U)

3-8. (U) During planning requirements, the intelligence staff categorizes intelligence and information requirements by type based on mission analysis and friendly COAs. (See ATP 2-01 and *MCTP 2-10A*.) Two important related terms that work in concert with categorizing requirements are PAI and private information:

- **PAI**, in context with DODM 5240.01 (see paragraph 1-3).

(b) (3)

Note. (U) 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. (b) (3) (b) (3) This strengthens the credibility of OSINT products that support all-source intelligence. OSINT validation provides the ability to cue other assets, thus enhancing accuracy and precision.

IDENTIFY ASSETS TO COLLECT INFORMATION (U)

3-9. (U) The intelligence and operations staffs use the commander's guidance and PIRs to complete the information collection plan. The information collection plan is used to assign tasks to subordinate units or submit requests to supporting intelligence organizations to achieve the desired information collection objectives. Therefore, it is imperative for intelligence and operations staffs to be familiar with the capabilities of any task-organized OSINT cell within their organizations. The information collection plan—

- Is used to request collection and production support from joint, interagency, intergovernmental, and multinational organizations.
- Is used to task-organize and deploy organic, attached, and contracted collection assets.
- Describes how the unit conducts remote, intelligence reach or distributed information collection activities.

3-10. (U) When developing information collection tasks for subordinate units, the intelligence and operations staffs use the task and purpose construct for developing task statements to account for the following:

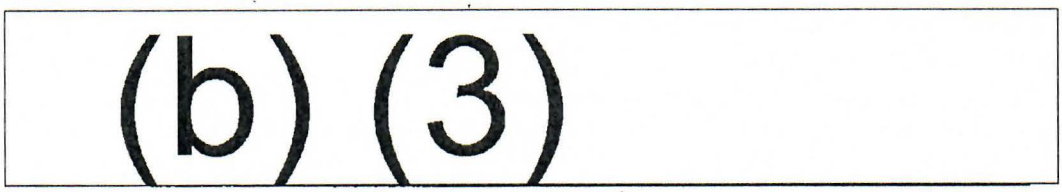
- **Who** executes the task?
- **What** is the task?
- **When** will the task begin?
- **Where** will the task occur?

DETERMINE COLLECTION TECHNIQUES (U)

3-11. (U) Determining the open-source collection technique involves deciding the most effective way to acquire open-source information. The extent to which open-source collection yields valuable information varies greatly with the nature of the target and the subject involved. Collection techniques, depending on operation complexities, can enhance the chances of satisfying intelligence and information requirements.

3-12. (U) Research and collection on the internet require a risk assessment. The result of the risk assessment affects the techniques used for conducting OSINT activities. While portions of the internet that are publicly available may be open-source, knowledge of the techniques used to collect the information may cause the targeted individual, group, or nation to block, change, deceive, or turn off the source. Thus, techniques used for collecting open-source information must be addressed in the risk assessment.

3-13. (U) Collection requires access to the internet to acquire PAI. OSINT practitioners apply the intelligence process to open-source information to produce a product and populate intelligence resources. Units can contact the AOO to identify requirements for PAI and open-source data and data sources. The AOO provides approved enterprise capabilities, resources, and solutions.



3-14. (U) The primary open-source requirements management database is (b) (3) Unit-level OSINT requirements and products are posted to (b) (3) (b) (3) This allows deconfliction with existing requirements and answers. New unit-level RFIs are added as needed. Units with intelligence analysis capacity and an authorized mission are encouraged to routinely review requirements relevant to their area of operations in (b) (3) and produce OSINT answers where possible. Using (b) (3) allows users to understand the scope of current OSINT activities in the DOD intelligence enterprise as well as obtain answers to the following:

- Who has requirements?
- Who is answering requirements?
- What requirements are answered?
- Who else has similar requirements?
- Who needs additional commercial data sources and what sources are needed?
- Who can provide those commercial data sources?

~~FOR OFFICIAL USE ONLY~~

(b) (3)

PREPARATION CONSIDERATIONS FOR OSINT ELEMENTS ACCESSING THE INTERNET (U)

3-16. (U) OSINT cells and intelligence analysis elements conducting OSINT activities need proper preparation in the areas of policies, training, tradecraft, and accesses. Table 3-1 identifies OSINT preparation considerations.

Table 3-1. (U) OSINT preparation considerations

UNCLASSIFIED
• Internet access. (b) (3) (b) (3) • SIPRNET access (b) (3) (b) (3) • JWICS access (b) (3) (b) (3) • Established intelligence oversight program (compliance of U.S. person information). • (b) (3) • Risk management plan. • Information collection plan. • OSINT security classification guide. • (b) (3) • Understanding of the supporting OSINT community of interest. • Possible co-location of unit OSINT analysts with established OSINT organizations or leveraging reach support from military intelligence (MI) brigades (theater), corps/expeditionary MI brigades. • OSINT training and tradecraft. Review Foundry, Open-Source Tradecraft Division, and the Academy for Defense Intelligence for appropriate OSINT offerings, including those related to— ▪ Operations security. ▪ Intelligence oversight. ▪ Basic OSINT tradecraft. ▪ Advanced OSINT tradecraft. • Account access requirements. Contact the Army OSINT Office (AOO)/*MCIA* or the supported combatant command: ▪ (b) (3) ▪ Secure web browsing. ▪ Information collection plan. ▪ Co-location of unit OSINT analysts with established OSINT organizations or leveraging reach support.
JWICS Joint Worldwide Intelligence Communications System SIPRNET SECRET Internet Protocol Router Network
UNCLASSIFIED

~~FOR OFFICIAL USE ONLY~~

3-17. (U) Additional OSINT considerations include—

- Compliance with laws and policies.
- OPSEC.
- Security classification guidance.
- Use of social media for OSINT purposes.
- Coordination.
- Deception and bias.
- Copyright.
- Linguist support.

(b) (3)

COMPLIANCE WITH LAWS AND POLICIES (U)

3-18. (U) OSINT is governed by EO 12333 as amended, DODM 5240.01, DOD 5240.1-R, and DODI 3115.12. AR 381-10 and *MCO 3800.2B* implement these orders and policies for Army and *Marine Corps* intelligence activities, respectively. Army and *Marine Corps* intelligence elements conducting OSINT activities should periodically review DODM 5240.01, DOD 5240.1-R, AR 381-10, and *MCO 3800.2B*, focusing on authorities and restrictions pertaining to U.S. person information. (See appendix A for additional information on the legal restrictions and regulatory limitations on OSINT.)

OPERATIONS SECURITY (U)

3-19. (U) Intelligence personnel who collect open-source information must pay careful attention and comply with OPSEC requirements as defined in AR 530-1 and *MCO 3070.2A* to prevent disclosure of critical and sensitive information in any public domain. Searches and visits to internet websites leave a virtual footprint exploitable by both technically sophisticated and relatively unsophisticated adversaries. Army intelligence component commanders should perform risk assessments before any internet collection activity with or without the use of secure web browsing techniques. (See appendix B for information on secure web browsing techniques.) Risk assessments assist in balancing the risks and expected benefits of conducting the proposed OSINT activity. Risk assessment results affect how intelligence personnel conduct OSINT activities, as detailed in the information collection plan, and the subsequent classification of information.

3-20. ~~(FOUO)~~ The results of risk assessment are instrumental when determining Army OSINT risk management level status in accordance with U.S. Army Directive 2016-37 and are as follows:

- **Risk management level 0:** A risk assessment that determines the threat knowledge of the OSINT activity will not pose a risk to imminent or ongoing military operations or intelligence priorities, sources, or methods is a risk management level 0 collection activity. Risk management level 0 activities require annual OPSEC training.
- **Risk management level 1:** A risk assessment that determines the threat knowledge of the OSINT activity could pose a risk to imminent or ongoing military operations or intelligence priorities, sources, or methods is a risk management level 1 collection activity. Risk management level 1 activities require that—
  - Intelligence professionals leverage OSINT data the intelligence community provides on government networks to the greatest extent possible before collecting open-source information from the internet.

(b) (3)

  - Army intelligence components must obtain approval from Headquarters, INSCOM; a national intelligence agency; a combat support agency; or supported combatant command before acquiring managed attribution capabilities.
  - Intelligence personnel complete annual OPSEC training as well as training in managed attribution.

3-21. (U) Since collection focuses on answering intelligence requirements, protection of both the type of data collected and the source from which it is collected is a priority. For example, if a local newspaper or the threat realizes that friendly forces are using the newspaper to develop intelligence, the threat may deny access to the newspaper or manipulate the information it contains. This situation could make friendly forces a deception target or put them at risk by denying them information. Protection of OSINT sources includes

~~FOR OFFICIAL USE ONLY~~

discrete use of the sources to prevent denial of access to the sources. The AOO can support unit requirements to identify and mitigate online risk while conducting OSINT activities.

3-22. ~~(FOUO)~~ Personnel who have accessed websites in a risk management level 1 capacity may not access those same websites using personally owned electronic devices for the purposes of OPSEC. This restriction does not apply to accessing commercially or publicly owned news media websites (such as CNN or ABC News). The use of the internet for purely personal interests, which include academic research and news information or subscriptions, is not an OSINT activity.

3-23. (U) Reading classified information and then going to the internet to conduct searches on open-source information based on the classified information may alert the target of friendly force interest. Knowing where friendly forces seek information may cause a target to change its behavior or place a classified source at risk. In some cases, this knowledge may endanger mission accomplishment or Soldiers'/*Marines'* lives. For this reason, it is important to obtain a current OSINT classification guide and perform a risk assessment regarding OSINT collection.

SECURITY CLASSIFICATION GUIDANCE (U)

3-24. (U) It is a common misperception that all information residing on the internet is automatically considered unclassified; however, there have been instances in which—

- Individuals intentionally leaked classified information to the public domain.
- An inadvertent disclosure of information was made available to unclassified sources.
- Two or more separate pieces of unclassified information, when combined, become classified information. (For example, a location, such as Abbottabad, and a person's name, such as Osama Bin Laden, are not classified pieces of information in and of themselves. However, combining those separate pieces of information-Osama Bin Laden is in Abbottabad—classifies the information.)

Note. (U) An OSINT practitioner must be aware that collection of a classified document on a DOD NIPRNET workstation constitutes a security violation.

3-25. (U) The exploitation, processing, and analysis of information holdings may increase the classification level. For example, two unclassified facts, when combined, could increase the classification of information obtained. Furthermore, an OSINT practitioner must be aware that combining site searches may give away information about PIRs. All personnel performing OSINT activities must possess the appropriate security clearance and access.

3-26. (U) Units under the operational command of a combatant command are required to use the combatant command security classification guidance. If there is no security classification guidance relevant to open-source information, information should be unclassified, controlled unclassified, and releasable to foreign partners for official use to the extent possible. However, there are several circumstances for which this information may or must be classified and/or not releasable. Security classification must be determined by judiciously considering all applicable elements—particularly the loss of a source of information or harm to an operational mission should the source be improperly revealed.

(b) (3)

(b) (3)

COORDINATION (U)

3-28. (U) The collection of open-source information requires coordination with higher and adjacent units to ensure the open-source collection effort is not redundant. Routine deconfliction of open-source collection allows units to focus on information specific to their area of operations.

3-29. (U) During planning, the intelligence and operations staffs ensure the synchronization of OSINT tasks with the scheme of maneuver (especially the scheme of information collection) and the scheme of intelligence. Acquiring open-source information may compromise the operations of other intelligence disciplines or tactical units. Open-source collection that is not synchronized may result in redundant tasking of collection assets and the improper use of forces and equipment. Redundant tasking may adversely affect the ability of nonintelligence organizations, such as civil affairs, military police, and public affairs, to accomplish their missions and tasks. Conversely, obvious contact with an open-source by nonintelligence organizations can compromise OSINT tasks and lead to the loss of intelligence.

(b) (3)

BCT/*MAGTF* would focus its open-source collection at the district and neighborhood levels.

