NATO STANDARD

AIntP–22

OPEN-SOURCE INTELLIGENCE (OSINT) TACTICS, TECHNIQUES AND PROCEDURES

Edition A, Version 1

MAY 2022

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED INTELLIGENCE PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

10 May 2022

1. The enclosed Allied Intelligence Publication AIntP-22, Edition A, version 1, OPEN-SOURCE INTELLIGENCE (OSINT) TACTICS, TECHNIQUES AND PROCEDURES, 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 6537.

2. AIntP-22, Edition A, version 1, is effective upon receipt.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60.

Dimitrios SIGOULAKIS
Major General, GRC (A)
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
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

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
EST	Estonia implements AIntP-22 subject to the following reservations: 1) Estonia retains the sovereign right to describe all roles and functions of OSINT as described in the standard in the national framework (see Comment). 2) Estonia does not use the OSINT collection plan described in Annex A domestically. Estonia will use the OSINT Collection Plan described in Annex A only if the national OSINT component is deployed in NATO's multinational joint environment.
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. MC 0647 Policy on Open Source Intelligence (OSINT)
B. AJP-2 Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security
C. AJP-2.1 Allied Joint Doctrine for Intelligence Procedures
D. AJP-2.7 Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance
E. AJP-2.9 Allied Joint Doctrine for Open-source Intelligence
F. AJP-3.9 Allied Joint Doctrine for Targeting
G. AJP-3.10 Allied Joint Doctrine for Information Operations
H. AIntP-10 Technical Exploitation
I. AIntP-11 NATO Intelligence Training
J. AIntP-14 Joint Intelligence, Surveillance and Reconnaissance (JISR) procedures in support of NATO Operations
K. AIntP-16 Intelligence Requirement Management and Collection Management
L. AIntP-17 Joint Intelligence Preparation of the Operating Environment (JIPOE)
M. AIntP-18 Intelligence Processing
N. NATOTerm – Official NATO terminology database (English and French)

INTENTIONALLY BLANK

TABLE OF CONTENTS

TABLE OF FIGURES

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1 CONTEXT

In response to intelligence requirements following a tasking, OSINT is derived from the systematic collection, processing, exploitation, and dissemination (TCPED) of open source data and information, in any form.[1] As per other intelligence collection disciplines, OSINT delivers a comprehensive contribution to the intelligence cycle. It provides decision makers with intelligence produced from publicly available information (PAI) to support the full spectrum of military operations.[2]

1.2. SCOPE

This document provides common recommended Tactics, Techniques and Procedures (TTPs) allowing NATO and national OSINT capabilities to generate OSINT in support of NATO operations. It supports designated OSINT Joint Intelligence, Surveillance and Reconnaissance (JISR) assets with guidance to implement the standardized OSINT process that facilitates a respective staff's intelligence cycle with OSINT results.

1.3. PURPOSE

The aim of this document is to introduce fundamental TTPs to improve interoperability between OSINT assets/capabilities and to provide understanding for NATO staffs at all levels. This publication is not intended to restrict the development of tactics or additional procedures and techniques of national assets/capabilities. The requirement is that all intelligence components that may be tasked to conduct OSINT within a NATO multinational joint environment are able to do so through the application of the standard procedures outlined herein. This document should also serve as a reference for training in national capabilities.

1.4. APPLICATION

This document is primarily intended for designated OSINT assets/capabilities within the NATO framework, and nations providing OSINT assets/capabilities within the JISR process. It will also provide a standardized foundation for OSINT personnel, addressing the considerations and concerns they may encounter. Finally, these TTPs shall support the development of standard operating procedures (SOPs) across the Alliance with respect to OSINT utilization in NATO operations, exercises, training and trials.

[1] AAP 6, AJP 2.9.

[2] See AJP-2(B) Chapter 4.7 and Figure 5.

1.5. LINKAGES

Allied Intelligence Publication (AIntP-22) Open-Source Intelligence Tactics, Techniques and Procedures is a level-3 doctrine that supports NATO operations and is based on general and fundamental considerations contained in the Allied Joint Publication Allied Joint Doctrine for Open-Source Intelligence (AJP-2.9). AIntP-22 is linked to Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance (AJP-2.7).

