

NATO UNCLASSIFIED

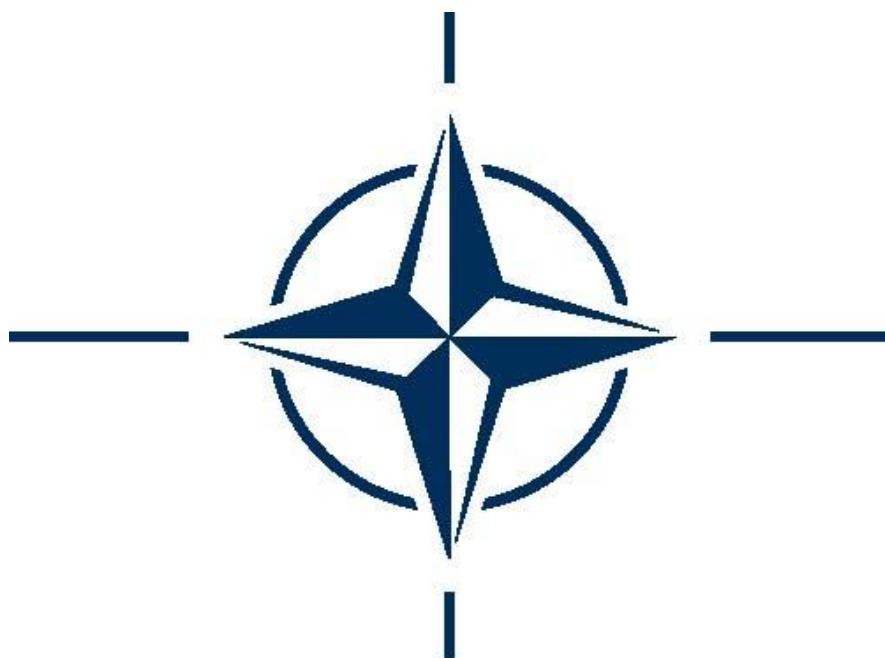
NATO STANDARD

AJP-2.9

**ALLIED JOINT DOCTRINE
FOR OPEN-SOURCE INTELLIGENCE**

Edition A Version 1

JUNE 2019



NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)
© NATO/OTAN

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Intentionally blank

NATO UNCLASSIFIED

NATO UNCLASSIFIED

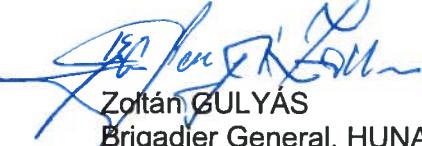
NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

12 June 2019

1. The enclosed Allied joint publication AJP-2.9, Edition A, Version 1, ALLIED JOINT PUBLICATION FOR OPEN-SOURCE INTELLIGENCE, which has been approved by the nations in the Military Committee Joint Standardization Board, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 6522.
2. AJP-2.9 Edition A, Version 1, is effective upon receipt.
3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.
4. This publication shall be handled in accordance with C-M(2002)60.



Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

NATO UNCLASSIFIED

NATO UNCLASSIFIED

Intentionally blank

NATO UNCLASSIFIED

NATO UNCLASSIFIED

AJP-2.9

RESERVED FOR NATIONAL LETTER OF PROMULGATION

Intentionally blank

RECORD OF RESERVATIONS

Intentionally blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
DEU	<p>Following the JISR-process of task, collect, process, exploit and disseminate the intelligence collection discipline OSINT provides JISR results to answer validated collection requirements in order to contribute to intelligence requirements. National implementation may compromise the given description but shall provide full interoperability with regard to the provision of JISR results. For a further version or edition of AJP-2.9 the development of OSINT results has to be described strictly along the JISR process. Same counts for the development of the supplemental doctrine of OSINT TTPs. Rational: Within the text of AJP-2.9 the development of OSINT results is not always described consistently, consequently and rigorously along the JISR process. Germany will not implement any other process to produce OSINT results besides the JISR process. In harmonization to AJP-2, AJP-2.1 and AJP-2.7 the development of OSINT results are to be described in the following version or edition of AJP-2.9 or supplemental doctrines strictly along the JISR process.</p>
USA	<p>Reservation 1. The United States recommends changing OSINT to PAI on paragraphs 1.16 subparagraph (C) and 3.8 subparagraph (A). OSINT is a form of intelligence derived from PAI that has been collected, processed, validated, and analyzed for intelligence purposes. While PSYOP specialists and IO planners can and will use PAI to aid their mission, they do not have authorities to conduct intelligence activities. If referring to Intelligence Collectors with the proper mission set and authority, assigned to PSYOP or IO organizations rather than PSYOP specialists themselves we request further clarification within this doctrine. This reservation will be removed when doctrine clarifies these relationships.</p> <p>Reservation 2. The United States recommends adding a note referencing Status of Forces Agreement(s) (SOFA) into paragraph 1.10 Legal Considerations and/or paragraph 2.7, sub-paragraph (G). Referencing the SOFA and how it may impact OSINT activities in a foreign country is imperative as it will ensure anyone conducting OSINT is aware of the agreement and help to avoid violations which may cause future operations issues for NATO elements.</p> <p>Reservation 3. The United States recommends changing the words "All-Source" intelligence analyst and replacing it with "Intelligence Professional throughout the document. Please refer to Public Law 109-163 National Defense Authorization Act for Fiscal Year 2006, Subtitle D Intelligence Related Matters; SEC 931 Department of</p>

	<p>Defense Strategy for Open Source Intelligence. OSINT is embedded in all Intelligence disciplines as a product of the TPED cycle.</p> <p>Reservation 4. The United States recommends adding a new section labeled “Tasking” as the first part of the TCPED process. Please refer to Public Law 109-163 National Defense Authorization Act for Fiscal Year 2006, Subtitle D Intelligence Related Matters; SEC 931 Department of Defense Strategy for Open Source Intelligence. OSINT is embedded in all Intelligence disciplines as a product of the TPED cycle.</p> <p>Reservation 5. The United States recommends adding a subparagraph to paragraph 2.3 that touches on de-confliction and ensures digital footprints are minimal and we are not conducting internet fratricide.</p> <p>Reservation 6. The United States recommends adding text into paragraph 3.27 Training and emphasizing “all persons conducting OSINT rather than referencing PAIs must be intelligence professionals with proper mission and authority. Open Source Intelligence is an intelligence function/discipline and therefore can only be conducted by intelligence professional.”</p> <p>Reservation 7. The United States does not accept that key leader engagements are by extension, part of psychological operations. This reservation will be lifted once the text has been corrected.</p> <p>Reservation 8. The United States does not accept terms and definitions listed in the lexicon that are not quoted verbatim from NATOTerm (e.g. measure of effectiveness, open source intelligence). This reservation will be lifted when the correct NATO terms and definitions are cited.</p> <p>Reservation 9. The United States does not accept any term that is not NATO Agreed or do not have a current terminology tracking form submitted to the Military Committee Terminology Board in an attempt to define the term (e.g. actor, casual source, collection discipline, controlled source, joint intelligence preparation of the operating environment, uncontrolled source). This reservation will be lifted when those terms and definition are removed from the Lexicon.</p> <p>Reservation 10. The United States does not accept terms introduced or revised in this AJP that have not been correctly introduced or revised IAW AAP-77, NATO Terminology Manual. This reservation will be lifted once the correct procedures are followed for introducing or revising terms.</p> <p>Reservation 11. The United States does not accept ‘humans right law’ as used in paragraphs 1.19 and 3.19. The law of war is the recognized term, also known as the law of armed conflict. Refer to</p>
--	--

	DODD 2311.01E, DOD Law of War Program. Linking the “law of armed conflict” with “human rights law” or “international human rights law” conflates the separate portions of law in a way that inconsistent with United States policy. Additionally, “human rights law” or “international human rights law” are a subset of international law and not a body of law in and of itself.
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Intentionally blank

Related Documents

- A. MCM-0077-2000, *Military Committee Guidance on the Relationship between NATO Policy and Military Doctrine*.
- B. MC 0114, *Procedures for Production of NATO Agreed Intelligence*.
- C. MC 0128/8, *Policy Guidance for NATO Intelligence*.
- D. MC 0133/4, *NATO Operations Planning*.
- E. MC 0166, *NATO Intelligence Warning System*.
- F. MC 0647, *NATO Policy on Open Source Intelligence*.
- G. MC 0646 *NATO Joint Intelligence Surveillance and Reconnaissance (JISR) Policy*.
- H. AJP-2(A), *Allied Joint Doctrine for Intelligence, Counter-intelligence and Security*.
- I. AAP-06, *NATO Glossary of Terms and Definitions*.