3-31. (U) Army intelligence organizations, units, and elements authorized to conduct OSINT activities that have RFIs requiring risk management level 1 OSINT collection will coordinate with their collection management team using the (b) (3) (b) (3) to manage OSINT production requirements. If the RFI requires new OSINT collection, the collection manager should articulate it as a collection requirement in (b) (3) Collection managers must deconflict existing requirements and insert new unit-level RFIs as needed. Army commands with available intelligence analysis capacity and a mission to conduct analysis activities in support of the intelligence community, DOD, or other Army intelligence requirements are encouraged to routinely review global intelligence information requirements inside (b) (3) and provide answers where possible. (b) (3) (b) (3) and Headquarters, INSCOM manages Army accounts.

DECEPTION AND BIAS (U)

(b) (3)

3-33. (U) Normally, collecting open-source information does not require direct observation of activities and conditions within the area of operations. However, some situations may require collection from secondary sources, such as government press offices, commercial news organizations, and nongovernmental organization spokespersons. These sources can intentionally or unintentionally add, delete, modify, or otherwise filter the information released to the public. (b) (3)

(b) (3)

(b) (3) It is important to know the background of open sources and the purpose of the public information. This knowledge assists analysts in identifying objectives and factual information, identifying bias, and highlighting deception efforts against the local audience as well as the overall operation. It would be of great value if a linguist had insight into cultural normalcies and identifying propaganda.

COPYRIGHT (U)

3-34. (U) When preparing OSINT products, intelligence personnel must consider intellectual property rights. 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. Intelligence personnel using copyrighted material for which permission from the author has been obtained cite the source of the material.

3-35. (U) There is considerable data available on the internet protected by copyright law. OSINT practitioners need to be aware of information protected by copyright and ensure their collection does not violate the ownership of the information. Intellectual property is considered any creation of the mind, including but not limited to—

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

3-36. (U) 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 (Section 107, Title 17, USC). 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 use of copyrighted work in intelligence products falls into the category of fair use for scholarship and research. Fair use information should include attribution citations in intelligence products referencing organizations or authors and the originating source title and date. The four factors in determining fair use include—

- 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.

3-37. (U) Questions for determining whether copyright permission is required or fair use applies should be directed to the local staff judge advocate or other legal counsel. If it is reasonably believed that the material will be publicly released, a written legal opinion by the supporting staff judge advocate or other legal counsel is required.

3-38. (U) AR 27-60, DODM 5240.01 and DOD 5240.1-R prescribe policies and procedures for the acquisition, protection, transfer, patent usage, copyrights, and trademarks of intellectual property. Army and *Marine Corps* policies recognize the rights of copyright owners, consistent with missions and worldwide commitments. OSINT practitioners 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 practitioners to forward the material to be published publicly outside of intelligence organizations to the Army Judge Advocate General's Corps/*Marine Corps Judge Advocate Division* for approval and waiver of notice to the copyright holder, if necessary, for OPSEC. (For more information on copyright laws and applicability, access the U.S. Copyright Office website on NIPRNET or contact the local staff judge advocate office.)

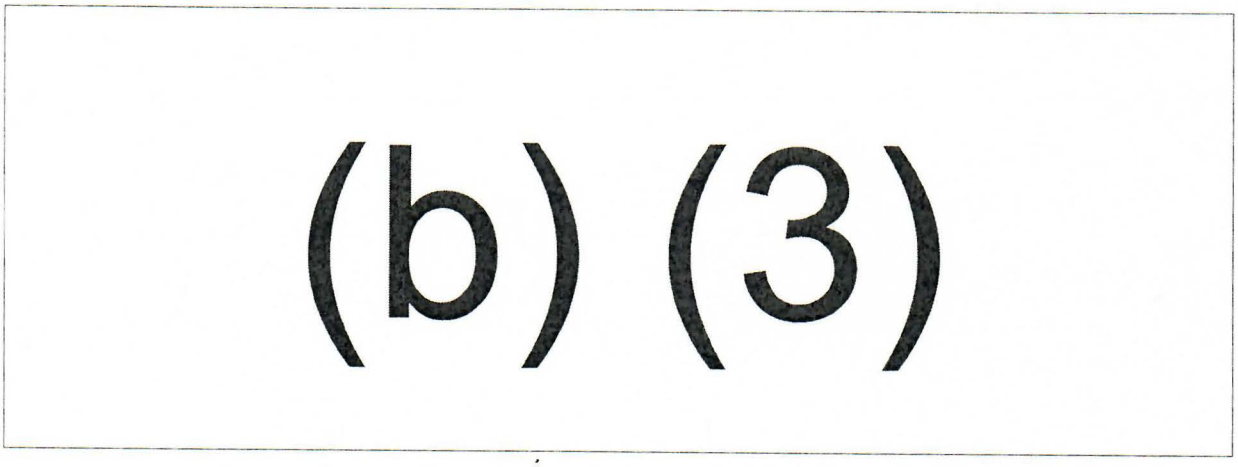
LINGUISTS (U)

3-39. (U) The collection of open-source information often requires linguists or foreign language translation capabilities or both. Local nationals are often the best source of linguists able to translate collected information correctly and in the proper context. All local nationals used for open-source collection must be vetted thoroughly for OPSEC reasons. (See FM 2-0 for information on language support; AR 11-6 for policy on evaluation and reevaluation of linguist proficiency; and *MCO 1550.25A for information on the Marine Corps Foreign Language Program.*)

~~FOR OFFICIAL USE ONLY~~

3-40. (U) The ability to collect and analyze foreign material is critical in OSINT exploitation. The effective use and employment of linguists, both civilian and military, facilitate this activity. The tasks for which foreign language skills and knowledge proficiency are most critical include—

- **Transcription.** Both listening and writing proficiency in the source language are essential for an accurate transcript. A transcript is extremely important when the transcriber's English-language skills are inadequate for authoritative or direct translation from audio or video into English text.
- **Translation.** Bilingual competence is a prerequisite for translations. Translators 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.** Interpretation is a specific skill. Not all linguists are trained to perform it. Bilingual competence is a prerequisite for interpretation. Interpreters 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.



~~FOR OFFICIAL USE ONLY~~

Chapter 4

Collect (U)

(U) There are several means of collecting open-source information during OSINT collection activities. Intelligence personnel should take advantage of these deep and important open sources of information. The employment of OSINT resources to collect from intelligence requirements varies by echelon. However, using search techniques is fundamental to OSINT collection and can be implemented in any unit. Exploiting media sources, using search engines, and collecting information specific to the operational environment should be standard operating procedures (SOPs) for any OSINT cell. These collection procedures should be planned and implemented the same way as those for any other intelligence discipline.

OSINT COLLECTION ACTIVITIES (U)

4-1. (U) OSINT collection, as with other collection activities, consists of collecting, processing, and reporting information in response to intelligence requirements. Soldiers/*Marines* and civilians collect information and data from open sources. Intelligence analysts subsequently use this information in intelligence production and ultimately support the commander's situational understanding. OSINT collection activities transition as requirements and missions change, operations proceed through different phases, and staffs prepare for future operations.

4-2. (U) Commander's guidance and intelligence and information requirements drive the collection of open-source information. Collected information is the foundation of intelligence databases, intelligence production, and situational awareness.

Note. (U) Staff personnel also acquire PAI from open sources that is incorporated into the running estimate and used during IPB.

4-3. (U) Analysts conducting OSINT activities perform several tasks to establish duties and maintain focus on requirements. The following include examples of tasks performed by OSINT cells:

- **Monitoring operations.** This task ensures responsiveness to the current situation and assists the cell in anticipating future collection, processing, reporting, and synchronization requirements.
- Collect information from publicly available open sources.
- **Perform source validation and report screening.** Information is verified and validated based on PIRs and the commander's guidance. This action ensures pertinent and relevant information is not overlooked. Information to be analyzed is screened first to reduce the volume to a workable size. Validation should encompass the elements of timeliness, completeness, and relevance to satisfy intelligence requirements.
- **Disseminate intelligence products and information.** OSINT products, information papers, executive summaries, and country studies are disseminated to customers via such means as email, M3 messaging system, (b) (3)
- Cue. OSINT cueing from other intelligence disciplines' information collection assets improves the information collection effort. Cueing enables the use of a multidiscipline approach to confirm or deny information by another information source, collection organization, or production activity. It also keeps organizations abreast of emerging unclassified information and opportunities.

~~FOR OFFICIAL USE ONLY~~

TYPES OF OPEN-SOURCE INFORMATION (U)

4-4. (U) Identifying the potential source of information is part of planning requirements and assessing collection. Open sources include but are not limited to—

- (b) (3)
- (b) (3)
- **Commercial and public information services.** Broadcasted, posted, and printed news on current international, regional, and local topics.
- (b) (3)
- **Individuals and groups.** Handwritten, painted, posted, printed, and broadcasted information disseminated as art; graffiti; leaflets; posters; tattoos; and websites.
- (b) (3)

Note. (U) Information and intelligence requirements that require confidential sources are not assigned to OSINT cells. Confidential sources consist of any persons, groups, or systems that provide information with the expectation that the information, relationship, or both are protected against public disclosure.

OSINT COLLECTION (U)

4-5. (U) Collection implies gathering, by a variety of means, data and information from which finalized intelligence is then created or synthesized and disseminated. After determining the collection technique (as discussed in paragraphs 3-11 through 3-15), OSINT practitioners conduct collection to satisfy intelligence requirements.

4-6. (U) OSINT collection—

- Leads to information used to populate intelligence databases and assist in developing OSINT products. These databases enable OSINT practitioners to respond to changes in the area of operations by providing accurate information to satisfy requirements.
- Is used to collect open-source information that contributes to understanding the area of operations.
- Is used to generate intelligence knowledge before and during deployments.

4-7. (U) PAI can be collected through several methods, two of which include—

- **Nontraditional**—the practice of using the internet for information (such as open-source information from the world wide web).
- **Traditional**—the practice of searching for open-source information that does not use any technological processes (for example, researching solely in books, libraries, broadcasting, newspapers, magazines).

4-8. (U) All inquiries begin with determining a requirement and developing a plan.

DETERMINE THE COLLECTION REQUIREMENT (U)

4-9. (U) Collection begins with determining a collection requirement. When considering OSINT collection, the requirement can be framed in terms of the mission variables (METT-TC/*METT-T*) or operational variables (PMESII-PT/*PMESII*). The collection requirement is refined through the development of intelligence requirements to be satisfied. Requirements that cannot be satisfied using open-sources are identified and tasked to another collection asset.

~~FOR OFFICIAL USE ONLY~~

DEVELOP THE OSINT COLLECTION PLAN (U)

4-10. (U) Different facets of a question may be expressed as information and intelligence requirements. These requirements form the basis for the OSINT collection plan, which can use both nontraditional and traditional collection methods. The OSINT collection plan consists of the following:

- Identification of open sources.
- Description of how to access those sources.
- Format for compiling the data.
- Collection methodology.
- Dissemination plan.