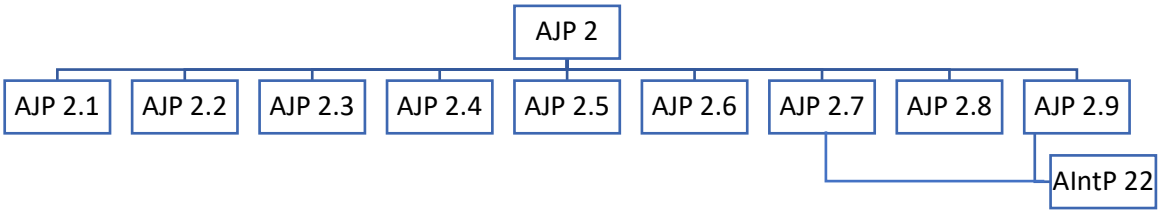

Figure 1: AJP-2 series

CHAPTER 2 THE OSINT PROCESS OVERVIEW

2.1. THE JISR PROCESS

2.1.1. Introduction

The JISR process is a coordination process through which intelligence collection disciplines, collection capabilities and exploitation activities provide data, information and single source intelligence to address an intelligence requirement. This can be accomplished in a deliberate, ad hoc or dynamic time frame in support of operations planning and execution. The JISR process consists of five steps: Task, Collect, Process, Exploit and Disseminate, referred to as TCPED.[3]

Figure 2: The JISR Process

2.1.2. JISR Architecture

In order to maintain the JISR process, a functioning JISR architecture is necessary. As part of NATO's intelligence architecture, NATO's JISR architecture consists of the organizations, processes and systems connecting taskers, controllers, collectors, exploiters, databases, applications, producers and requesters of data, information and intelligence and operational data in a joint environment. The JISR architecture facilitates the management of JISR results, enables JISR functions and supports intelligence and operations functions at all levels.[4]

2.1.3. JISR Task

A JISR task is a collection, processing, exploitation and dissemination directive for the appropriate employment of JISR assets. Depending on the considered JISR asset, JISR tasks may be refined into specific orders/formats to enable automated or standardized tasking of JISR capabilities.[5]

[3] AJP 2.7, 1.4 a, b.
[4] AJP 2.7, 1.4 c.
[5] AJP 2.7, 1.4 g.

2.2. OSINT CONSIDERATIONS

2.2.1. Introduction

In the operating environment, and the information environment in particular, certain factors need to be taken into consideration before describing the OSINT process. OPSEC, classification and the explicit legal situation have a significant impact on the generation of OSINT and need to be reflected in procedural adaptation of the generic JISR process in order to mitigate negative effects.

2.2.2. Automated Collection and Processing

In the environment of massive information flows, OSINT capabilities need to leverage automated collection and processing to augment and expedite manual collection and processing. This should be performed by an information system capable of collecting information from various publicly available sources, with advanced search and export options to meet NATO standard for ISR reporting and to encourage interoperability. This information system should cover at least the sources that have a high probability of contributing to the intelligence requirement (IR) response. The selective character of the open source information system has to be taken into consideration when verifying and corroborating information or evaluating a source. OSINT personnel need to be aware that any selective information system does not provide a comprehensive approach to the digital information sphere. It would be preferable if the OSINT information system was able to automatically identify basic metadata and entities mentioned in the source document.

2.2.3. Operations Security (OPSEC)

1. OPSEC is a process used to identify and protect critical information, using passive or active means, to deny the enemy knowledge of operational dispositions, capabilities or intentions of friendly forces, and as such, is mandatory for OSINT activities.

2. Digital hygiene and the digital footprint of OSINT activities must be carefully considered during the planning and collecting phases of an OSINT activity. Risk management, including use of managed attribution (MA), must be applied for any sensitive or discreet activity; however, even overt activity within the open source domain should involve OPSEC consideration.

3. MA and OPSEC are related terms since the former may enhance the latter. However, it should be noted that MA consists of procedural, policy and technical solutions for reducing or modifying the digital footprint with the purpose of protecting the collector and the interests of the organization. It should be noted that, in some cases, it is preferable to have a distinguishable digital footprint, for example, when conducting research on a source which would be alarmed by a severely reduced footprint.

2.2.4. Classification

1. The member state or NATO originator of OSINT has the sole responsibility in determining the security classification of the OSINT result and any additional release and handling restrictions. The classification and these conditions cannot be changed without the consent of the originator.[6]

2. Open source data before they have been processed are unclassified as they are available to a public audience. Aggregated PAI and especially OSINT, however, may be classified if it conveys topics and areas of NATO military interest or a national capability. When collection is in conjunction with a validated IR the results will need to be adequately protected through classification by the originator/drafter. Additionally, a higher classification may need to be given to a comment or assessment provided by the OSINT asset/capability. OSINT is regularly employed in the early stages of the operational planning process, so OPSEC has to be applied to preserve the secrecy of operational information.