Intentionally blank

Preface

Context

1. Advances in technology are contributing to exponentially growing volumes of data and information that are publicly available and relevant to NATO operations. Allied joint publication (AJP) *Allied Joint Doctrine for Open Source Intelligence* AJP-2.9 considers Open Source Intelligence (OSINT) in this context, where information is constantly being generated and shared across the operating environment (OE) by all actors.

Scope

2. AJP-2.9 describes how OSINT activities are planned, conducted and assessed in NATO, with a focus on the operational level. It explains the role of OSINT as one of the intelligence collection disciplines in the context of the joint intelligence surveillance and reconnaissance (JISR) process, and its application within the intelligence cycle.

Purpose

3. This doctrine is intended primarily for NATO operational level commanders and staffs. It is also intended as a reference document on the use of OSINT for intelligence staffs within NATO, but is also applicable as a reference at any level of command. It provides an explanation of the NATO OSINT collection discipline to those external to the NATO organization.

Application

4. NATO intelligence doctrine is deliberately written to allow considerable flexibility in its application. It does not provide detail on who exactly does what in any given scenario. The situation encountered at the time will shape the intelligence structures and responsibilities required to deliver end to end management of intelligence to commanders and decision makers.

Target audience

5. AJP-2.9 is intended primarily as guidance for joint NATO commanders and staff. However, the doctrine provides a useful framework for operations conducted by a coalition of NATO member states, partners and non-NATO states. It also provides a reference for civilian personnel.

Linkages

6. AJP-2.9 is intended to be read with the keystone intelligence document AJP-2. Other documents that are linked to AJP-2.9 are:
 - a. *Allied Joint Doctrine for Intelligence Procedures (AJP-2.1)*.
 - b. *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance (AJP-2.7)*.
 - c. *NATO Policy on Open Source Intelligence (MC 0647)*.
 - d. *Allied Joint Doctrine for Human Intelligence (AJP-2.3)*.
 - e. *Allied Joint Doctrine for Targeting (AJP-3.9)*.

Table of contents

Related documents.....	ix
Preface.....	xi
Table of contents.....	xiii
Chapter 1 – Open source intelligence fundamentals	1-1
Section 1 – Introduction.....	1-1
Section 2 – Explanation and clarification of terms.....	1-2
Section 3 – Overview	1-3
Section 4 – Open source intelligence principles	1-7
Section 5 – OSINT sources.....	1-8
Chapter 2 – OSINT and the intelligence cycle.....	2-1
Section 1 – Introduction.....	2-1
Section 2 – Direction.....	2-2
Section 3 – Collection	2-3
Section 4 – Processing	2-4
Section 5 – Dissemination.....	2-7
Chapter 3 – OSINT support to NATO operations	3-1
Section 1 – Introduction.....	3-1
Section 2 – OSINT support by level of command.....	3-1
Section 3 – Command and staff responsibilities.....	3-2
Section 4 – Special provisions.....	3-5
Lexicon.....	LEX-1
Part I – Acronyms and abbreviations	LEX-1
Part II – Terms and definitions	LEX-2

Annex A – OSINT

Sources.....	A-1
Appendix 1 – Media characteristics.....	1-A-1

CHAPTER 1 – Open source intelligence fundamentals

Section 1 - Introduction

1.1 The aim of AJP-2.9 is to describe the framework procedures and considerations required to facilitate the delivery of open source intelligence (OSINT) results during operations. This framework provides a common understanding of OSINT procedures at all NATO levels.

1.2 OSINT is developed in accordance with the procedures described in AJP-2.7 and AIntP-14. OSINT results are developed through the JISR process and are utilized in the processing phase of the intelligence cycle (see Ch. 2) but may when needed also be disseminated directly to the requestor. The specific techniques will be described in a future level-3 doctrine.

1.3 AJP-2.9 also informs wider intelligence staff including Intelligence Requirements Management and Collection Management (IRM&CM) staff, who will have closely related functions to perform. However, AJP-2.9 does not list instructions on how to carry out OSINT procedures; this is the domain of tactical publications and standard operational procedures (SOPs). Instead, it offers authoritative guidance that requires judgment in application, and should be used to influence subordinate documents.

1.4 OSINT is an independent intelligence collection discipline which can contribute to intelligence requirements (IRs) and satisfy collection requirements. OSINT can thereby complement or confirm the results of other intelligence collection capabilities. Also, it can greatly aid in focusing other intelligence collection disciplines by providing contextual information.

1.5 To operate and succeed in the modern operating environment, NATO commanders need intelligence not only on potential adversarial military capabilities, intelligence limitations and intentions but also on the social environment, including cultures, fears, perceptions, motivations, and aspirations of all actors within the battlespace. Other elements of the operating environment, including political, economic, social, infrastructure and information (PMESII), contribute significantly in providing a comprehensive preparation of the joint intelligence preparation of the operating environment (JIPOE). OSINT, with its abilities to collect and exploit information from the public realm, is vital for successful NATO operations.

Section 2 – Explanation and clarification of terms

1.6 **OSINT:** OSINT is derived from the systematic collection, processing, exploitation, and dissemination (CPED) of open source information, in any form, in response to intelligence requirements. Publicly available information includes any information or material posted on the Internet, published, broadcast (radio and television), or provided for general

public consumption such as newspapers, placards, billboards, or transcripts of public meetings or speeches. Information of limited public distribution implies material that is available to the public for a fee.

1.7 **Internet:** The Internet is a global network of private, public, academic, business, and government computer networks. The Internet has no centralized governance in either technological implementation or policies for access and usage, although constituent networks may set their own policies. As the Internet has neither technological nor content/usage restrictions, it has evolved to include a vast array of services such as Internet sites, email, file transfer, remote computer control, newsgroups, and messaging in numerous formats.

1.8 Open sources of data are publicly available but unstructured facts, figures and entities that can be gathered together as the basis for analysis. This includes the metadata¹ of a particular piece of information that is publicly available.

1.9 **Publicly Available Information (PAI):** Publicly available information is open source information that comprises any material published or broadcast for general public consumption; available on request to a member of the general public; accessible online or offline to the public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public. It is any information where there is a reasonable basis to believe that it is lawfully made available to the general public. Publicly available information is comprised of data that has been put together, generally by an editorial process that provides some filtering and validation as well as presentation management.

1.10 OSINT is distinct from personal, academic, business or journalistic research of publicly available information in that it represents the application of the proven process of intelligence to the diversity of resources by trained intelligence analysts, with the intent of fulfilling intelligence requirements for the commander. Research and discovery of publicly available Information that is not part of the NATO intelligence process falls below the threshold for OSINT and remains as PAI.

1.11 **Social networks and networking:** Social networking is the way individuals/groups use the various sites, email, and messaging services available on the Internet. These sites can be closed (limited access) or open. Social networking is one of the most popular activities on the Internet and comprises a powerful mixture of human social instincts and Internet technologies. It is rapidly evolving due to availability, audience demographics and the way the audience itself experiences social networks. However, the main push for social networking is the fact that it is becoming this generation's fundamental means of communication.

¹ Data that describe data objects. (NATOTerm)

1.12 **Social media (SM)**²: Social media refers to the interaction of individuals in which they share, and exchange information in virtual communities. Social media encompasses social network sites that use Internet and other telecommunication services to allow people to construct a public or semi-public profile³ within a network, define a list of other users with whom they wish to share information, and view and access their list of connections and those made by others within that system.

- a. In states where the government exercises direct-control of the media and the Internet, social media is a major influence in the respective societies. Social, cultural, and political movements, in addition to individuals, use social media capabilities to organize demonstrations and to rapidly spread their messages to large audiences, even globally. Social media provides subjugated populations with the ability to organize “virtually,” even in the face of physical repression. Analysis of social media content is fraught with potential danger as the users of social media are the ultimate uncontrolled casual sources. Analysis of social networks seeks to identify and comprehend the network nodes and relationships between them. These analyses require expertise built upon advanced multi-disciplinary knowledge of the social, mathematical, and anthropological sciences, concepts, and methodologies.
- b. While individuals around the world have gravitated to social media, so too have political organizations, governments, and commercial enterprises. As such, the content of social media can range from strictly controlled to completely uncontrolled. Some examples of social media are:
 - (1) Blogs and micro-blogs;
 - (2) Social networks;
 - (3) Professional networks;
 - (4) Video sharing (video weblogs);
 - (5) Audio sharing (podcasts);
 - (6) Photo sharing; and
 - (7) Social bookmarking.

² Source: MC 0647, *NATO OSINT Policy*.