IMPLEMENT THE OSINT COLLECTION PLAN (U)

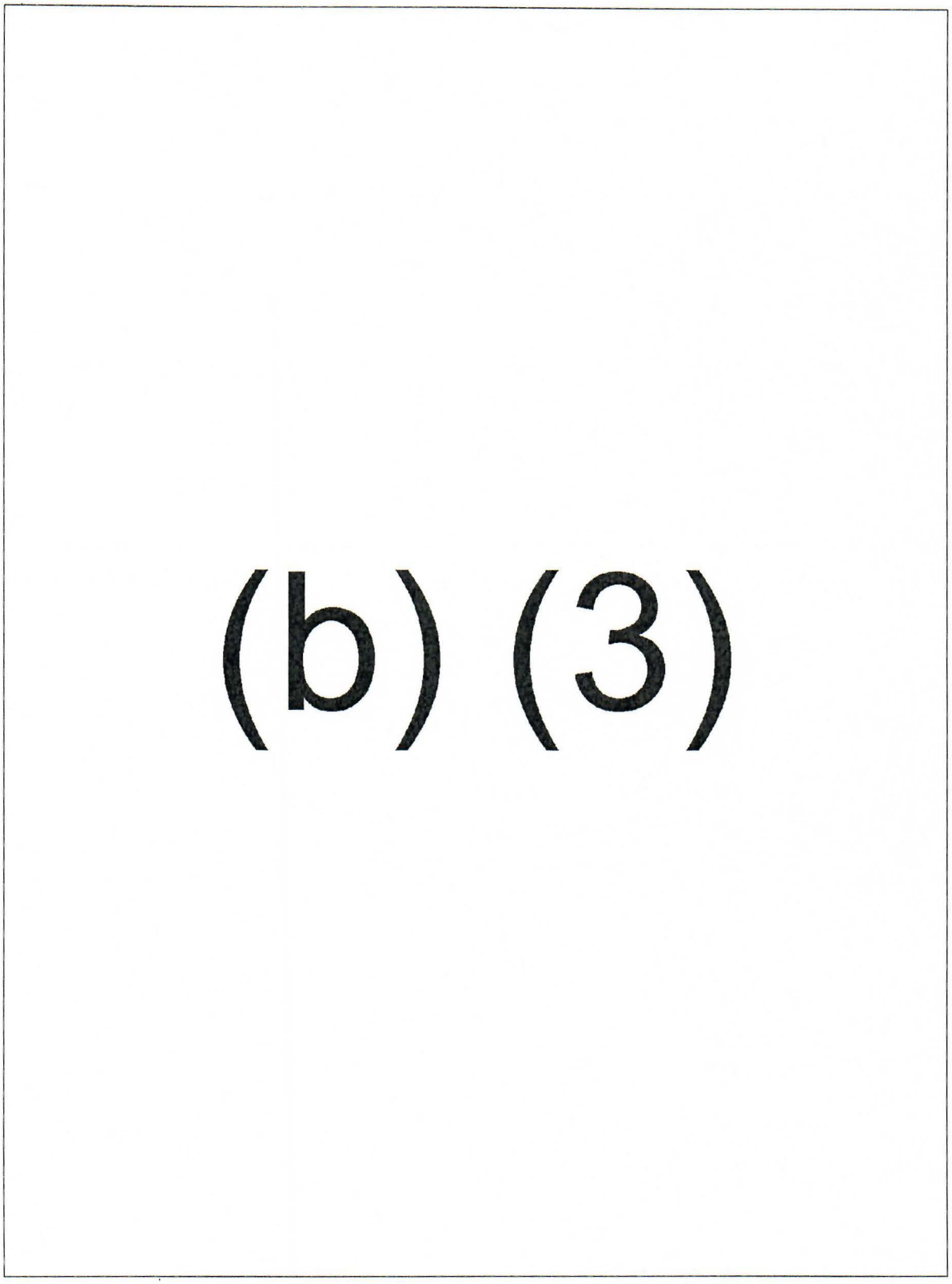
4-11. (U) Utilizing open-source media (the means of sending, receiving, and recording information), components, and associated elements (see table 4-1), OSINT practitioners implement the OSINT collection plan. The following includes the primary media used to implement a collection plan:

(b) (3)

- Public documents.
- Public broadcasts.
- Internet websites.

Note. (U) Table 4-1 does not illustrate an all-inclusive list of open-source media types but rather the categories of open-source media to consider when collecting OSINT.

(b) (3)



~~FOR OFFICIAL USE ONLY~~

Public Documents (U)

4-13. (U) Publicly available documents can be discovered in a variety of places. An OSINT practitioner must comply with all provisions of intelligence oversight when acquiring public documents. Examples of publicly available documents include but are not limited to—

(b) (3)

- Documents from newspaper stands, book stores, and publishers.

Broadcast Services (U)

4-14. (U) Broadcast services refers to the transmission of audio and/or video information in the electromagnetic wave frequency format. OSINT practitioners can obtain broadcast services freely from civilian resellers or from the enterprise. (For information on collecting information from public broadcasts, access the Open Source Enterprise website on NIPRNET.)

Internet Websites (U)

4-15. (U) OSINT practitioners' ability to search the internet safely and securely is an essential skill for collecting open-source information. The internet provides access to websites and databases that hold a wide range of information on current, planned, and potential areas of operations. (See appendix C for more information on using internet websites.)

(b) (3)

4-17. (U) Intelligence professionals directly accessing open-source information to satisfy specific intelligence requirements are conducting an OSINT activity. All OSINT activities must be supported by an officially approved collection plan. An intelligence professional is prohibited from creating or using a personal social media account when conducting OSINT activities and will not create a false persona. Engagement (for example conversing, exchanging information) with individuals or personas is an interactive activity not authorized under OSINT authorities.

This page intentionally left blank.

Chapter 5

Produce (U)

(U) Intelligence professionals produce the intelligence resulting from open sources and integrate it into the larger holdings of intelligence data. OSINT, as with all intelligence disciplines, produces specific products as its contribution to intelligence production. The goal of these products is to provide timely and accurate intelligence that answers an intelligence requirement.

PROCESSING INFORMATION (U)

5-1. (U) During OSINT processing and exploitation, collection is converted and/or reduced to forms that can be readily used by commanders, decision makers at all levels, intelligence analysts, and other consumers. Processing and exploitation include—

- First phase exploitation.
- Data conversion and correlation.
- Document and media translation.
- Reporting of action results to analysis and production elements.

5-2. (U) Processing and exploitation may be federated or performed by the same element that collected the data. Federated exploitation planning is typically conducted during planning based on anticipated single-source analytic throughput. It ensures the appropriate intelligence systems architecture is in place to route the collection to predetermined exploitation nodes. An example of processing and exploitation occurs when the collection is compared and associated with the known state actor. Rather than providing an analyst with an overwhelming amount of information, the analyst only receives the essential facts.

5-3. (U) Open-source information may answer intelligence and information requirements. Based on the type of information and how it was received, it must be processed before being reported and disseminated as finalized OSINT. Personnel convert open-source information into a form suitable for exploitation by—

- Digitizing.
- Transcribing and translating.
- Reviewing.

DIGITIZING (U)

5-4. (U) Documents collected from the internet using enterprise tools and practices do not require digitization. For physical documents, 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 dissemination of a document to external databases and organizations. It also allows the use of machine translation tools to screen documents for keywords, names, and phrases.

TRANSCRIBING AND TRANSLATING (U)

5-5. (U) 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.

~~FOR OFFICIAL USE ONLY~~

5-6. (U) A **translation** is not verbatim but an approximation of the literal and implied meaning of the foreign language. (b) (3) (b) (3) (See paragraphs 3-40 through 3-42 for more information on translation and machine language translation.)

5-7. (U) 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.

REVIEWING (U)

5-8. (U) 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 of processing foreign open-source information. Each transcription and translation undergoes two levels of review:

- **Quality control**—a qualified linguist ensures 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 to use in OSINT production.
- **Quality assurance**—a qualified U.S. linguist or OSINT analyst reviews the transcript or translation to ensure it contains all required information and reads naturally in English. Once reviewed, the completed transcription or translation is saved to internal databases and available for further use.

TYPES OF INTELLIGENCE PRODUCTS (U)

5-9. (U) Personnel engaging in open-source activities typically gather and receive information, conduct collection, and report and disseminate information in accordance with local SOPs. OSINT may be incorporated into any of the following intelligence products:

- **Intelligence estimate** is the appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption (JP 2-0).
- **Intelligence summary** refers to the current assessment of the threat situation and civil considerations. Information and intelligence used to develop the intelligence summary are ultimately applied to develop and update the staff estimate.
- **Intelligence running estimate** details the ability of the intelligence staff to support current and future operations.

5-10. (U) OSINT products may also be categorized by intended use and purpose. Categories can overlap, and some PAI and open-source information can be used in more than one product. (See ADRP 2-0 and *MCDP 2* for information on the types of intelligence products.)

5-11. (U) In addition to contributing to the intelligence products listed in paragraph 5-9, OSINT practitioners also prepare open-source intelligence reports (referred to as OSIRs). This report is a (b)(3) standard template for OSINT serialized reporting, and is a national and defense enterprise standard to monitor, track, and access serialized OSINT reporting. The OSINT summary, like the intelligence summary, does not have an established format. However, the OSINT summary should minimally include translated reports applicable to intelligence requirements and an evaluation of the source of the information.

EVALUATING INFORMATION (U)

5-12. (U) After information translation, collection, and exploitation, OSINT practitioners use indicators, such as volume, velocity, variety, viscosity, vitality, and availability, to evaluate the information. It is important to evaluate the reliability of open-source information to distinguish objective, factual information from biased and deception efforts. The information rating is based on the subjective judgment of the evaluator and the accuracy of the previous information produced by the same source. The types of sources are—

- **Primary source**, which has direct access to the information and conveys the information directly and completely.
- **Secondary source**, which conveys information through intermediary sources using the vernacular and summarizes or paraphrases information.

PRIMARY SOURCE (U)

5-13. (U) A primary source refers to a document, person, or physical object that was sampled during the time under study. These sources are present during an experience or time-period and offer an inside view of a particular event.

SECONDARY SOURCE (U)

5-14. (U) 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.
- Histories.
- Textbooks.
- Criticisms.
- Magazine articles.
- Encyclopedias.
- Commentaries.

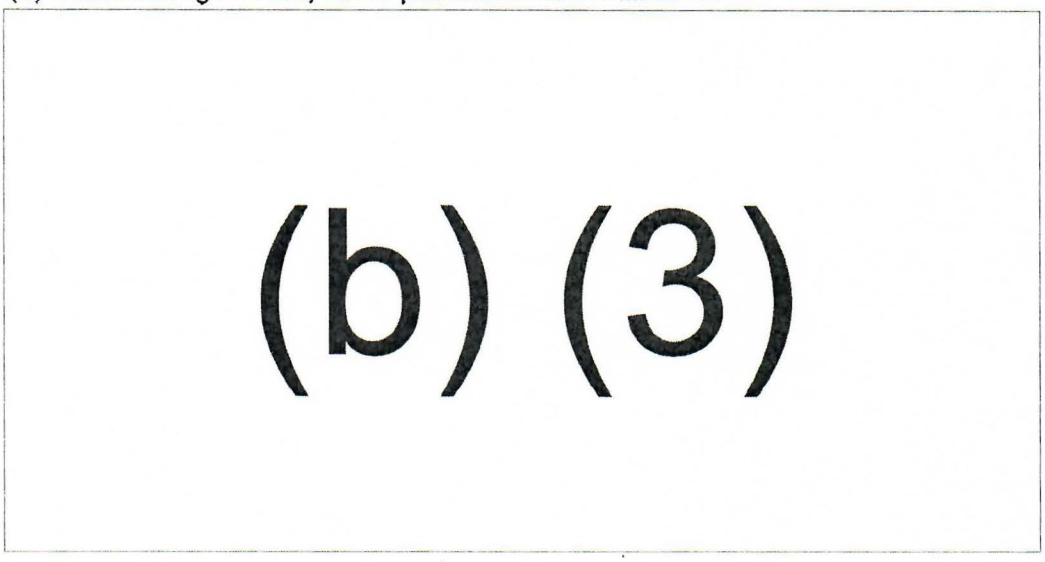
Note. (U) It is often difficult to distinguish primary from secondary sources since both are subjective. A primary source is not necessarily more of an authority or better than a secondary source. For any source, primary or secondary, it is important for OSINT practitioners to evaluate the information for deception and bias.

OPEN-SOURCE RELIABILITY (U)

5-15. (U) To avoid bias, OSINT practitioners must assess the reliability and credibility of information independently. When evaluating sources of information to determine reliability and credibility, analysts consider—

(b) (3)

5-16. (U) When accessing a website, OSINT practitioners should consider the—



~~FOR OFFICIAL USE ONLY~~

Chapter 6

Disseminate (U)

(U) Commanders must receive combat information and intelligence products timely and in an appropriate format to facilitate situational understanding and support decision making. Timely dissemination of intelligence is critical to the success of operations. Effective dissemination is deliberate and ensures consumers receive the intelligence they need to conduct operations.

DISSEMINATION (U)

6-1. (U) Intelligence and information requirements satisfied through open-source information should be reported immediately, as specified in unit SOPs. Reporting and dissemination are not synonymous. The disseminate step does not include the passing of information through normal reporting and technical channels by intelligence organizations and units during the intelligence process. Rather, it involves the passing of products based on intelligence analysis to users requiring that intelligence. (See ADRP 2-0 and *MCDP 2*.)

6-2. (U) OSINT products provided to other intelligence and operational elements facilitate all-source intelligence, targeting, and cueing of other collectors.