2.2.5. Legal Situation

1. Every application of the JISR process under operational circumstances, including the wide array of topics covered by the OSINT process, has to consider national and international laws. OSINT methods and tools may be subject to legal constraints. OSINT activities conducted by OSINT personnel are to respect the constraints and restrictions imposed by national and international law and apply tools and methods which do not create the risk of legal liability for the Alliance.

2. As information is collected from sources via the Internet and other publicly available sources such as printed media, which are not constrained within national borders, the application of national and international law has many grey areas. OSINT personnel need to be aware of the limitations imposed by national and international law. Regular consultation with a legal advisor is advisable even for seasoned practitioners, as the legal and ethical framework is undergoing a constant transformation process.

3. While inadvertent collection is unavoidable, OSINT capabilities under NATO command should not purposefully collect personal information relating to private citizens of NATO nations, unless this is sanctioned by appropriate legal and policy authorities. NATO OSINT reporting should not be routinely directed at other nations within NATO. Information concerning NATO partners may be found in open source repositories.

4. Member states are responsible for their own OSINT operations and as such continue to operate under national laws when deployed to a NATO environment. As a result, they may have to place routine restrictions on releasability to NATO of nationally produced data, information and single discipline intelligence. Restrictions of this nature should be kept to a minimum and reconsidered in crises and operational situations.

[6] See NATO Security policy, NATO CM (2002)49.

INTENTIONALLY BLANK

CHAPTER 3 OSINT AS JISR PROCESS

3.1. OVERVIEW

3.1.1. Introduction

AJP-2, NATO Intelligence, Counter Intelligence & Security Doctrine, considers OSINT one of the primary intelligence collection disciplines. As such, the OSINT process is linked to the standard intelligence cycle, and adheres to the JISR process. The OSINT process consequently includes the steps of TCPED. OSINT assets are JISR assets. The OSINT process generates OSINT as single discipline intelligence/JISR result/OSINT result as it has not been processed in the main intelligence cycle phase of processing.

3.2. TASK

3.2.1. Introduction

1. The first step of the OSINT process is tasking. It is initiated with the receipt of validated collection requirements (CR) and consists of developing collection, exploitation and dissemination guidance, directives and orders to coordinate OSINT operations and assets. OSINT must be tasked through the intelligence requirements management and collection management (IRM & CM) process.

2. Deliberate tasking should be approved by a Joint Collection Management Board (JCMB). The board should convene on a regular basis to prioritize tasks that have a short turnaround time.

3.2.2. TTP T1: Task OSINT Asset/Capability

The NATO staff collection management element, determines whether or not the OSINT assets/capabilities assigned at the considered level of command can fulfil the collection requirements. This decision process is supported by dialogue with the IRM & CM element of the OSINT asset/capability, if capacity exists to have a dedicated IRM & CM element within the OSINT asset/capability. Alternatively, the OSINT liaison element within the staff CM element should be engaged.

3.2.3. TTP T2: Verify OSINT Task

Upon receipt of a tasking from IRM & CM, the OSINT capability needs to understand the scope and nature of the request, in consultation with the requestor, and then make a determination if sufficient resources exist to respond to the task. The task should be verified using the following criteria: specific, measurable, assignable, realistic and timely. The results of this decision need to be conveyed to IRM & CM. If the task is accepted, appropriate OSINT assets should be identified.

3.2.4. TTP T3: Legal Advice

In consultation with IRM & CM, consideration should be given as to whether the task needs to be referred to a legal advisor for guidance.

3.2.5. TTP T4: Operationalize OSINT Task

The OSINT asset/capability analyses the OSINT task in order to define the collection requirement and its corresponding indicators. At this time, formal parameters for output in terms of timelines and format should be established.

3.2.6. TTP T5: Assess the Threat

The OSINT asset/capability should determine and assess the threat level involved in the collection activity. A strategy to mitigate the assessed threat will be developed in the collection step.[7] The collection requirement should be assessed to determine the proportionality of risk vs. gain.

3.3. COLLECT

3.3.1. Introduction

The collection step of the OSINT process consists of three stages: (1) preparation (2) exploration and (3) focused collection. In the preparation stage, the OSINT collection asset/capability needs to build a collection plan in which a collection methodology will be outlined, according to the requisite risk management strategy, developed by the respective OSINT capability. The exploration stage will involve searching known sources and recording new ones. The final stage is focused collection, which may lead to extended collection, depending on the set timeframe. Sources should be evaluated during each stage and compiled to enhance a source registry. If evaluation is not possible within a step due to time constraints during critical operations, the evaluation should take place as soon as practicable and care should be taken to identify the use of an unevaluated source.