³ A public profile means that all personal information posted on a social network is available to anyone who chooses to view it. A semi-public profile means that a user has adjusted their privacy settings so as to limit the content shared, and the audience with whom it is shared.

1.13 **Social media monitoring (SMM)**: SMM is the activity of finding, combining and detecting information, patterns and trends in social media in order to support an intelligence or information requirement.

1.14 **Media**: In the context of OSINT, media refers to and encompasses all means through which journalists and other accredited media personnel disseminate their products. In the past media was generally restricted to print, radio, and television. With the increase in access to and use of the Internet, this communication tool has become a favoured means for the dissemination of media. Media personnel both outnumber military intelligence collectors and often have access to valuable and authoritative sources during emerging situations. Characteristics of the media are discussed in appendix 1 to annex A.

1.15 The terms ‘Overt’ and ‘Discreet’ further distinguish OSINT collection activity from activities that are ‘Covert’ or ‘Clandestine’⁴. ‘Overt’ is deemed to be at an acceptable Operational Security (OPSEC) or personal security risk in that there is licensed access and permission to use. ‘Discreet’ access is deemed to be generally passive, masked to the source owner or non-attributable identity. ‘Covert’ is deemed to be masked active engagement or use of aliases and ‘Clandestine’ is the need for complete deniability of the activity, for instance, by the use of aliases. Overt or discreet methods consider licensing arrangements of the source information and therefore define the limits of activity for NATO Military Authorities intelligence personnel. Additionally, OSINT activity should be passive and must not entail active engagement on digital sites, such as interaction on social media forums, posting information or comments.

Section 3 - Overview

1.16 OSINT is a key contributor to the Joint Intelligence Preparation of the Operating Environment (JIPOE). Through the PMESII methodology it aids commanders in understanding their operating environment. Further, the systematic CPED of publicly available information supports answering Information Requirements (IRs) and the subsequent tipping and cueing of other collection disciplines. Other examples are:

- a. In support of current intelligence, OSINT, more than other intelligence collection disciplines, can enhance situational awareness by providing broader coverage and timeliness, primarily through social media (SM) and live news feeds.
- b. In support of basic intelligence, OSINT can provide encyclopaedic information on leadership, security, military capabilities, terrorism, WMD/CBRN indicators, possible CBRN threat and risk potentials, international relations, economics, media, infrastructure, health, demographics, climate and geography, etc. Information on international organizations, governmental and non-governmental organizations, and cultural and anthropological studies on

⁴ See lexicon AAP-6 (2018) and illustration MC 0647, *NATO OSINT Policy*.

potential operating areas can give commanders a critical understanding of their complex operating environment. Support to basic intelligence is OSINT's main contribution within intelligence.

- c. In support of psychological operations (PsyOps), OSINT provides cultural information as well as valuable insights concerning perceptions, intentions and capabilities that may influence decisions/actions of the considered targets and the target audiences in the local area.
- d. In support of trend analysis and assessing measures of effectiveness (MoE), social media networks provide a unique opportunity to understand the impact of all the PMESII factors in the battlespace, both adversary and friendly.
- e. In support of the development of alternate scenarios, OSINT can provide access to authoritative thinking and opinions from academia, think tanks and strategic studies institutes.

1.17 Advantages. Significant advantages of open source information include availability, accessibility, diversity of information, language, and ease of use. OSINT supports a broad-based understanding of the OE allowing for rapid orientation and monitoring of an ongoing situation. OSINT also allows the all-source intelligence analyst to add context to higher classified material that may result in new assessments, or other avenues of inquiry for the intelligence requirement. Data and information obtained by OSINT personnel may be the only source of knowledge or can pose a trigger for further requirements. When integrated with results obtained by other intelligence collection disciplines, OSINT can provide a response to an intelligence requirement with a higher level of confidence. OSINT may also be shared with a wider audience, including non-NATO elements. Another advantage of OSINT exploitation is that it is often less expensive than other intelligence collection disciplines. Furthermore, OSINT can be very flexible. Most of the time, priorities can be shifted easily with low costs and effort, and a low and acceptable influence on mission integration.

1.18 Constraints. Appropriate tradecraft must be employed at all times by OSINT analysts to ensure that intelligence collection plans, OSINT technical capabilities, and the underlying military intent are not compromised. OSINT can only be conducted by trained analysts employing appropriately approved capabilities. Open source data and information may contain inaccuracies, biased perspectives, irrelevant information and disinformation. Source verification, like the use of scoring criteria, would help to mitigate these issues, although it does not eliminate them completely. While it is easier not to follow proper operations security when "surfing the net", this behaviour may result in unintentional exposure of friendly intelligence interests to adversaries and or potential adversaries. Open source collection can also result in a vast volume of information, the processing and exploitation of which may be very resource intensive as well as time-consuming. There are numerous legal complexities associated with collecting, storing, retaining and utilizing OSINT which must be taken into consideration. Finally, rapidly evolving Internet and information technologies can

quickly make existing collection technologies redundant. This issue can be mitigated with proper management of paid and free sources, although it may result in an increase in cost.

1.19 Legal Considerations. Publicly available data and information and open sources cover a wide array of areas. OSINT methods and tools are subject to legal constraints stemming from Human Rights Law, including the right to privacy, the freedom of speech and the protection of personal data, the law of intellectual property rights and other national laws which affected nations must respect. OSINT activities conducted by intelligence personnel will apply tools and methods that respect the law; (for example as it applies to licenses), as well as attempt to mitigate the risk of legal liability attributable to the Alliance and individual NATO personnel.

1.20 These legal considerations may differ for each collection and subsequent PED⁵ activity depending on geographical location, the analyst, the organisation and the type, content and associated license of the data or information being used. Assistant Secretary General for Intelligence and Security (ASG I&S) and SACEUR will provide the detailed direction and guidance concerning OSINT activity that will include legal advice based on the overarching intelligence requirements of the NATO Command Structure. All efforts are to be taken to ensure there is appropriate legal control over the actions, tools, licensing and methodology used by the NATO Intelligence Community for OSINT, including Social Media exploitation.

Section 4 - Open source intelligence principles

1.21 Apart from the core principles of OSINT activities described in the OSINT policy, the following principles are also applicable for the collection, processing, exploitation and dissemination of OSINT:

- a. **Focused.** OSINT activities must be conducted as part of the all-source intelligence effort and focused on providing answers to the commander's intelligence requirements.
- b. **Compliance.** NATO, and individuals operating on behalf of the Alliance, have to abide by the usage laws under which the information was made public. This includes information that has an open license and therefore the source owner has placed no stipulation on subsequent use. Copyright restriction is the most common form of licence requirement for use beyond that of personal consumption. License restrictions are in many forms: requiring a fee; acknowledgement via citation; registration (particularly for deep web content) or permission for use from the source. This does not apply to member states, which operate under their own national laws.

⁵ PED – Process, Exploit and Disseminate steps of the JISR process.

- c. **Efficiency.** Activities for collection of open source information must ensure unnecessary collection is reduced or eliminated. Given the vast stores of available open source data and information, collection efforts must strive to reduce the volume of collected material to manageable levels. All-source intelligence analysts must not be presented with reams of tangential information, but rather with only the relevant information that will allow them to answer the intelligence requirements most efficiently.
- d. **Source evaluation.** There is a risk of open source information being biased or containing disinformation. The veracity and validity of any open source information must be determined to identify biases of the author and sources. Awareness of possible bias in the material is an important consideration for the analyst when deciding whether and how to use the material. To assist all-source intelligence analysts in determining what open source information to use, open source personnel must evaluate all information collected. This will require critical thinking and sound judgment, qualities dependant on the capabilities and qualifications of the OSINT personnel. As with other intelligence reporting, source evaluation must be preserved throughout the intelligence production processes.
- e. **Accessibility.⁶** Open source personnel must have access to the widest array of material possible, including paid and unpaid sources. Limiting the spectrum of open sources increases the risk of incorporating biased information into the analytical process. Continual evaluation of sources used as well as discovering and gathering new sources is an essential process of OSINT collection.

Section 5 – OSINT Sources

1.22 In intelligence usage, a source⁷ is a person from whom or a thing from which information can be obtained. Sources are categorized as controlled, uncontrolled and casual. They are defined as:

- a. **Controlled.** Controlled sources are under control of an intelligence agency or organization, or specifically nominated intelligence staff. They can be tasked directly.⁸ From an OSINT perspective, controlled sources are those open sources that may be tasked within the limits of commercial contracts or the conditions of subscriptions. Examples include academia, commercial providers of services, and think tanks.

⁶ AJP-2.

⁷ NATOTerm.

⁸ AJP-2.