Note. (U) Close cooperation between OSINT practitioners and other staff members who collect open-source information fosters a supportive environment about **what** and **how** to report information of potential operational or intelligence value through the proper channels.

6-3. (U) OSINT must be timely, accurate, and properly disseminated to commanders and other customers in a useable form. Disseminating OSINT products includes but is not limited to incorporating the products into—

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

DISSEMINATION METHODS AND TECHNIQUES (U)

6-4. (U) There are numerous methods and techniques for disseminating information and intelligence. The appropriate technique in any particular situation depends on many factors such as capabilities and mission requirements. Information and intelligence must be disseminated in accordance with unit SOPs and joint force guidelines. Dissemination methods and techniques include—

- Direct electronic dissemination (a messaging program).
- Instant messaging.
- Web posting (with notification procedures for users).
- Recording information on removable media and sending it via a secure mail service.
- Recording information on removable media and sending it via electronic means.
- Sending hardcopy documents via mail or fax.

~~FOR OFFICIAL USE ONLY~~

6-5. (U) The basic standards for reporting and disseminating information are—

- **Timeliness.** Information should be reported to affected units without being delayed for the sole purpose of ensuring the correct format.
- **Relevance.** Information must contribute to answering intelligence requirements. Relevant information reduces collection, organization, and transmission times.
- **Completeness.** Using prescribed formats and following SOPs contribute to the completeness of transmitted information.

REPORTING METHODS (U)

6-6. (U) The three reporting methods used to convey intelligence and information are—

- **Written.** Written methods include formats (such as spot reports), tactical reports, and information intelligence reports. OSINT publications, while not having an established format, should also provide analysis of the sources discussed. These assessments can assist in evaluating the reliability of the information.
- **Graphic.** Web-based report dissemination is an effective technique to ensure the widest awareness of written and graphical information across echelons. OSINT practitioners can collaborate and provide statuses of intelligence requirements through websites. Information can also be uploaded to various databases to support future open-source missions and operations. Graphics should also display, if from a local source, the areas that the information impacts. For instance, a newspaper written in Quetta, Pakistan, will have a higher distribution amongst the Pashtun population than it would in a highly populated Tajiki area of Afghanistan.
- **Verbal or 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 communications methods are the most efficient to deliver information to commanders.

~~FOR OFFICIAL USE ONLY~~

Appendix A

Legal Restrictions and Regulatory Limitations (U)

(U) Open-source information covers a wide range of areas. Exploring, assessing, and collecting PAI and information from open sources has the potential to adversely affect organizations that conduct OSINT missions. As with all intelligence activities, OSINT activities must comply with intelligence oversight law, policy, and regulation. For the Army, the AOO, in coordination with the U.S. Army Forces Command, ensures intelligence collection authority and appropriate mission orders are documented for U.S. Army Forces Command units provisioned with AOO OSINT capabilities.

Note. (U) EOs, Army regulations, *Marine Corps policies*, and guidance change frequently. Appendix A discusses the legal restrictions and regulatory limitations at the time of this writing. It is imperative that readers ensure adherence to the most recent laws and regulations.

EXECUTIVE ORDER 12333 (U)

A-1. (U) All OSINT activities performed by intelligence personnel must comply with the legal restrictions, policies, and guidelines outlined in EO 12333 as amended and other associated regulations, instructions, or directives.

A-2. (U) EO 12333 as amended was implemented in response to operations and activities conducted by the intelligence community against U.S. persons, especially those involved in civil rights and anti-Vietnam war movements during the 1960s and 1970s. At that time, intelligence personnel, including DOD intelligence personnel, used overt and covert means to collect information on political activities of U.S. persons, retained that information in intelligence files, and disseminated that information to other intelligence and law enforcement organizations. The purpose of EO 12333 as amended is to enhance—

- Human and technical collection techniques, especially those undertaken abroad.
- The acquisition of significant foreign intelligence.
- Detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers.

A-3. (U) EO 12333 as amended is also intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. 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 consistent with the U.S. Constitution and applicable laws and principles.

ASSIGNED FUNCTIONS (U)

A-4. (U) Based on EO 12333 as amended, the assigned intelligence functions of the Army are to—

- Collect, produce, and disseminate defense and defense-related foreign intelligence and counterintelligence to support Army and DOD requirements, and as appropriate, national requirements.
- Conduct counterintelligence activities.

~~FOR OFFICIAL USE ONLY~~

- Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities.
- Conduct MI liaison relationships and MI exchange programs.

INTERPRETATION AND IMPLEMENTATION (U)

A-5. (U) AR 381-10 and *MCO 3800.2B* interpret and implement EO 12333 as amended and DOD 5240.1-R. DODM 5240.01 is the most current guidance on intelligence oversight. AR 381-10 and DODM 5240.01 enable the Army intelligence community to perform authorized intelligence functions in a manner that protects the constitutional rights of U.S. persons. However, the regulation does not authorize intelligence activity. An Army intelligence unit or organization must have the mission and the authority to conduct any intelligence activity, and particularly those directed against U.S. persons. Army intelligence personnel operating under the authority of Title 10, USC, or Title 50, USC, must comply with the Posse Comitatus Act (Section 1385, Title 18, USC) and have prior approval by the Secretary of Defense when involved with civilian law enforcement.

U.S. PERSON INFORMATION (U)

A-6. (U) Army intelligence personnel will conduct OSINT activities in accordance with the requirements of EO 12333 as amended, DODM 5240.01, and AR 381-10 in a manner that ensures legality and propriety, and preserves and respects the privacy and civil liberties of U.S. persons. All Army intelligence personnel conducting OSINT activities will complete intelligence oversight training as required in DOD 5240.1-R and AR 381-10. For OSINT collection purposes, U.S. person information may only be retained if the information is reasonably believed to be necessary for the performance of an authorized OSINT mission and the information is publicly available. If, during authorized OSINT collection, U.S. person information is incidentally collected (it was not the target of the OSINT collection), all such information may be temporarily retained, evaluated for permanent retention, and disseminated only in accordance with DODM 5240.01, Procedures 3 and 4, and AR 381-10.

ARMY REGULATION 381-10 (U)

A-7. (U) AR 381-10 requires any Army component performing authorized intelligence functions to execute those 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 counterintelligence purposes. This regulation does not authorize specific intelligence activity.

COLLECTION OF U.S. PERSON INFORMATION (U)

A-8. (U) In accordance with AR 381-10, a **U.S. person** is—

- 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.

A-9. (U) The following are presumed to be non-U.S. persons unless the intelligence component obtains specific information to the contrary:

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

A-10. (U) **Collection**, in accordance with DODM 5240.01, concerns information that is received by a Defense Intelligence Component, whether or not it is retained by the Component for intelligence purposes or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the Component. Collected information does not include—

~~FOR OFFICIAL USE ONLY~~

- Information that only temporarily passes through a computer system of the Component.
- Information on the internet or in an electronic forum or repository outside the Component that is simply viewed or accessed by a Component employee but is not copied, saved, supplemented, or used in some manner.
- Information disseminated by other Components or elements of the Intelligence Community.
- Information that is maintained on behalf of another U.S. Government agency and to which the Component does not have access for intelligence purposes.

A-11. (U) Action must be taken to demonstrate the intended use of the collected information, such as producing an intelligence information report, incident report, or adding the information to an intelligence database. 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 PAI, open-source information, and information data exploitation.

A-12. (U) Army intelligence components may collect U.S. person information by lawful means; however, collection must be limited to the least intrusive means feasible and shall not violate the law. (See DODM 5240.01.) The least intrusive means must be attempted before requesting or utilizing more intrusive collection means. (b) (3)

- (b) (3)

A-13. (U) Within the United States, foreign intelligence concerning U.S. persons may be collected only by overt means, unless all of the following conditions are met:

- (b) (3)

A-14. (U) 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. The rules in EO 12333 as amended and AR 381-10 protect U.S. persons' rights under the First Amendment to the Constitution of the United States.

RETENTION OF U.S. PERSON INFORMATION (U)

A-15. (U) In this context, **retention** is the maintenance of information in either hardcopy or electronic format regardless of how the information was collected or how it was disseminated to a Defense Intelligence Component by another Component or element of the Intelligence Community (DODM 5240.01). DODM 5240.01, Procedure 3, authorizes the retention of U.S. person information.

A-16. (U) In accordance with DODM 5240.01, **incidental collection of U.S. person information** refers to—

(a) Collection about a person reasonably believed to be in the United States. A defense intelligence component may intentionally collect information about a person or object that, at the time of collection, is in the United States or about a place in the United States. If a component does so and incidentally may have collected U.S. person information about a person other than the subject of intentional collection, the component may retain all of the collected information for evaluation for up to five years. The component head or a single delegee may approve an extended period in accordance with Paragraph 3.3.c.(5).

~~FOR OFFICIAL USE ONLY~~

(b) Collection about a person reasonably believed to be outside the United States. A defense intelligence component may intentionally collect information about a person or object that, at the time of collection, is outside the United States or about a place outside the United States. If a component does so and incidentally may have collected U.S. person information about a person other than the subject of intentional collection, the component may, subject to Paragraph 3.3.c.(5)(b), retain all of the incidentally collected information for evaluation for up to 25 years.

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

A-18. (U) 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 the 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 (U)

A-19. (U) In this context, **dissemination** is the transmission, communication, sharing, or passing of information outside a Defense Intelligence Component by any means, including oral, electronic, or physical means. Dissemination includes providing any access to information in a Component's custody to persons outside the Component (DODM 5240.01).

(b) (3)

QUESTIONABLE INTELLIGENCE ACTIVITY (U)

A-20. (U) Questionable intelligence activity occurs when intelligence operations (in this context, all intelligence or counterintelligence tasks) potentially violate laws, EOs, Presidential directives, and DOD or Army policies.

A-21. (U) 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 regarding 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. (U) 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 staff judge advocate's office. (For more information on EO 12333 as amended and intelligence oversight, access the DOD Senior Intelligence Oversight Official website on NIPRNET.)

~~FOR OFFICIAL USE ONLY~~

MARINE CORPS ORDER 3800.2B (U)

A-23. (U) MCO 3800.2B establishes policy, procedures, and responsibilities governing the inspection and oversight of activities of Marine Corps intelligence and the reporting requirements regarding those activities.

COLLECTION, RETENTION, AND DISSEMINATION OF U.S. PERSON INFORMATION (U)

A-24. (U) The collection, retention, and dissemination of information concerning U.S. persons by Marine Corps intelligence components will be governed by the requirements set forth in references EO 12333 as amended, DODM 5240.01, DOD 5240.1-R change 1, SECNAVINST 3820.3E, and MCO 3800.2B.

A-25. (U) MCO 3800.2B defines a ***U.S. person*** *as one of the following—*

- *A citizen of the United States.*
- *An alien known by the intelligence agency concerned to be a permanent resident alien.*
- *An unincorporated association substantially composed of U.S. citizens or permanent resident aliens.*
- *A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.*

A-26. (U) Marine Corps intelligence activities shall be carried out in a manner that protects the constitutional rights and privacy of U.S. persons, and shall not request any person or entity to undertake unauthorized activities.

A-27. (U) Marine Corps intelligence units and staffs can collect, retain, and disseminate intelligence on U.S. persons, provided they adhere to a very specific set of criteria and restrictions. Information that identifies a U.S. person may be collected by a Marine Corps intelligence component only if it—

(1) Is necessary to the conduct of a function assigned to the collecting component.

(2) Falls within one of the 13 categories authorized under DODM 5240.01. Extracts of information categories are provided in MCO 3800.2B, Enclosure (2).

A-28. (U) Collection techniques authorized by DODM 5240.01 will be limited to those necessary to perform assigned functions. The least intrusive means of collection will always be the preferred collection method.

A-29. (U) Special considerations exist for intelligence support to command antiterrorism/force protection programs within U.S. territory and/or involving information regarding U.S. persons. DODM 5240.01 provides specific guidance.

A-30. (U) Intelligence training, or support to unit training, in an off-base domestic civilian environment demands due diligence to ensure that not only intelligence personnel but also other key personnel (for example commanders, controllers, or nonintelligence Marines who may be conducting intelligence activities) are aware of intelligence oversight provisions. Specific guidance is provided in MCO 3800.2B, Enclosure (4).