3.3.2. TTP C1: Develop Collection Strategy

1. The collection asset/capability assigned to the task needs to prepare by completing item analysis. This entails identifying pertinent information about the target in order to determine the best methodology for collection such as prevalence of Internet access, literacy rates, popularly used Internet and social media platforms, and languages spoken. This information can in turn be used to develop a collection strategy detailing a list of relevant keywords or queries in all applicable languages at the required classification to be discovered through a search engine or open source

[7] For additional information on threat levels, see AD 65-11, ACO Standing Policy and Procedures for Intelligence Production Management, 12 July 2010.

information system, tradecraft measures for obfuscations or data access as well as risk management measures. The list of keywords is important to update on a continual basis, with due consideration to the terminology used by the components of the information environment in which the collection activity is taking place.

2. The tasking may contain classified data. The collection strategy must take into consideration the fact that this data assists in understanding the request and guiding the collection.

3. As part of the planning stage of the collection step, a collection plan should be created, approved and archived by the OSINT capability management, or the OSINT asset/capability itself if no separate management exists. An example of a collection plan is included in ANNEX A.

3.3.3. TTP C2: Apply Risk Management Strategy

1. The OSINT asset/capability shall apply a risk management strategy based on the threat assessment conducted during the tasking step. The risk management strategy is the operationalization of measurements taken to prevent threats assessed during TTP T5. This should involve using managed attribution through a virtual private network or anonymous browsing software. An example of risk management strategy is included in ANNEX B.

2. Within the risk management strategy, each capability must engage their oversight and compliance personnel and/or legal department to seek advice for the use of credentials, unless otherwise predefined in the OSINT capability's respective SOPs. The unit commander must provide amplifying guidance, with consideration to national legal frameworks, stating that he/she accepts the risk to create accounts for collection purposes.

3. The creation of generic accounts utilizing the appropriate managed attribution is permitted for OSINT collection purposes. This should be considered only as a technical means to secure access to data. There should be no interaction or engagement with the target, although discreet interaction with the platform in so far as necessary to maintain access is permitted.

4. The use of false personas for collection of data from open source accounts is not permitted by OSINT personnel within existing NATO command structures. Private personal open source accounts of personnel should never be used for intelligence collection.

3.3.4. TTP C3: Source Exploration

The exploration stage involves searching known sources and exploring new and unfamiliar ones, which will be evaluated during the exploitation step. Source exploration collects information on the author and agency, the author's bias or agenda in publishing the information, the author's expertise or affiliations, the date of most

recent update, and the date of publication. Source exploration allows OSINT personnel to make a preliminary assessment of the extent to which the source could be used, lays the foundation for a source evaluation, and facilitates discovery of other independent OSINT sources that could be used for verification.

3.3.5. TTP C4: Exploratory Collection

1. Exploratory collection is preliminary searching to uncover relevant sources of information to satisfy the intelligence requirement. This process includes conducting introductory research into the subject in order to better understand the context. In the course of the investigation, new and unfamiliar sources will be discovered and should be evaluated and recorded prior to inclusion in the OSINT result. As with Source Exploration, Exploratory Collection should strive to collect and record a diverse array of independent OSINT sources. Preference should be given to primary sources[8]. One strength of OSINT is the ability to verify data or information from different open sources in order to ascertain relevance and veracity.

2. If any problems of accessibility occur at this point, the information technology (IT) support element of the OSINT asset/capability should be notified in order to affect a resolution.

3. Collection activity can be assisted or enhanced through the application of algorithms employed by data scientists or tools.

4. During this stage, guidance should be sought from the tasking authority and/or legal advisor, if required.

3.3.6. TTP C5: Focused Collection

Once the sources best suited for the collection task have been identified and evaluated, focused collection should take place within the set of collection parameters, as established by available time and policy and legal considerations. The focused collection efforts should emphasize collection from high value sources, especially primary sources, for optimal results. Sources which are suitable for repeated use should be collected into a source registry at the appropriate classification. Collection should be conducted in an automated fashion, if possible.

3.3.7. TTP C6: Extended Collection

Depending on the set timeframe and number of assigned personnel, an extended collection stage can add to the breadth and depth of focused collection activity. Secondary sources[9] identified during exploration and focused collection which require additional investment of time and effort serve as a starting point for extended collection. Any result collected during this stage can trigger an iteration of the collection step.

[8] Primary sources are first-hand accounts from people who had a direct connection with the information
[9] Secondary sources are one step removed from primary sources but often quote or otherwise use primary sources. They can cover the same topic, but add a layer of interpretation and analysis.