- b. **Uncontrolled.** Uncontrolled sources are those not under formal control of an intelligence agency or organization, or specifically nominated intelligence staff. Therefore, they cannot be tasked directly.⁹ This type of material is a crucial part of OSINT collection. Examples include media, established Internet sites, and published documents.
- c. **Casual.** Casual sources provide unsolicited information. Information provided by a casual source should be treated with caution, as the collector has no history to utilize in order to verify a source's reliability. Casual sources may be considered a sub-category of uncontrolled sources. Examples include previously unexplored Internet sites and unprocessed social networking information.

1.23 A description of potential OSINT sources is provided in nnex A. This list is not exhaustive and is presented for illustrative purposes only.

⁹ AJP-2.

CHAPTER 2 - OSINT and the intelligence cycle

Section 1 – Introduction

2.1 The intelligence cycle is the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available for users. The systematic exploitation of all sources is an essential part of the intelligence cycle. The activities are divided into four phases: direction, collection, processing and dissemination. While the intelligence cycle outwardly appears as a simple process, in reality its activities are complex and it comprises many simultaneous cycles operating at different levels and speeds. Some activities can overlap while others may coincide so that they are conducted concurrently, rather than sequentially. The four phases of the intelligence cycle are underpinned by intelligence requirements management (IRM) and collection management (CM). Both the IRM and CM enable the intelligence cycle to operate in a timely and efficient manner. (see Figure 2.1)

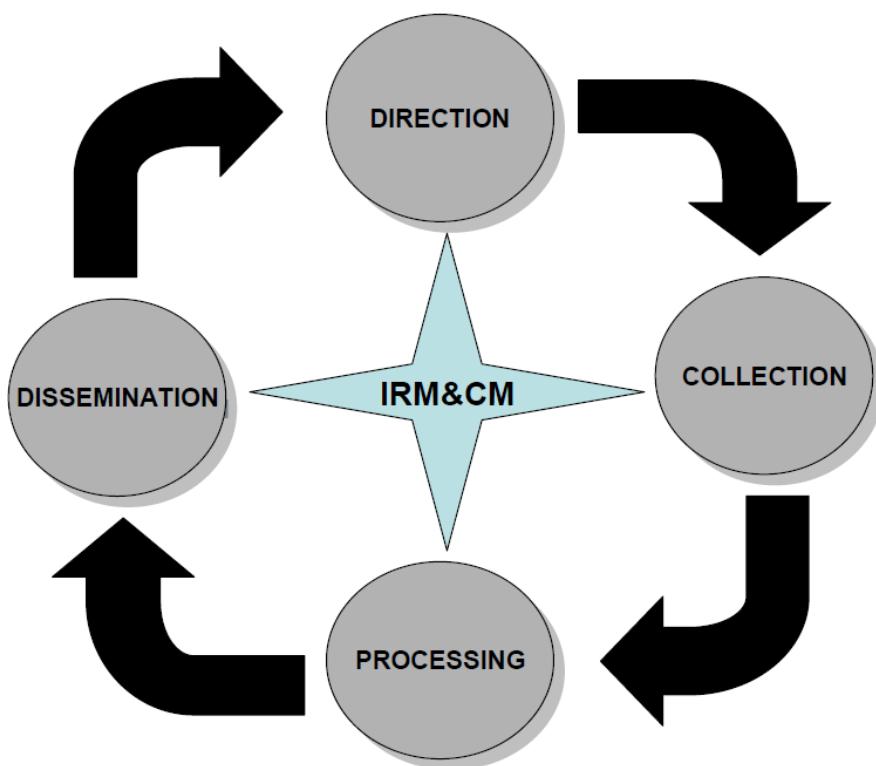


Figure 2.1: The Intelligence Cycle

Section 2 - Direction

2.2 Commanders direct their intelligence staff by clearly defining the CCIRs. The intelligence staff accordingly prioritise their requirements into PIRs, further broken down into SIRs and identify those that are essential to the planning process. From this direction, the intelligence staff determines how the IRs are to be met and what information and intelligence is required to answer them. This information is included in the commander's intelligence collection and processing plan (ICPP), and subsequently tasked to the appropriate subordinate commands, JISR capabilities and agencies via the IRM&CM function.

2.3 Tasking involves:

- a. An assessment of whether SIRs can be answered through existing intelligence. If not, the tasking of subordinated commands, JISR capabilities, agencies, etc., and, where appropriate, coordinating their activities to collect the necessary information;
- b. Monitoring intelligence CPED to ensure that the IRs are being satisfied;
- c. Ensuring that OSINT activities are conducted in a timely manner, and when delays occur, ensure that collectors and CPED capabilities are re-tasked and re-prioritised, as required;
- d. Ensuring that OSINT activities are conducted legally, considering that some collections means and methods, as well as sources, may be subject to legal restrictions in certain jurisdictions¹⁰ (e.g. copyrights or license restrictions, by international/national laws, etc); and
- e. Ensuring that NATO arrangements for the sharing of OSINT, such as NATO security and release and disclosure directives are respected.

2.4 Inside the direction phase of the intelligence cycle intelligence requirements are determined and collection efforts are planned, supported through the IRM&CM functions¹¹ as depicted in Figure 2.1. This ensures identification and articulation of intelligence gaps and matches them with available collection capabilities with OSINT being one of the capabilities. It also enables cross-cuing from one collection discipline to another.

2.5 Intelligence sections and elements may have imbedded OSINT capabilities in the form of dedicated OSINT personnel. IRM&CM specialists inside the intelligence staff should have an adequate understanding of OSINT activities. When commands do not have enough resources to collect and exploit open source information, it can be collected through

¹⁰ Some OSINT activity may meet the threshold of being covert surveillance and require an additional governance regime to be compliant with national law.

¹¹ For more information on the IRM&CM functions, refer to AJP-2.1, Chapter 3.

subscription to academics/think tanks, etc. Such support may be especially advantageous when in-depth collection and processing are required.

Section 3 - Collection

2.6 Inside the collection phase of the intelligence cycle the JISR capabilities – as OSINT – collect data and information and process this data and information to a useable format and exploit it for further usage. Like in any other intelligence collection discipline, collection and exploitation within OSINT is determined by time, topic, scope and capabilities, i.e. available human resources and equipment. Upon receipt of collection tasks from the CJ2, the OSINT collection team plans how to collect the required information, as the tools, procedures and time required to complete the collection will vary with the sources. The design of the collection is a continuous, iterative and dynamic process which relies on OSINT personnel to creatively define the analytical interest and the most suitable approaches.

2.7 Factors that affect the OSINT collection plan include:

- a. Planning and allocation of resources for acquisition of printed publications or commercial subscriptions. This is a long-term and deliberate collection activity. Selection of material should be done in collaboration with the all-source intelligence analysts expected to use the OSINT results. Renewal of contracts and subscriptions should likewise be a deliberate process.
- b. Assessment of the risks of bias, disinformation, and the likelihood that foreign intelligence services will track and identify our own open source collection efforts. The results of these risk assessments may drive the collection effort to use Internet services that are not attributable to NATO.
- c. OSINT personnel may face incredibly large datasets which require access to individuals with specialist data science skills to interpret.
- d. OSINT personnel may be required to reach-back to a NATO or National support function.
- e. Consideration of the time available and the type of information required to determine the breadth, depth, strategies and techniques to collect data and information for open source results.
- f. Operations Security (OPSEC) in order to deny an adversary the ability to better understand NATO or its Allies' intentions or capabilities.
- g. Consideration of international and national laws, such as Human Rights, for each NATO member to avoid the risk of legal liability for the organisation or member state.

- h. Human resources and skillsets, including linguistic capabilities.
- i. Consideration of deconfliction with other friendly collection efforts.

2.8 Collection of information from open sources is either systematic or ad-hoc. Both methods can answer standing, long-term or specific intelligence requirements. Systematic collection generally means that sources are visited on a periodic basis, generally to answer standing, long-term, intelligence requirements. Beyond that, it can provide answers for specific requirements as well. Ad-hoc or dynamic collection is usually conducted to meet new or urgent short-term requirements. Furthermore, it can help to satisfy other intelligence requirements, e.g. when systematic collection does not yield the required information.

Section 4 - Processing

2.9 The processing phase of the intelligence cycle describes the conversion of open-source data and information, and other JISR results, into intelligence through collation, evaluation, analysis, integration and interpretation. It is a structured series of sequential activities. Processing may also be iterative, identifying additional intelligence gaps and spawning requirements for additional collection. OSINT personnel may assist in processing by creating professional products that require little interpretation by the collator to categorise and place in the collection database.