A-31. (U) Use of the internet by intelligence components to conduct intelligence activities presents unique challenges beyond traditional collection methods. To maximize the use of the internet while properly applying the provisions of EO 12333 as amended, intelligence personnel must understand how to analyze, as well as characterize, information collected via the internet. The DOD Office of General Council (known as OCG) memo, "Principles Governing the Collection of Internet Addresses by DOD Intelligence and Counterintelligence Components," dated 06 February 2001, addresses internet-based collection activity against the network (as opposed to network content). Commanders can access the memo on the Inspector General of the Marine Corps website on NIPRNET.

QUESTIONABLE INTELLIGENCE ACTIVITY (U)

A-32. (U) MCO 3800.2B defines **questionable activity** as any conduct that constitutes, or is related to, an intelligence activity that may violate U.S. laws, statutes, Executive Orders, Presidential directives, applicable Department of Defense directives, and Department of the Navy or other Services' policies.

This page intentionally left blank.

Appendix B

Security Awareness (U)

(U) Personnel conducting open-source collection must be aware of the digital operational environment by minimizing and reducing digital footprints, practicing effective OPSEC, using safe online browsing techniques and habits, and understanding that embedded metadata can be contained in documents.

SITUATIONAL AWARENESS AND SECURITY (U)

B-1. (U) Awareness is the beginning of effective security. When searching the internet, a computer will transmit machine identification data to the site being visited. (Machine identification data may include the operating system, version type of each enabled program, security levels, a history of websites visited, cookie information, user preferences, internet protocol [IP] addresses, enabled languages, and the referring uniform resource locater [URL].) Visitors are frequently redirected to alternative websites based on the search criterion, location, language, and time the search is conducted.

B-2. (U) Collection involving open-source information could unintentionally reveal PIRs. The internet is a network of networks. It encompasses 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 identifies the address where transferred information and data are delivered. Therefore, by visiting nonstandard or questionable internet websites on U.S. Government computers, sensitive unit information could inadvertently be revealed.

B-3. (U) There are OPSEC and computer security risks to searching and interacting with internet websites. Searching the internet may compromise the intelligence mission by leaving machine data (also called digital footprints) on visited websites. Browsing internet websites 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 OPSEC measures.

(b) (3)

B-5. (U) URL information from the previous website visited is frequently an OPSEC issue because it identifies the user's characteristics and interests. While necessary, the use of specific and focused search terms also has potential OPSEC implications. For example, If the user enters the search terms [bradley us army], the referring URL from the search engine would be: http://www.[search engine name].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.

~~FOR OFFICIAL USE ONLY~~

B-6. (U) All actions on a website are logged and saved. The information is saved and linked to what is referred to as cookie data. User actions recorded include but are not limited to—

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

B-7. (U) On many websites, information that users provide or fill in becomes part of the website 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-8. ~~(FOUO)~~ Threats, such as regular, irregular, terrorist forces, and criminal elements, are disruptive and use cyberspace to execute operations against the Army. Often, these threats are innovative, networked, and technologically adept. They capitalize on emerging technologies to establish and maintain a cultural and social advantage, leveraging areas that include but are not limited to mission command, recruiting, logistics, fund raising, money laundering, information operations, and propaganda.

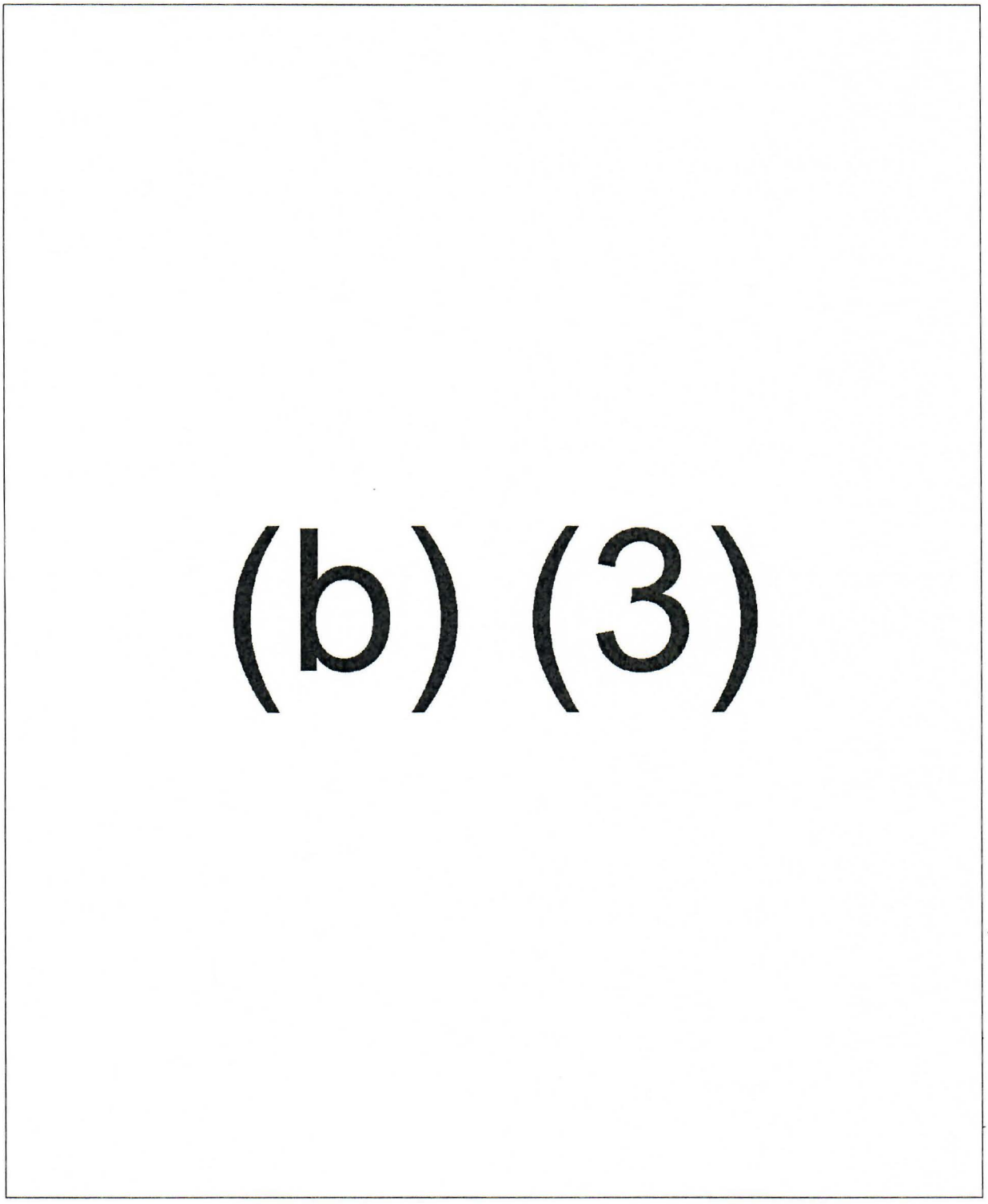
B-9. (U) Units engaged in OSINT exploitation using computer systems and internet usage should develop cyberspace awareness assessments. These assessments should cover areas including but not limited to network vulnerabilities, network threats (physical and virtual), and future risks. For information about—

- Cybersecurity awareness, access the U.S. Army Cyber Command website on NIPRNET.
- Cybersecurity threats and tips, access the U.S. Computer Emergency Readiness Team's website on NIPRNET.
- Threat and vulnerability assessments and counterintelligence-cyber elements that perform internet open-source collection and provide support to DOD and Army network and system analysis to determine OPSEC vulnerabilities, see ATP 2-22.2-1.

SECURE WEB BROWSING (U)

B-10. (U) Oftentimes, information on U.S. Government networks is insufficient to answer intelligence requirements. Intelligence professionals must conduct OPSEC risk mitigation and use secure web browsing capabilities to protect information requirements, information gaps, and/or collection activities from adversaries and threats.

B-11. (U) A best practice for intelligence professionals using the internet is to use a U.S. Government-assigned computer with secured protocols. Army units with a requirement to conduct secure web browsing on the internet to support intelligence requirements or activities should contact the AOO to obtain training on and access to the approved enterprise capabilities.



~~FOR OFFICIAL USE ONLY~~

(b) (3)

~~FOR OFFICIAL USE ONLY~~

(b) (3)

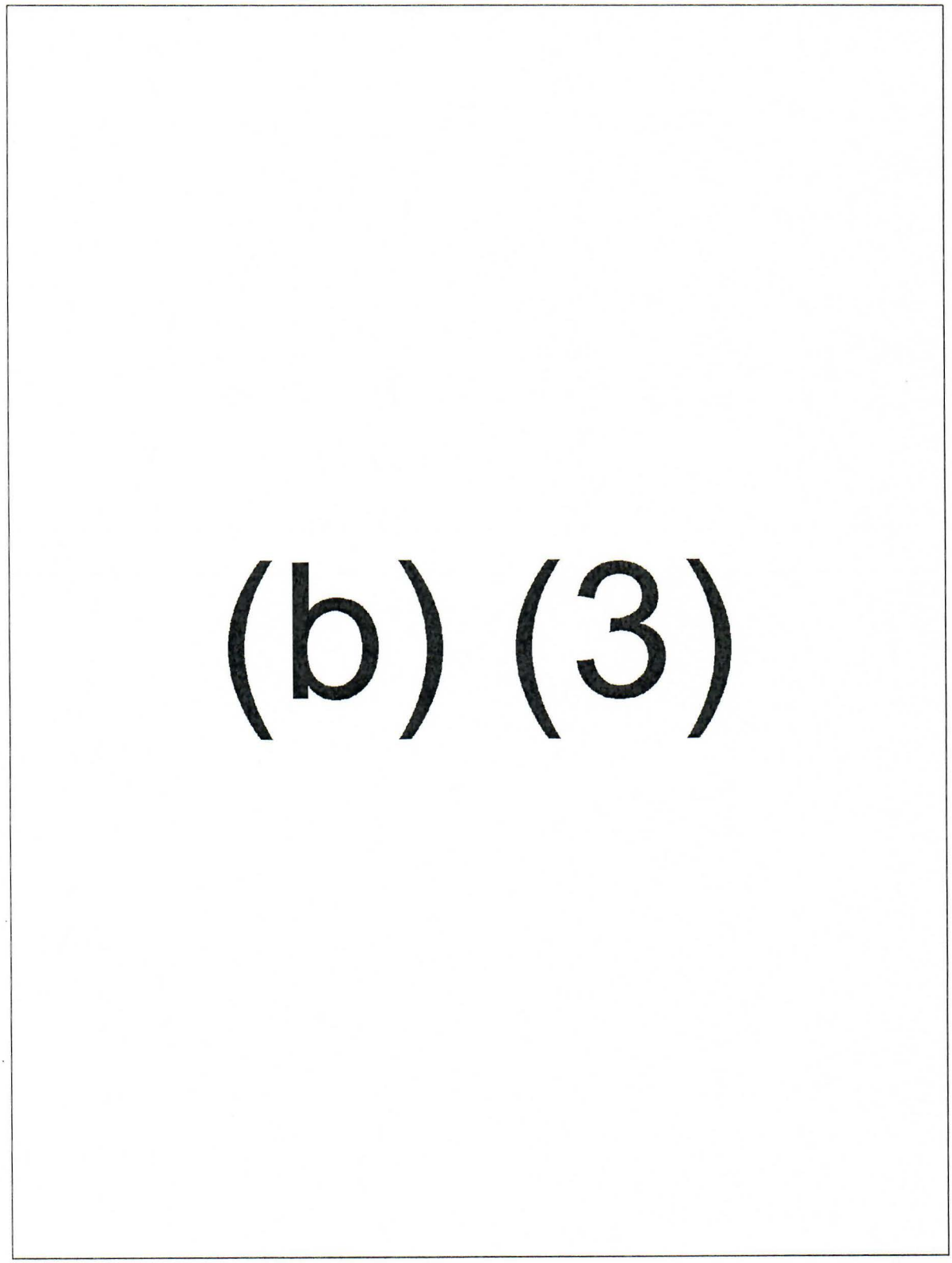
~~FOR OFFICIAL USE ONLY~~

(b) (3)