2.10 **Collation**¹². Collation is the first step of the processing phase inside the intelligence cycle, in which related items of JISR results are grouped together. In practice, it comprises of the procedures for receiving, grouping, recording, and filing all reports and collected information, and involves registering the receipt of each incoming piece of information and intelligence. Furthermore, it comprises filing each piece of information or intelligence into a database and placing them into an appropriate category or group. These categories or groups are related to the commander's intelligence requirements and the area of responsibility. If required, metadata can be added during this process to facilitate any further data retrieval.

2.11 By clearly citing and detailing information used for OSINT results delivered to all-source intelligence analysts, issues such as circular reporting may be identified. Circular reporting occurs when information on the same event is reported by different JISR capabilities or agencies, giving the impression that the information was collected by multiple different JISR capabilities or agencies, even though it was collected only once. Circular reporting can create a false sense of enhanced credibility and can slow down both the collation effort and intelligence communications systems.

¹² NATOTerm.

2.12 **Evaluation**¹³. Evaluation is the second step of the processing phase inside the intelligence cycle, in which items of data, information, open-source data and information as well as intelligence are assessed regarding their relevance. Reliability of the source and credibility of the information must be considered independently of each other to ensure that the rating allocated to the reliability of the source does not influence the rating given to the credibility of the information, or vice versa. Given the innumerable amount of open sources available, OSINT requires a particularly thorough evaluation process.

2.13 The principal basis for judging the reliability of a source is its previous reporting experience. OSINT will consider biographical information about the author in terms of academic and professional history, as well as who supports the authors' work. A highly reliable source will have historically provided information that has been highly accurate and unbiased. Thus, a highly reliable source is one that works at a credible institution, has a strong background in the topic and has had other credible sources quote their work. That said, analysts must consider that even highly reliable sources have limitations and may over time begin to apply bias as a means of influencing events. As a result of the differing nature and characteristics of open source material, OSINT personnel need to apply a methodological approach to evaluation. Including the criteria previously stated, OSINT personnel must also consider numerous other factors that can alter the reliability of a source, such as the source's allegiance, personal agenda, objectives and interests.

2.14 Credibility refers to the accuracy of the information reported, and should be assessed independently of the reliability of the source. As with other intelligence collection disciplines, credibility is essential for evaluating OSINT. The credibility of a particular piece of information will ideally be corroborated by reporting obtained through other collection capabilities or agencies. OSINT personnel must judge credibility on logic, professional experience, trends, the veracity and validity of alternative assessments, and the collection capability's capacity to observe, evaluate, process and report information.

2.15 Understanding that deception¹⁴ and bias may be applied to material is of particular interest when evaluating open source data and information. Sources such as government press offices, commercial news organizations, political campaign staffs, research centre publications, and others that publish or broadcast information can intentionally or unintentionally add, delete, modify or otherwise filter the original information for their own gain. This application of bias may also be applied for deception purposes. In order to distinguish objective and factual information from biased or deceptive information, the exploitation of open sources, as any other intelligence reporting, requires practitioners to understand the sources' reporting capabilities, postures and agendas so as to assess their reliability and the credibility of the information.

¹³ NATOTerm.

¹⁴ NATOTerm.

2.16 **Analysis.**¹⁵ Analysis is the third step of the processing phase inside the intelligence cycle of reviewing collected information in order to identify significant facts for subsequent interpretation. During this step, collated and evaluated information is analysed independent of other information so that salient facts of each piece of information can be identified. OSINT personnel collect material in an organized and professional manner for the production of intelligence products, according to the ICPP.

2.17 **Integration.**¹⁶ Integration is the penultimate step of the processing phase inside the intelligence cycle, whereby the factors identified during analysis are considered and combined with other known facts and intelligence to develop patterns that answer the commander's intelligence requirements. In advance of their collection and exploitation, OSINT personnel have to consider the relevance of the information with respect to the IR addressed.

2.18 **Interpretation.**¹⁷ Interpretation is the last step of the processing phase inside the intelligence cycle where the significance of information or intelligence is judged in relation to the current body of knowledge. Interpretation is an objective mental process of comparison as well as deduction based on common sense and professional knowledge and experience of both adversarial and friendly forces and existing information and intelligence. For each hypothesis or pattern developed during analysis and integration, all source intelligence personnel may ask a series of questions, which could be redirected to OSINT personnel:

- a. What if NATO knows the identity of the actor, equipment, or place? This is the consideration of all the implications of the presence of that actor or piece of equipment at that particular point;
- b. What if NATO knows what activity is taking place? The significance of the activity must always be compared with information about previous or expected activity, in order to discover whether there is any change in the pattern of activity;
- c. What is the significance of this information? The analyst must be sure that the piece of information has been fully exploited. Each deduction should be challenged, taking into account the original intelligence requirements, so the final product is relevant and useable.
- d. Has this information been made available as a means of deceiving NATO as to the target's real intentions? The intelligence community is a prime target for hostile deception and analysts should always be apprehensive of the information in front of them. In short, OSINT personnel should seek

¹⁵ NATOTerm.

¹⁶ NATOTerm.

¹⁷ NATOTerm.

confirmation, validation and verification of even the most credible information as part of their working processes.

2.19 OSINT personnel may assist in the interpretation of the material provided and they can be contacted to help with intelligence gaps that may arise during the analysis-integration-interpretation phases. They may also assist to address intelligence gaps with open source materials at any time during this phase or any time.

Section 5 - Dissemination

2.20 Dissemination¹⁸ is the last phase of the intelligence cycle. It is the process of providing all source intelligence, based on all available data, information and JISR results, including OSINT, to users in the format they need and by the time requested. To complete the cycle, dissemination includes a feedback activity which allows the CJ2 to determine if the provided intelligence satisfied the intelligence requirement and to identify any new requirements. For OSINT personnel, the dissemination of products to other analysts is just as important as the passage of intelligence to the commander.

2.21 Intelligence must be provided in a form that is readily usable and understandable by the user. This should be done in a timely manner without overloading the user and while minimizing the load on communications capabilities. Dissemination systems can consist of both “push and pull” control principles¹⁹. The “push” principle allows the CJ2 to push information out to satisfy the intelligence requirements at lower, higher, and flanking levels of command. Within OSINT, the “push” system could include the provision of alerts to those who need it when information has become available from a source being monitored. The “pull” concept involves requesters having direct access to databases, web sites, or other intelligence repositories or through the Request for information (RFI) process. An OSINT web site that can be accessed by the entire NATO force and that provides links to topical OSINT collection is an example of a “pull” system. The process of dissemination and archiving must adhere to NATO information management policies and directives.

¹⁸ NATOTerm.

¹⁹ For further description of “push” and “pull” principles see AJP-2. Ch. 4.5

Intentionally blank

CHAPTER 3 - OSINT support to NATO operations

Section 1 - Introduction

3.1 OSINT teams are an integral part of most NATO intelligence staffs and units. Most NATO member states also maintain OSINT capabilities within their intelligence organizations.

Section 2 – OSINT Support by Level of Command

3.2 OSINT is an integral part of intelligence at all levels of command. Its role and contributions evolve as the conditions of the operating environment changes. If performed rigorously and in a deliberate manner, OSINT can have numerous advantages. It can provide insights and context as a JISR result, enhancing understanding across all levels, and contributing to basic and current intelligence.

3.3 **Strategic level.**²⁰ Intelligence at the strategic level is required for the formulation of strategy and policy, monitoring the international situation for strategic indications and warnings, developing military plans, supporting the conduct of operations and providing situational awareness. Thorough understanding of the operating environment, a prerequisite for achieving strategic success, is where OSINT is especially advantageous.

3.4 OSINT plays an important role in the identification of strategic trends and socio-cultural conditions that are precursors or potential triggers for crisis. OSINT also contributes to the general intelligence effort through the provision of basic and current intelligence. Throughout a crisis, OSINT greatly aids in the intelligence analyst's development of assessments and re-evaluation of assessments during a campaign.

3.5 **Operational level.**²¹ OSINT results can contribute to the planning, execution and assessment of operations. OSINT focuses both on the capabilities and the intentions of current and potential adversaries and on the effects of the sociological and cultural environment on adversary and friendly operations.

3.6 OSINT is the predominant source of sociological and cultural basic intelligence for JIPOE. JIPOE provides information and intelligence regarding the sociological and cultural environment, such as social and cultural perspectives, demographics, politics, and economics. It can also provide information on adversary leadership capabilities, locations, and intentions. The PMESII model consists of factors that should be considered when conducting JIPOE.

3.7 OSINT can also support other operational level activities, such as:

²⁰NATOTerm

²¹NATOTerm

- a. Evaluation of operational effectiveness;
- b. OSINT supports the joint targeting process by providing information to assist in the development of target folders, and the prioritization of targets, and ultimately helps minimize collateral damage. Moreover, OSINT can assist in providing battle damage assessment. This particular OSINT support to targeting is applicable in both combat operations and in crisis response operations;
- c. Indications and warning of threats to the transitional environment and to security, e.g., through exploitation of social media monitoring and other sources; and
- d. Enhance the cooperation with the non-NATO coalition forces and international or non-governmental organizations as well as between NATO coalition forces and states through the provision of releasable unclassified intelligence.

3.8 **Tactical level.**²² OSINT plays a distinct role within the general intelligence activity at the tactical level and can provide support in areas such as:

- a. **Psychological operations.** OSINT may be used to support psychological operations, and by extension key leader engagements, by providing information and reporting that describe the targeted audience in terms of the relevant actors (individuals, groups, organizations) and their perceptions, opinions and opinion-forming processes, objectives, attitudes and aspirations, rivalries, supporters, followers, interrelations and interdependencies, receptivity, literacy and other factors that affect cognition, perceptions and emotions. One of the key tools to be used in this research is social media; and
- b. **Media activities.** OSINT can support media activities by identifying the publishers, authors, and stakeholders within the media environment and their themes, messages, affiliation, audience and infrastructure. This aids the intelligence analyst by indicating the biases of the various media outlets.

Section 3 – Command and Staff Responsibilities

3.9 **The CJTF Commander.** The Combined Joint Task Force's (CJTF) commander is responsible for the planning and conduct of all intelligence activities. To ensure the intelligence system is able to support operations, commanders must clearly and concisely state their CCIRs and PIRs. Although commanders bear overall responsibility for

²²NATO Term

intelligence, they normally delegate responsibility for most of its aspects to individuals in their staff.

3.10 **CJ2.** As the commander's staff principle for intelligence, the head of CJ2 is responsible for prioritizing, directing, and monitoring the OSINT effort and ensuring OSINT is collected, processed, exploited and disseminated in accordance with the intelligence requirements and the ICPP. At the operational level, the head of CJ2 may establish an OSINT coordinator position to directly manage OSINT activities. Other responsibilities and tasks of the CJ2 include:

- a. Establish and maintain the OSINT architecture in accordance with the CJTF operational requirements²³;
- b. Identify open source contract and subscription requirements and ensure the necessary funding is secured through the CJ8;
- c. Ensure OSINT personnel are aware of the commander's intent and intelligence requirements;
- d. Ensure that copyrights and other intellectual property rights are respected;
- e. Ensure OSINT results have the widest possible distribution and are shared with all-source analysts;
- f. Ensure OSINT information gaps are fed back into the intelligence collection planning cycle for effective re-tasking of JISR capabilities;
- g. Plan and coordinate access to managed attribution Internet services through the CJ6 when required for operations security reasons;
- h. Coordinate with the CJ6 to ensure the OSINT aspects of the intelligence communication and information systems (CIS) are operating as required;
- i. Determine and oversee the OSINT release, disclosure and security policies; and
- j. Ensure compliance with applicable domestic and international laws.

3.11 **CJ3 Staff.** As the commander's operations officer, the CJ3 must keep the CJ2 aware of the evolving situation and any new intelligence requirements that have arisen due to changes to the operation plan.

²³ NATOTerm

3.12 **CJ5 Staff.** The CJ5 must work hand-in-hand with the CJ2 when conducting the operation planning process, and must consider the intelligence needed for planning well ahead of when it will be needed.

3.13 **CJ6 Staff.** OSINT is dependent on the Internet and on radio and television. Without these services, OSINT capabilities will be severely restricted. The CJ6 must ensure that access to these critical sources of OSINT is available.

3.14 **Legal advisor.** OSINT activities/operations must be conducted in accordance with applicable national and international laws. Early engagement with the legal advisor will ensure that such operations are conducted lawfully.

3.15 Other staff elements will support the OSINT effort as required.

3.16 **OSINT personnel.** The personnel required to support OSINT may include: OSINT specialists, collators, analysts, researchers, managers, linguists, data scientists, and information technology staff, etc. Many OSINT personnel come from the fields of library and information sciences and other research disciplines. OSINT personnel should work forward from their IRs, and backwards from the risk with the information environment to develop their collection plan. They should apply appropriate tradecraft to ensure the risks identified are mitigated through good technique and thorough consideration of how they will actually collect the required information. Analytical skills are essential for OSINT personnel. These tasks include:

- a. Manage OSINT activity, including requirements, policies, systems, processes, procedures;
- b. Perform collection and exploitation of open source information;
- c. Identify and develop new sources of information, and new OSINT results and services, in accordance with the requirements of commanders and their staff;
- d. Provide OSINT training, support and assistance to other elements of the intelligence staff;
- e. Manage OSINT referral services, in which questions are redirected to other sources or agencies that are better positioned to respond;
- f. Manage online and offline subscriptions and accounts;
- g. Provide advice on copyright, operations security and source reliability;
- h. Apply OPSEC measures; and
- i. Comply with the appropriate legal requirements.

Section 4 – Special provisions

3.17 **Commercial subscriptions.** Commercial subscriptions constitute a valuable source of information and are widely used by NATO OSINT personnel and all-source intelligence analysts to access authoritative alternative opinions, analyses, reports, databases or other bespoke information resources. For example, Allied open source system (AOSS) provides access to a variety of premium OSINT resources. The use of common subscriptions helps to ensure that basic open source information is available for all NATO commands. Centralization of common subscriptions maximizes their use, but more importantly eliminates multiple subscriptions for the same information. This frees up financial resources that can be applied to other OSINT requirements. Acquisitions of commercial subscriptions in support of NATO intelligence requirements follow NATO acquisition regulations and information security directives.

3.18 The selection of commercial subscriptions or the decision to renew them is based on an assessment of the quality of their services. Evaluation criteria include:

- a. The reputation and professional eminence of the service provider;
- b. The service provider's access to valuable sources and the relevance of this information to answer intelligence requirements;
- c. The expertise of the service provider's contributors and collaborators;
- d. The uniqueness and applicability of proprietary analytical models, such as instability assessments in support of indications and warning requirements;
- e. The availability of additional services such as providing tailored products, access to additional databases, or facilitating contact with experts;
- f. The findings and conclusions presented by the service provider are supported by facts and sound analysis;
- g. The service provider's ability and propensity to provide detailed and credible insights compared to the main stream media and other freely accessible OSINT sources;
- h. The likelihood that the content will be biased or contain disinformation, based on the ownership or affiliation of the service provider; and
- i. The security risk associated with contracting the required information from a third-party service provider.

3.19 **Legal basis.** Publicly available data and information and open sources cover a wide array of areas. OSINT methods and tools are subject to legal constraints stemming from

Human Rights Law, including the right to privacy, the freedom of speech and the protection of personal data, the law of intellectual property rights and other domestic legal, as well as policy, provisions of the affected states. OSINT activities conducted by intelligence personnel will apply tools and methods that respect the law; (for example as it applies to licenses), as well as attempt to mitigate the risk of legal liability attributable to the Alliance and individual NATO personnel.

3.20 These legal considerations may differ for each collection and subsequent PED activity depending on geographical location, the analyst, the organisation and the type, content and associated license of the data or information being used. ASG I&S and SACEUR will provide the detailed direction and guidance concerning OSINT activity that will include legal advice based on the overarching intelligence requirements of the NATO Command Structure. All efforts are to be taken to ensure there is appropriate legal control over the tools, licensing and methodology used by the NATO Intelligence Community for OSINT, including social media exploitation.

3.21 Social Media (SM) Legal Considerations. The operating environment for SM represents a substantial ‘grey area’ of the law. There has yet to be a broad international dialogue on the interpretation and application of existing rules and principles of international law to social media, and as a result, wider policy and law have yet to mature fully. It is important to keep the legal advisors involved in the planning phase and on hand to advise on execution decisions. In addition to national and NATO sensitivities concerning the potential collection of personal data it is highly likely that active²⁴ SM engagement will be deemed attributable to NATO. OSINT activities on SM on behalf of NATO must remain passive and must not breach domestic and international civil law relating to the privacy rights, freedom of expression and rights of nationals. This will mean that there must be in place, as a minimum, clear procedures for authorizing SM OSINT operations as well as policies and guidelines that actively monitor and police SM engagement.