~~FOR OFFICIAL USE ONLY~~

(b) (3)

~~FOR OFFICIAL USE ONLY~~



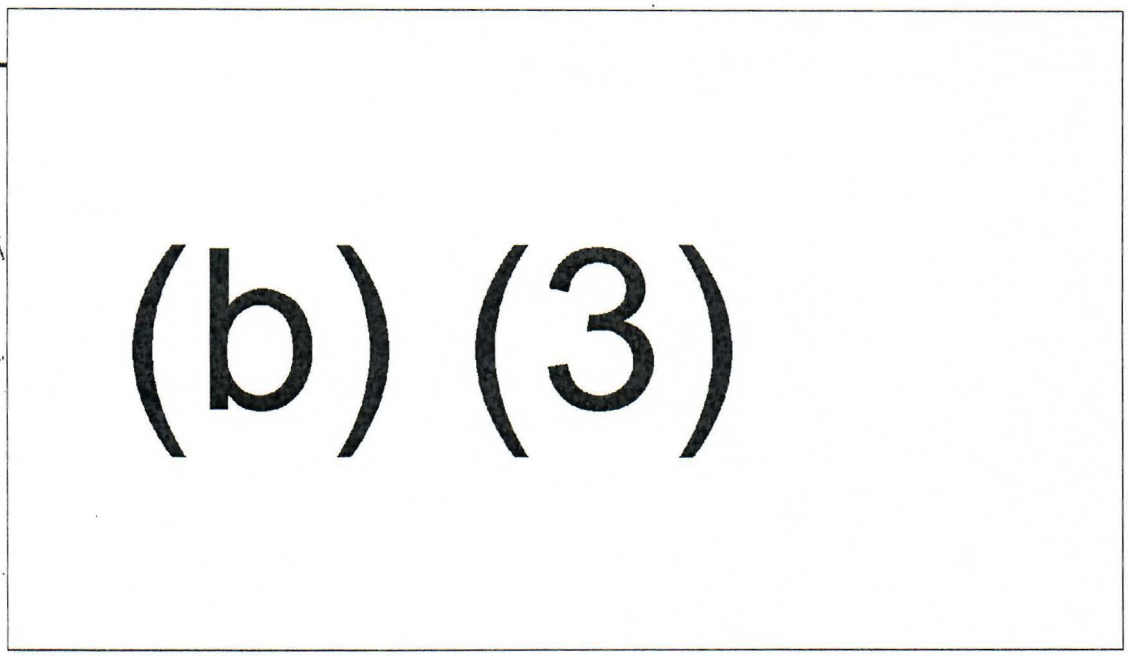
~~FOR OFFICIAL USE ONLY~~

(b) (3)

~~FOR OFFICIAL USE ONLY~~

(b) (3)

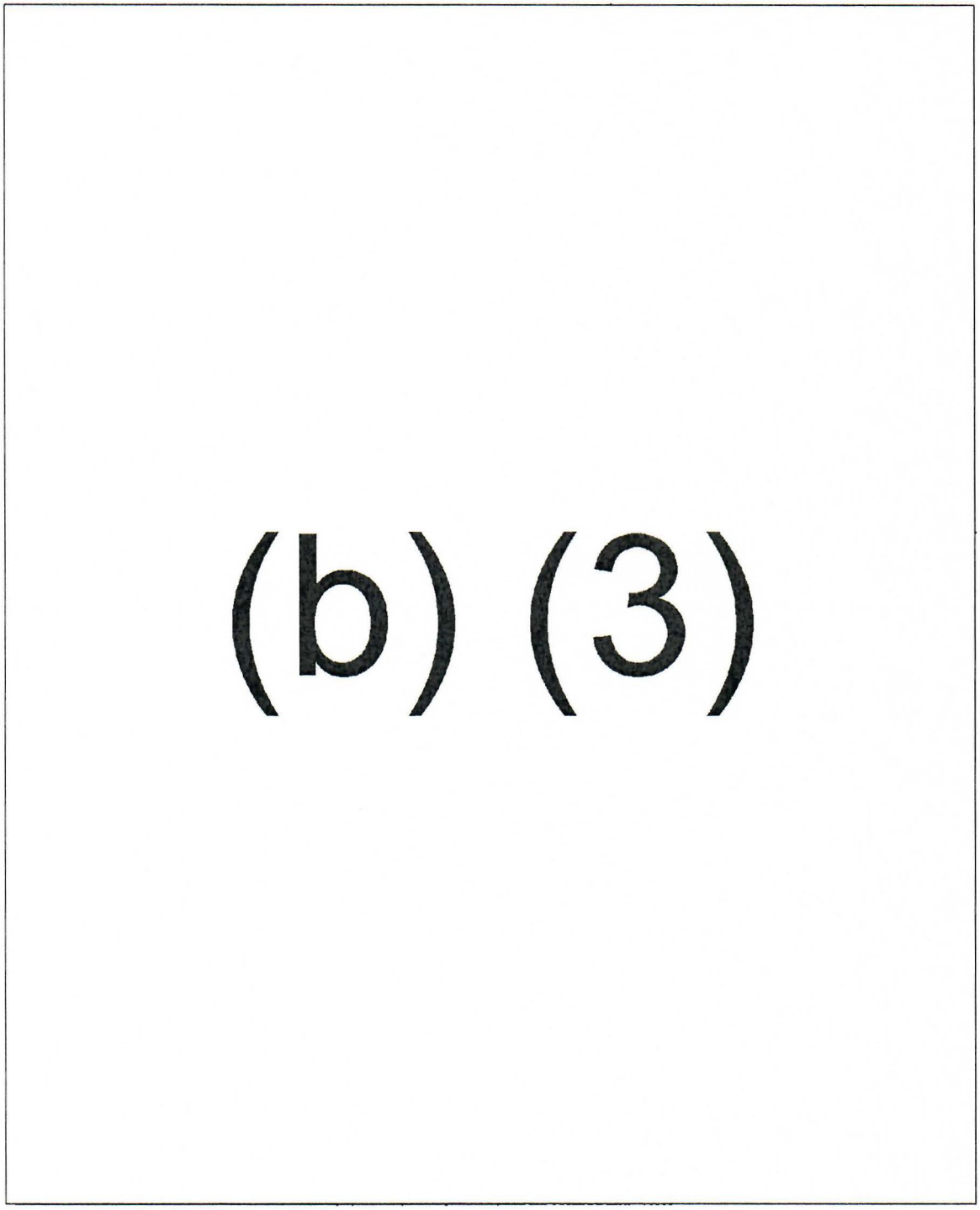
~~FOR OFFICIAL USE ONLY~~



~~FOR OFFICIAL USE ONLY~~

This page intentionally left blank.

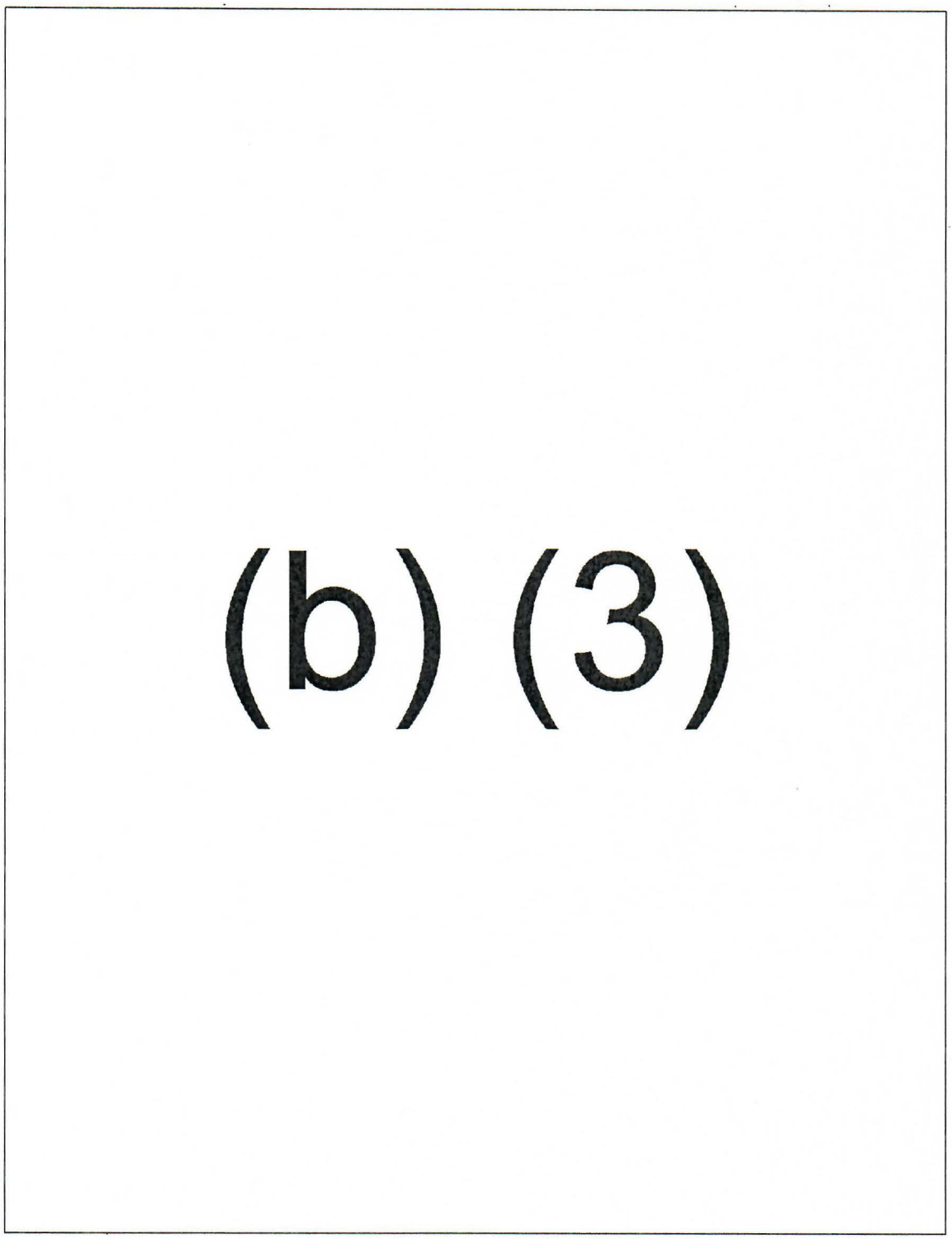
Appendix D



~~FOR OFFICIAL USE ONLY~~

(b) (3)