3.22 Much open source information, especially publicly available information acquired under contract or subscription and news media, is protected by copyright laws. NATO intelligence staffs are entitled to use NATO purchased copyrighted materials strictly in support of their duties and missions. NATO intelligence staffs are to be aware of the range of commercial subscriptions and services available to them and know the terms and conditions for use and release. Care must be taken, and due diligence applied to ensure these laws are abided by. Open source information may also contain private or personal information subject to protection in law. Care must be taken to ensure that any OSINT research, analysis, storage and dissemination comply with applicable data protection and privacy laws. When in doubt as to which laws apply, and how, legal advice should be sought.

²⁴ Active means engaging with social media through posting new content, or explicitly responding to posted content through text and/or emotional reactions, such as using the “like” button. Semi-active means implicitly responding to content through sharing it on a public forum. Passive means reading content without responding in any publicly discernible way.

3.23 **Operations security.** Maintaining OPSEC is critical to mission success and requires the appropriate technical and procedural means for open source collectors to deny an adversary the ability to better understand NATO, or its allies', intentions or capabilities. The technical specification of equipment, procedural governance and direction for open source capabilities should be adequately articulated through comprehensive security operating procedures developed in compliance with NATO security regulations. This includes accreditation of CIS through the CIS Planning & Implementation Authority, the Operational Authority and the Security Accreditation Authority.

3.24 Digital hygiene and digital footprint of activities surrounding publicly available information and OSINT must be carefully considered when conducting any activity in this area. Whilst NATO gateways provide a certain level of protection and control of access onto the Internet, they do not obscure or hide activity of an individual operating on behalf of NATO. Even overt activity within the publicly available information space requires Managed Attribution (MA) and OPSEC consideration that go beyond the standard individual use of the Internet.

3.25 Managed Attribution will be required for NATO personnel conducting OSINT collection. MA involves a solution designed to facilitate access to the Internet while providing protection of the identity of the operator and organization, and the concealment of activity through the use of assumed online identities. When licensing requirements prohibits obfuscation of the identity under MA, legal counsel must be consulted, though this should not discourage the use of MA to access licensed content on the Internet. Care should be taken that the provided managed attribution service is not linked to other NATO activities. Personnel must be thoroughly trained in the use of MA systems.

3.26 NATO personnel are not permitted to engage in OSINT collection activities that require false persona or active human engagement entailing false information or collection processes, tools and techniques.

3.27 **Training.** OSINT staff must be able to contribute to all aspects of the operations planning and intelligence production processes. They must be able to undertake their work based on a solid knowledge of the operating environment and the CCIRs. The key enabler for OSINT personnel, as some are not intelligence professionals, is training. Key training objectives for OSINT personnel, and other members of the intelligence staff working with OSINT are:

- a. The ability to identify and understand the nature and extent of the intelligence needed in support of the planning and conduct of operations. This requires a basic understanding of how intelligence and operations are planned and conducted;
- b. The ability to search, discover, acquire and access open source information efficiently and effectively;

- c. The ability to critically evaluate information and its sources and to process it into reliable intelligence;
- d. An understanding of the operations security concerns related to OSINT including the effective use of MA; and
- e. An understanding of the legal and economic issues related to the use of open source information.

Lexicon

Part I – Acronyms and Abbreviations

AAP	Allied administrative publication
AIIntP	Allied intelligence publication
AJP	Allied joint publication
AOSS	Allied open source system
ASG I&S	assistant secretary general for intelligence and security
CCIR	commander's critical information requirement
CIR	critical intelligence requirement
CIS	communication and information systems
CJ2	Combined Joint Intelligence Staff
CJ3	Combined Joint Operations Staff
CJ5	Combined Joint Planning Staff
CJ6 Staff	Combined Joint Command, Control, Communications, and Computer Systems
CJ8	Combined Joint Force Structure, Resources, and Assessments Staff
CJTF	Combined Joint Task Force
CM	collection management
CPED	collection, processing, exploitation, and dissemination
EEI	essential element of information
ENG	Electronic NewsGathering
HTML	Hyper-Text Mark-up Language

ICPP	intelligence collection and processing plan
IR	intelligence requirement
IRM&CM	intelligence requirements management and collection management
JIPOE	joint intelligence preparation of the operating environment
JISR	joint intelligence, surveillance and reconnaissance
MA	managed attribution
MOE	measure of effectiveness
NATO	North Atlantic Treaty Organization
OE	operating environment
OPSEC	operations security
OSINT	open source intelligence
PAI	publicly available information
PED	processing, exploitation, dissemination
PIR	priority intelligence requirement
PMESII	political, military, economic, social, infrastructure and information
PsyOP	psychological operation
RFI	request for information
SIR	specific intelligence requirement
SM	social media
SMM	social media monitoring

Part II – Terms and Definitions

actor

A person or organization, including state and non-state entities, within the international system with the capability or desire to influence others in pursuit of its interest and objectives. (*This term is a new term and definition and will be processed for NATO Agreed status*)

agency

In intelligence usage, an organization or individual engaged in collecting and/or processing information. (NATO Agreed)

battlespace

The environment, factors and conditions that must be understood to apply combat power, protect a force or complete a mission successfully.

Note: It includes the land, maritime, air and space environments; the enemy and friendly forces present therein; facilities; terrestrial and space weather; health hazards; terrain; the electromagnetic spectrum; and the information environment in the joint operations area and other areas of interest. (NATO Agreed)

analysis

In intelligence usage, a step in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation. (NATO Agreed)

casual source

Casual sources provide unsolicited information. Information provided by a casual source should be treated with caution, as the collector has no history to utilize in order to verify a source's reliability. (AJP-2; *This term is a new term and definition and will be processed for NATO Agreed status*)

collection

The exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. (*This term is a new term and definition and will be processed for NATO Agreed status*)

collection discipline

Intelligence collection disciplines are the means or systems used to observe, sense, and record or convey information of conditions, situations, threats and events. (*This term is a new term and definition and will be processed for NATO Agreed status*)

controlled source

Controlled sources are under control of an intelligence agency or organization, or specifically nominated intelligence staff. They can be tasked directly. (AJP-2; *This term is a new term and definition and will be processed for NATO Agreed status*)

deception

Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (NATO Agreed)

direction

Determination of intelligence requirements, planning the collection effort, issuance of orders and requests to collection agencies and maintenance of a continuous check on the productivity of such agencies. (NATO Agreed)

dissemination

The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. (NATO Agreed)

evaluation

In intelligence usage, a step in the processing phase of the intelligence cycle constituting appraisal of an item of information in respect of the reliability of the source, and the credibility of the information. (NATO Agreed)

integration

In intelligence usage, a step in processing phase of the intelligence cycle whereby analyzed information and/or intelligence is selected and combined into a pattern in the course of the production of further intelligence. (NATO Agreed)

intelligence cycle

The sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users. This sequence comprises the following four phases:

- a. Direction - Determination of intelligence requirements, planning the collection effort, issuance of orders and requests to collection agencies and maintenance of a continuous check on the productivity of such agencies.
- b. Collection - The exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.
- c. Processing - The conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation.
- d. Dissemination - The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. (NATO Agreed)

interpretation

In intelligence usage, the final step in the processing phase of the intelligence cycle in which the significance of information and/or intelligence is judged in relation to the current body of knowledge. (NATO Agreed)

Joint Intelligence Preparation of the Operating Environment (JIPOE)

"JIPOE provides an understanding of the operational environment and is a basis for planning. Drawing on the Joint Intelligence Estimate, it focuses the intelligence effort and delineates the prioritization of intelligence requirements. It is a living product and in addition to contributing to the early stages of the Operational Estimate, assists in the implementation of the plan by identifying opportunities to promote decisive action." (AJP-2; *This term is a new term and definition and will be processed for NATO Agreed status*)

measure of effectiveness (MOE)

A criterion used to evaluate how well an activity has achieved the desired result. (AAP-15 (2016) and Canadian defence terminology standardization board (2012))

open source intelligence

Intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access. (NATO Agreed)

operational level

The level at which campaigns and major operations are planned, conducted and sustained to accomplish strategic objectives within theatres or areas of operations. (NATO Agreed)

operational requirement

An established need justifying the timely allocation of resources to achieve a capability to accomplish approved military or civil objectives, operations, missions or actions. (NATO Agreed)

processing

The conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation. (NATO Agreed)

source

In intelligence use, a person from whom or a thing from which information can be obtained. (NATO Agreed)

strategic level

The level at which a nation or group of nations determines national or multinational security objectives and deploys national, including military, resources to achieve them. (NATO Agreed)

tactical level

The level at which activities, battles and engagements are planned and executed to accomplish military objectives assigned to tactical formations and units. (NATO Agreed)

uncontrolled source

Uncontrolled sources are those not under formal control of an intelligence agency or organization, or specifically nominated intelligence staff. Therefore, they cannot be tasked directly. (AJP-2; "this term is a new term and definition and will be processed for NATO Agreed status,")

Annex A OSINT sources

2. **Public speaking forums.** Public speaking, the oldest medium, is the oral distribution of information to audiences, during events that are open to the public or that occur in public places. These events, or forums, include but are not limited to academic debates, educational lectures, news conferences, political rallies, public government meetings, religious sermons, and commercial and scientific exhibitions. Neither the speaker nor the audience has the expectation of privacy when participating in a public speaking forum, unless there is an expressed condition of privacy. Unlike other open source collection, monitoring public speaking events is done through direct observation and, due to its overt nature, could entail risk to the collector.
3. **Public documents.** A document is any recorded information regardless of its physical form or characteristics. Like public speaking, public documents have always been a source of intelligence, and they generally provide more in-depth information than public speaking. Books, leaflets, professional journals, maps, manuals, marketing brochures, newspapers, photographs, public property records, and other forms of recorded information all yield information of intelligence value. The review of documents over time can contribute to the identification of trends in a potential operating environment.
4. **Public broadcasts.** A public broadcast entails the simultaneous transmission of information for general public consumption to all receivers or terminals within a computer, radio, telecommunications or television network. Public broadcasts are important sources of current information about the operating environment. These broadcasts often provide the first indications of developing situations. Journalistic commentary and analysis on radio, television, the Internet, social networks or other media outlets also provide windows into how governments, civilians, news organizations, and other elements of society perceive a specific situation. Public broadcasts are, however, particularly susceptible to be used for purposes of disinformation and propaganda. The characteristics of the media are listed at appendix 1.
5. **Internet.** The Internet is a global network of private, public, academic, business, and government computer networks. The Internet carries an extensive range of information resources and services, such as the inter-linked documents of the world wide web, the infrastructure to support email, and peer-to-peer networks.

- a. The world wide web is only one of various services available on the Internet. The unique aspect of the world wide web is that all information is linked using a standardized code (Hyper-text Mark-up Language – HTML) that is used to both identify the document and its location on the world wide web. Standardized coding also allows world wide web users to tag their documents with descriptive information which makes finding their documents easier. The

Web is generally fully accessible to any Internet user and its content can be accessed through common search engines.

- b. The Deep Web refers to content on the world wide web that is not accessible through a common search engine, although it is usually written in HTML. This content is sometimes also referred to as the hidden or invisible web. The Deep Web includes private web sites that require registration and login information before access can be gained and dynamic content pages which are returned in response to a submitted query or accessed only through a form. Dynamic content pages are hard to navigate without knowledge of the domain they are generated from.
- c. The Dark Web refers to a collection of websites that are publicly visible, yet intentionally hide the IP addresses of the servers that run them. The Dark Web is a portion of the Deep Web that has been intentionally hidden and is inaccessible through most web browsers. In many cases, websites hosted on the Dark Web are only accessible through encrypted networks that usually require specific software, configurations or authorizations to access.

6. **Social Media.** Social media refers to the interaction of individuals in which they share, and exchange information in virtual communities. Social media encompasses social network sites that use Internet and other telecommunication services to allow people to construct a public or semi-public profile within a network, define a list of other users with whom they wish to share information, and view and access their list of connections and those made by others within that system.

- a. In states where the government exercises direct-control of the media and the Internet, social media is a major influence in the respective societies. Social, cultural, and political movements, in addition to individuals, use social media capabilities to organize demonstrations and to rapidly spread their messages to large audiences, even globally. Social media provides subjugated populations with the ability to organize “virtually,” even in the face of physical repression. Analysis of social media content is fraught with potential danger as the users of social media are the ultimate uncontrolled casual sources. Analysis of social networks seeks to identify and comprehend the network nodes and relationships between them. These analyses require expertise built upon advanced multi-disciplinary knowledge of the social, mathematical, and anthropological sciences, concepts, and methodologies.
- b. While individuals around the world have gravitated to social media, so too have political organizations, governments, and commercial enterprises. As such, the content of social media can range from strictly controlled to completely uncontrolled. Some examples of social media are:

- (1) Blogs and micro-blogs;
- (2) Social networks;
- (3) Professional networks;
- (4) Video sharing²⁵ and streaming²⁶ (video weblogs);
- (5) Audio sharing and streaming (podcasts);
- (6) Photo sharing; and
- (7) Social bookmarking.

7. **Grey Literature.** Grey literature refers to information that is unclassified but not sold commercially. It could include working papers, technical reports, technical standards documentation, blueprints and technical drawings, data sets, and commercial imagery. Grey literature may be available through specialized channels or from direct access to organizations that produce it, such as non-governmental organizations, universities, public and private companies, professional societies, and government agencies.

²⁵ Sharing means making content (video, audio, or imagery) available online for the consumption of other users.

²⁶ A method of transmitting or receiving data (especially video and audio material) over a computer network as a steady, continuous flow, allowing playback to start while the rest of the data is still being received.

Appendix 1 - Media Characteristics²⁷

1. Most news media are involved in commercial competition for audiences. While individual journalists may have a personal view of events, their loyalty is to their editor's agenda and to their news organizations' commercial imperatives. Therefore, their primary goal is to produce newsworthy coverage and to produce it fast. They may appear sympathetic to the issue at hand, but their main concern is the production of information, which is commercially attractive and in line with editorial policy. One must be aware of the pressures journalists are under in order to evaluate media products appropriately.
2. Many journalists have only a limited understanding of events and issues. This means that their articles may be set out of context or be over-generalized. This lack of experience also means that they can have unrealistic expectations about what can be done, misinterpretations about what is being done, and a tendency to jump to conclusions.
3. In general, the mainstream media is under significant pressure to meet tight, and often fleeting, deadlines where their over-riding imperative is to be first with the news. The breaking story is all-important; sometimes this can be at the expense of depth, completeness, and most importantly accuracy.
4. A visual component can help make a news story which would otherwise fail. The quality or dramatic impact of video footage or pictures can determine whether a story is given airtime or not. Similarly, radio stories require background noise to underline the theme of the article and to add authenticity. In terms of grabbing attention and helping to shape perceptions, a picture can be the defining attribute.
5. It is widely recognized that there are differences in approach between media from different states. This is of particular note in multinational operations where cohesion of the Alliance is of critical importance. Therefore, it is important to note that coalition national media outlets may approach reporting of current NATO operations in a different manner, often introducing a national bias into the story.
6. Television and radio remain the main platforms for global news consumption. Digitized technology has radically altered television newsgathering, to the extent that it is now referred to as electronic newsgathering (ENG). Increasingly television news is as much about comment and entertainment as it is about comprehensive reporting. Satellite television news channels are gaining increasing importance around the world, where the appetite for news is relentless. The acceptance of presented television pictures can give television journalists excessive power to influence both public and political opinion. Radio is often a less sensationalist medium but the influence of radio news programs should not be underestimated. In the developing world, radio is often the primary source of news and information. In many less developed countries radio may be the primary source of news for

²⁷Adapted from Media Operations Doctrine of the United Kingdom.

a local population, particularly where literacy rates are low and local/regional newspapers are less established.

7. Increasingly, the Internet is becoming a major source of news and information. Engagement with online media has become important, particularly as adversaries seek to dominate this medium. The difficulty of identifying the origin of a website is, for many web-based journalists, the Internet's greatest advantage. It should be remembered that the Internet is unregulated and the ability to upload information is open to anyone with a proper device and communication link.

8. The collection and provision of information for the majority of media reporting is done by international news agencies. Each of these agencies maintains a sophisticated global operation based on the collection and distribution of their product to a wide range of media networks, acting as information wholesalers. Agency reporting, both for print and broadcast, tends to focus on hard facts leaving further interpretation and expansion to individual distribution networks.

9. Commercial analytical media companies focus on providing in-depth and predictive analysis, usually from strategic perspective, of topics such as politics, economics, and security and defence. They use analytical methods and techniques similar to those used by governmental intelligence organizations. These sources can cover a broad spectrum of topics and usually offer a broad range of subscriptions, from limited access to their databases and web pages to direct tasking. Some of these companies also use commercial imagery to obtain their desired information.

10. In regimes where the government or ruling elite exercises direct-control of the media, the propensity to engage in propaganda and deception is high. These regimes tend to control all forms of media, including online media. They also tend to block access to outside information sources, which generally results in a skewed view of the world, and local events, by any journalist trying to produce unbiased reporting.

NATO UNCLASSIFIED

AJP-2.9(A)(1)

NATO UNCLASSIFIED