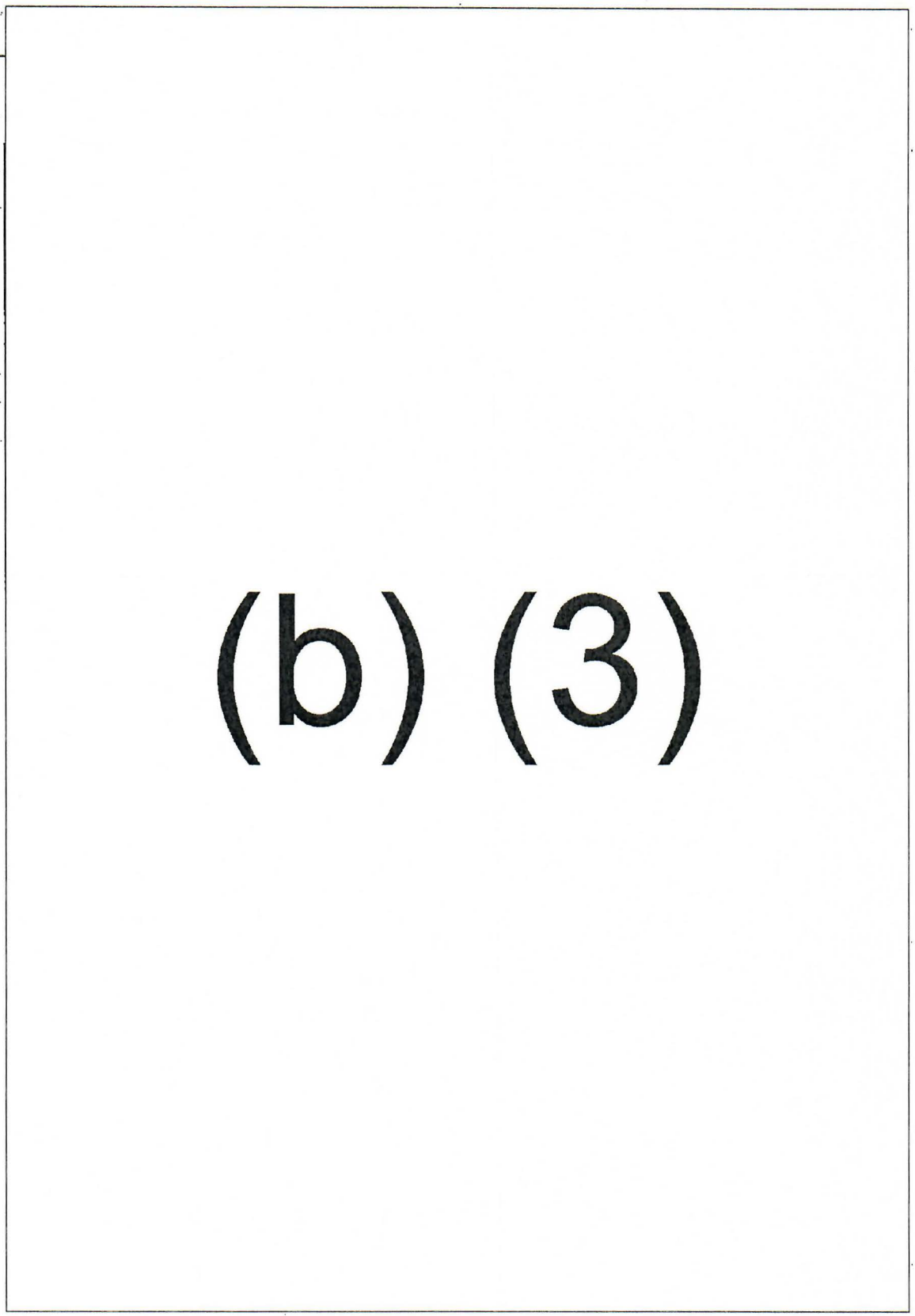
~~FOR OFFICIAL USE ONLY~~



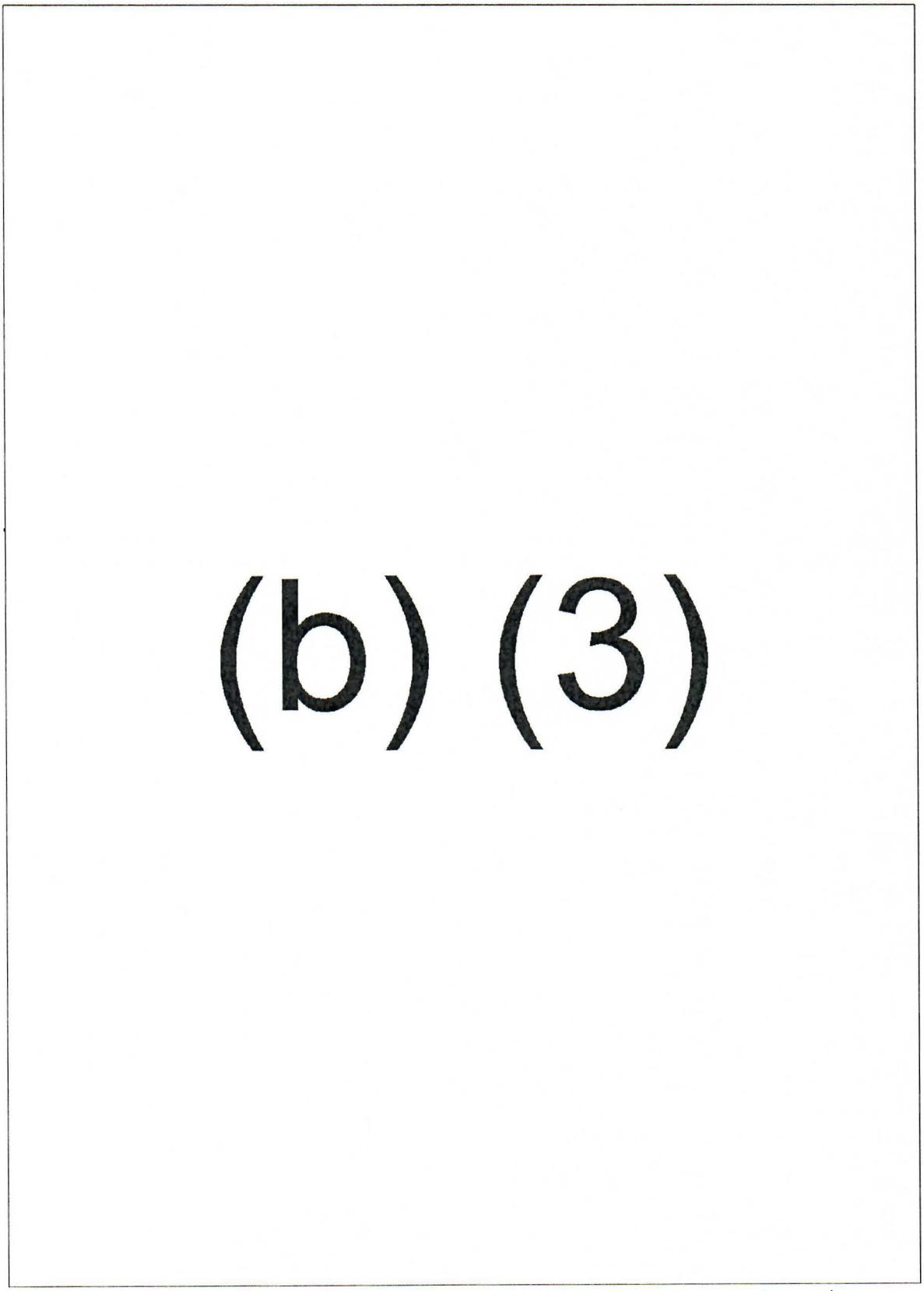
~~FOR OFFICIAL USE ONLY~~

(b) (3)

~~FOR OFFICIAL USE ONLY~~



~~FOR OFFICIAL USE ONLY~~



~~FOR OFFICIAL USE ONLY~~

(b) (3)

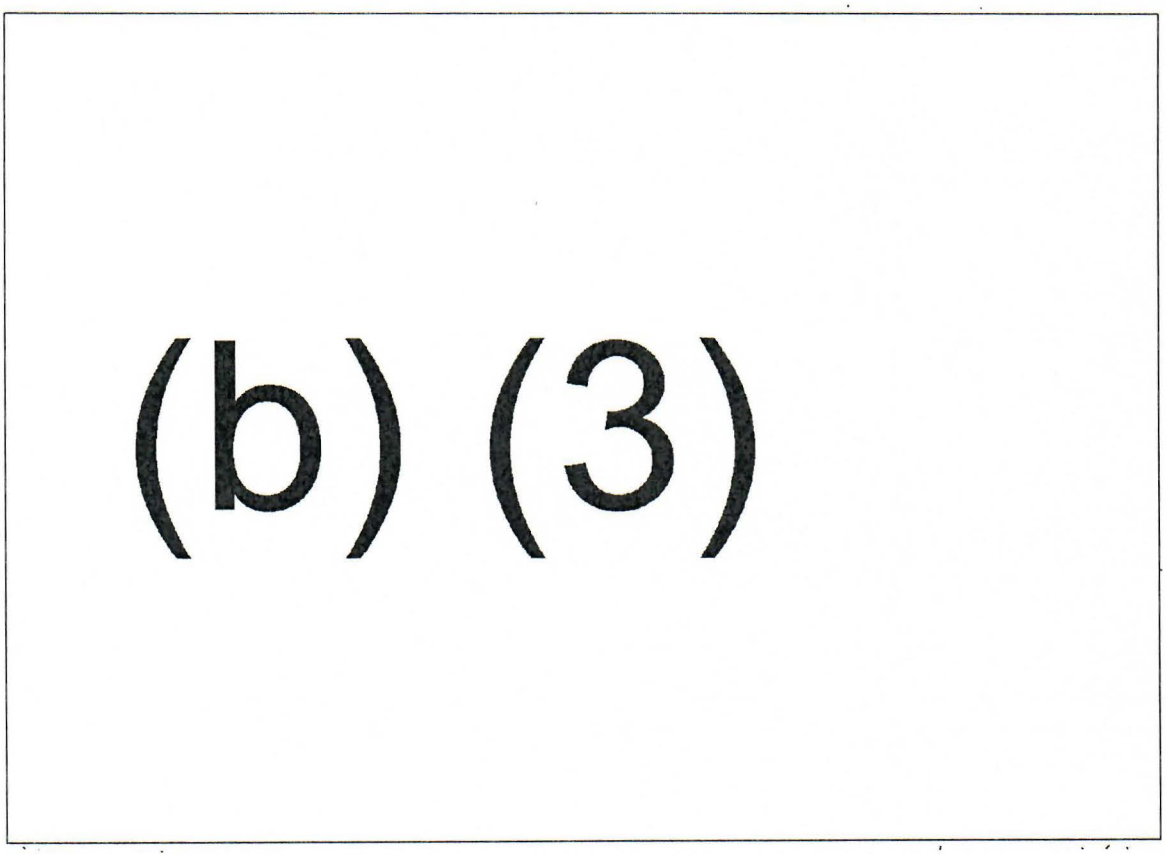
~~FOR OFFICIAL USE ONLY~~

(b) (3)

~~FOR OFFICIAL USE ONLY~~

(b) (3)

~~FOR OFFICIAL USE ONLY~~



~~FOR OFFICIAL USE ONLY~~

Glossary (U)

(U) For Army terms and definitions, (Army) precedes the definition. For *Marine Corps* terms and definitions, *(Marine Corps)* precedes the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS (U)

ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AOO	Army Open-Source Intelligence (OSINT) Office
AR	Army regulation
ATP	Army techniques publication
BCT	brigade combat team
CCIR	commander's critical information requirement
COA	course of action
DA IIS	Department of the Army Intelligence Information Service
DCGS-A	Distributed Common Ground System-Army
DIA	Defense Intelligence Agency
DOD	Department of Defense
DODI	Department of Defense instruction
DODM	Department of Defense manual
DOSC	Defense Open-Source Council
EO	executive order
FM	field manual
G-2	intelligence staff officer (Army)
G-2/S-2/R-2	intelligence staff section (Army)
G-6	signal staff officer (Army)
INSCOM	United States Army Intelligence and Security Command
IP	internet protocol
IPB	intelligence preparation of the battlefield (Army)/*intelligence preparation of the battlespace (Marine Corps)*
JP	joint publication
MAGTF	*Marine Corps air-ground task force (Marine Corps)*
MCDP	*Marine Corps doctrinal publication (Marine Corps)*
MCIA	*Marine Corps Intelligence Activity (Marine Corps)*
MCO	*Marine Corps order (Marine Corps)*
MCPP	*Marine Corps planning process (Marine Corps)*
MCRP	*Marine Corps reference publication (Marine Corps)*

~~FOR OFFICIAL USE ONLY~~

MCTP	*Marine Corps training publication (Marine Corps)*
MCWP	*Marine Corps warfighting publication (Marine Corps)*
MDMP	military decision-making process (Army)
METT-T	*mission, enemy, terrain and weather, troops and support available–time available (Marine Corps)*
METT-TC	mission, enemy, terrain and weather, troops and support available–time available and civil considerations (mission variables) (Army)
MI	military intelligence
MIC	*Marine Corps air-ground task force (MAGTF) intelligence center (Marine Corps)*
MSC	*major subordinate command (Marine Corps)*
NIPRNET	Nonsecure Internet Protocol Router Network
NOSC	National Open-Source Committee
OPSEC	operations security
	(b) (3)
OSINT	open-source intelligence
PAI	publicly available information
PED	processing, exploitation, and dissemination
PIR	priority intelligence requirement
PMESII	*political, military, economic, social, information, and infrastructure (Marine Corps)*
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time (operational variables) (Army)
RFI	request for information
SECNAVINST	Secretary of the Navy instruction
SOP	standard operating procedure
URL	uniform resource locater
U.S.	United States
USC	United States Code

SECTION II – TERMS (U)

collection (U)

(U) (DOD) Information is collected when it is received by a Defense Intelligence Component, whether or not it is retained by the Component for intelligence purposes or other purposes. Collected information includes information obtained or acquired by any means, including information that is volunteered to the Component. Collected information does not include: information that only momentarily passes through a computer system of the Component; information on the Internet or in an electronic forum or repository outside the Component that is simply viewed or accessed by a Component employee but is not copied, saved, supplemented, or used in some manner; information disseminated by other Components or elements of the Intelligence Community; or information that is maintained on behalf of another U.S. Government agency and to which the Component does not have access for intelligence purposes. (DODM 5240.01)

~~FOR OFFICIAL USE ONLY~~

commander's critical information requirement (U)

(U) (joint) An information requirement identified by the commander as being critical to facilitating timely decision making. (JP 3-0)

cyberspace (U)

(U) (joint) A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12[R])

dissemination (U)

(U) (DOD) The transmission, communication, sharing, or passing of information outside a Defense Intelligence Component by any means, including oral, electronic, or physical means. Dissemination includes providing any access to information in a Component's custody to persons outside the Component. (DODM 5240.01)

friendly force information requirement (U)

(U) (joint) Information the commander and staff need to understand the status of friendly force and supporting capabilities. (JP 3-0)

intelligence (U)

(U) (joint) 1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities. (JP 2-0)
(U) (Marine Corps) Knowledge about the enemy or the surrounding environment needed to support decision making. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. Intelligence is one of the six warfighting functions. (MCRP 1-10.2)

intelligence estimate (U)

(U) (joint) The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 2-0)

intelligence preparation of the battlefield (U)

(U) (Army) The systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. (ATP 2-01.3)

intelligence preparation of the battlespace (U)

(U) (Marine Corps) The systematic, continuous process of analyzing the threat and environment in a specific geographic area. (MCRP 2-10B.1)

intelligence reach (U)

(U) (Army) The activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command. (ADRP 2-0)

intelligence warfighting function (U)

(U) (Army) The related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment. (ADRP 3-0)

~~FOR OFFICIAL USE ONLY~~

Marine Corps planning process (U)

(U) (Marine Corps) A six-step methodology which helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the mission and the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of problem framing, course of action development, course of action war game, course of action comparison and decision, orders development, and transition. (MCRP 1-10.2)

military decision-making process (U)

(U) (Army) An interactive planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. (ADP 5-0)

open-source information (U)

(U) (joint) Information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access. (JP 2-0)

open-source intelligence (U)

(U) (DOD) Intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (Public Law 109-163)

priority intelligence requirement (U)

(U) (joint) An intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or other aspects of the operational environment. (JP 2-01)

publicly available information (U)

(U) (DOD) Information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public. (DODM 5240.01)

questionable activity (U)

(U) (Marine Corps) Any conduct that constitutes, or is related to, an intelligence activity that may violate U.S. laws, statutes, Executive Orders, Presidential directives, applicable Department of Defense directives, and Department of the Navy or other Services' policies. (MCO 3800.2B)

retention (U)

(U) (DOD) The maintenance of information in either hardcopy or electronic format regardless of how the information was collected or how it was disseminated to a Defense Intelligence Component by another Component or element of the Intelligence Community. (DODM 5240.01)

U.S. person (U)

(U) (Army) A U.S. citizen; an alien known by the intelligence component to be a 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. A corporation or a subsidiary incorporated abroad is not a U.S. person even if partially or wholly owned by a corporation incorporated in the United States. (AR 381-10)
(U) (Marine Corps) A citizen of the United States; an alien known by the intelligence agency concerned to be a permanent resident alien; an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. (MCO 3800.2B)

~~FOR OFFICIAL USE ONLY~~

References (U)

(U) All URLs accessed on 15 June 2017.

REQUIRED PUBLICATIONS (U)

(U) These sources must be available to intended users of this publication.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS (U)

(U) Most joint publications are available online: www.dtic.mil/doctrine/new_pubs/jointpub.htm.

(U) Most DOD publications are available at the DOD Issuances website: www.dtic.mil/whs/directives.

(U) DOD 5240.1-R. *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Personnel*. 07 December 1982.

(U) *DOD Dictionary of Military and Associated Terms*. May 2017.

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

(U) DODM 5240.01. *Procedures Governing the Conduct of DOD Intelligence Activities*. 08 August 2016.

(U) JP 2-0. *Joint Intelligence*. 22 October 2013.

ARMY PUBLICATIONS (U)

(U) Most Army doctrinal publications are available online: www.apd.army.mil.

(U) ADRP 1-02. *Terms and Military Symbols*. 16 November 2016.

(U) AR 381-10. *U.S. Army Intelligence Activities*. 03 May 2007.

(U) U.S. Army Directive 2016-37. *U.S. Army Open-Source Intelligence Activities*. 22 November 2016.

MARINE CORPS PUBLICATIONS (U)

(U) Most Marine Corps doctrinal publications are available online: https://doctrine.usmc.mil/.

(U) Most MCOs are available online: http://www.marines.mil/News/Publications/ELECTRONIC-LIBRARY.aspx.

(U) MCO 3800.2B. Oversight of Intelligence Activities. 30 April 2004.

(U) MCRP 1-10.2. Marine Corps Supplement to the DOD Dictionary of Military and Associated Terms. 16 November 2011.

OTHER PUBLICATIONS (U)

(U) EO 12333. *United States Intelligence Activities*. 4 December 1981. Amended by EO 13284 (2003) and 13470 (2008). Available online: http://www.archives.gov/federal-register/codification/executive-order/12333.html.

~~FOR OFFICIAL USE ONLY~~

RELATED PUBLICATIONS (U)

(U) These sources contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS (U)

(U) Most joint publications are available online: www.dtic.mil/doctrine/new_pubs/jointpub.htm.

(U) Most DOD publications are available at the DOD Issuances website: www.dtic.mil/whs/directives.

(U) JP 2-01. *Joint and National Intelligence Support to Military Operations*. 05 January 2012.

(U) JP 3-0. *Joint Operations*. 17 January 2017.

(U) JP 3-12(R). *Cyberspace Operations*. 05 February 2013.

ARMY PUBLICATIONS (U)

(U) Most Army doctrinal publications are available online: www.apd.army.mil.

(U) ADP 5-0. *The Operations Process*. 17 May 2012.

(U) ADRP 1-03. *The Army Universal Task List*. 02 October 2015.

(U) ADRP 2-0. *Intelligence*. 31 August 2012.

(U) ADRP 3-0. *Operations*. 11 November 2016.

(U) ADRP 3-90. *Offense and Defense*. 31 August 2012.

(U) ADRP 5-0. *The Operations Process*. 17 May 2012.

(U) AR 11-6. *Army Foreign Language Program*. 18 February 2016.

(U) AR 25-400-2. *The Army Records Information Management System (ARIMS)*. 02 October 2007.

(U) AR 27-60. *Intellectual Property*. 01 June 1993.

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

(U) AR 530-1. *Operations Security*. 26 September 2014.

(U) ATP 2-01. *Plan Requirements and Assess Collection*. 19 August 2014.

(U) ATP 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace*. 10 November 2014.

(U) ATP 2-22.2-1. *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities (U)*. 11 December 2015.

(U) FM 2-0. *Intelligence Operations*. 15 April 2014.

(U) FM 3-55. *Information Collection*. 03 May 2013.

(U) FM 3-90-2. *Reconnaissance, Security, and Tactical Enabling Tasks Volume 2*. 22 March 2013.

(U) FM 27-10. *The Law of Land Warfare*. 18 July 1956.

NAVY AND MARINE CORPS PUBLICATIONS (U)

(U) Most Marine Corps doctrinal publications are available online: https://doctrine.usmc.mil/.

(U) Most MCOs are available online: http://www.marines.mil/News/Publications/ELECTRONIC-LIBRARY.aspx.

(U) MCDP 2. Intelligence. 07 June 1997.

(U) MCO 1550.25A. Marine Corps Foreign Language Program. 06 March 2012.

(U) MCO 3070.2A. The Marine Corps Operations Security (OPSEC) Program. 02 July 2013.

(U) MCO 3500.26A. Universal Naval Task List (UNTL). 30 January 2007.

(U) MCO 3900.20. Marine Corps Capabilities Based Assessment. 27 September 2016.

(U) MCRP 2-10A.6. Ground Reconnaissance Operations. 25 November 2015.

(U) MCRP 2-10A.8. Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance, and Reconnaissance Optimization. 14 April 2015.

(U) *MCRP 2-10B.1. Intelligence Preparation of the Battlefield/Battlespace. 10 November 2014.*

(U) *MCTP 2-10A. MAGTF Intelligence Collection. 01 July 2004.*

(U) *MCTP 3-20G. Air Reconnaissance. 21 July 2003.*

(U) *MCWP 5-10. Marine Corps Planning Process. 24 August 2010.*

(U) SECNAVINST 3820.3E. *Oversight of Intelligence Activities Within the Department of the Navy (DON).* 21 September 2005. Available online: http://www.secnav.navy.mil.

OTHER PUBLICATIONS (U)

(U) Constitution of the United States of America. 1787. Available online: http://www.archives.gov/exhibits/charters/constitution.html.

(U) *"Principles Governing the Collection of Internet Addresses by DOD Intelligence and Counterintelligence Components." 06 February 2001. Available online through the Inspector General of the Marine Corps website:* http://www.hqmc.marines.mil/igmc/Units/Intelligence-Oversight-/References/.

(U) National Security Act of 1992. Available online: https://www.gpo.gov/fdsys/granule/CRI-1992/CRI-1992-NATIONAL-SECURITY-ACT/content-detail.html.

UNITED STATES LAW (U)

(U) Most USCs are available online: http://uscode.house.gov/.

(U) Public Law 109-163. *National Defense Authorization Act for Fiscal Year 2006.* 06 January 2006. Available online: https://www.gpo.gov/fdsys/pkg/PLAW-109publ163/content-detail.html.

(U) Title 10, USC. *Armed Forces.*

(U) Title 17, USC. *Copyrights.*

(U) Title 18, USC. *Crimes and Criminal Procedure.*

(U) Title 50, USC. *War and National Defense.*

WEBSITES (U)

(U) *Inspector General of the Marine Corps. http://www.hqmc.marines.mil/igmc/.*

(U) Open Source Enterprise. http://www.opensource.gov/.

(U) Open-Source Resources. See appendix D of this publication for the list of websites for the open-source resources.

(U) U.S. Army Cyber Command. http://www.arcyber.army.mil.

(U) U.S. Computer Emergency Readiness Team. http://www.us-cert.gov/.

(U) U.S. Copyright Office. https://www.copyright.gov/.

PRESCRIBED FORMS (U)

(U) This section contains no entries.

REFERENCED FORMS (U)

(U) Unless otherwise indicated DA forms are available on the Army Publishing Directorate website: www.apd.army.mil.

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

This page intentionally left blank.

Index (U)

(U) Entries are by paragraph number unless indicated otherwise.

~~FOR OFFICIAL USE ONLY~~

(U) Entries are by paragraph number unless indicated otherwise.

~~FOR OFFICIAL USE ONLY~~

(U) Entries are by paragraph number unless indicated otherwise.

~~FOR OFFICIAL USE ONLY~~

This page intentionally left blank.

By order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

b6

GERALD B. O'KEEFE
Administrative Assistant to the Secretary of the Army
1718004

By Direction of the Commandant of the Marine Corps:

b6

ROBERT S. WALSH
Lieutenant General, U.S. Marine Corps
Deputy Commandant
Combat Development and Integration

DISTRIBUTION:

Active Army, the Army National Guard, and the United States Army Reserve. Not to be distributed; electronic media only.

~~**FOR OFFICIAL USE ONLY**~~

PIN: 102813-000

MARINE CORPS PCN: 144 000278 00

~~FOR OFFICIAL USE ONLY~~