3.4. PROCESS

3.4.1. Introduction

The processing step of the JISR process differs from that of the intelligence cycle in that it does not include analysis and is purely technical in nature.

3.4.2. TTP P1: Compile Relevant Data

The data collected during the collection step should be analysed for relevance. Any irrelevant data can be deleted or disposed of in accordance with legal framework. Remaining data should be stored in accordance with mission guidelines and prepared and sorted for processing.

3.4.3. TTP P2: Translation

1. During this stage, all foreign language data should be machine translated to identify relevant data for further processing. Relevant foreign language data should either be translated into the working language, or a synopsis of the content should be produced.[10] Both the translation and the original should be retained, and may be included in the result if assessed to be relevant. Foreign language capacity within an OSINT capability is highly valuable. The number of linguists and languages covered are mission dependent; however, OSINT capabilities should ideally have linguists for common languages. The defence intelligence community, or other reach back OSINT capabilities, can be used for translation of other languages.

2. It is recognized that linguists are a scant resource, therefore, in the event that linguists are not available, machine translation tools may be employed, although the translations they offer may be limited, particularly if the text being translated includes colloquialisms. When machine translation has been utilized, it should be annotated in the result.

3. When using linguists or machine translation tools due consideration for OPSEC should always be a factor. Copying relevant text into an online translation tool may risk compromising intentions. Whenever possible, it is preferable to use offline machine translation tools or tools on a secure network.

3.4.4. TTP P3: Add Metadata

Standardized metadata should be determined and annotated on the document, or on an accompanying form. Metadata assists in future retrieval of the data, and so should be as detailed and consistent as necessary for this purpose.[11] Most metadata can be

[10] The two official languages of NATO are English and French.
https://www.nato.int/cps/en/natohq/faq.htm
[11] Metadata should be included IAW the Dublin Core Metadata Initiative http://dublincore.org/

collected automatically via an open source information system. This can consist of automated detection of entities mentioned in the document.

3.4.5. TTP P4: Collate Data

1. Collation is an activity in which the grouping together of related items of information provides a record of events and facilitates further processing.

2. Collation involves the actions of receiving, grouping and recording all new data and/or information by registering it in databases and tagging it with appropriate categories. In order to be efficient, collation must follow a common, standardized set of rules. The purpose of collation is to make it possible to sort, filter and group together available information, which later in the analytical process can be extracted.

3. Collation is the key activity during the preparation stage to make information and intelligence available for the analytical process. Collation is concluded with a fully consolidated data set. These data sets are intended for exploitation, and as such, are not meant to be distributed beyond the OSINT asset/capability.

4. Collation activity can be assisted or enhanced through the application of algorithms employed by data scientists or tools.

3.4.6. TTP P5: Store Open Source (OS) Data

Information, in particular personal data, should be stored using the need to know principle and in accordance with application policies and laws. All sensitive information should be deleted when it is no longer required in accordance with legal frameworks.

3.5. EXPLOIT

3.5.1. Introduction

1. In the exploitation step, OSINT personnel transform processed, verified data into an OSINT result. It consists of four stages: (1) source evaluation, (2) OSINT result generation, (3) assessment and (4) review. There are two main types of exploitation: quantitative and qualitative. Both are used in combination to generate reliable OSINT tailored to the mission. Exploitation should be undertaken on the basis of verified information.

2. Verification refers to the factual comparison of a source’s content with other independent OSINT sources that either support or refute the provided content. It aims at establishing the veracity and currency of the content, providing an assessment for the credibility of the source. Additional independent OSINT sources that verify the content lend strength to the verification. The veracity and currency of the information is established by verification through at least one other independent open source. Each piece of information or data that is relevant to the OSINT result should be verified. If

verification is not possible, the information or data should be marked as non-verified. Preference should be given to primary sources.

3. Advanced quantitative exploitation is supported by data scientists or tools employing algorithms, statistics and other approaches to visualize, interpret and interrogate all available information applicable to relevant variables in order to generate insight and predictive analysis based on analytic methodologies and tradecraft.

4. Qualitative exploitation is conducted by personnel who employ analytic tradecraft, on the basis of verified, processed information and experience to identify and employ only the relevant pieces of information in order to draw meaning from the collated sources and communicate it in a clear and concise manner as single discipline intelligence. Qualitative exploitation is especially apt to determine the quality of parameters used in quantitative exploitation and to provide in-depth analysis of a given subject matter.

5. Different levels of exploitation can exist within an OSINT asset/capability. The initial level of exploitation is the rapid and preliminary assessment of collected verified information. This type of exploitation is usually conducted by the exploiter associated with the collection asset. Further exploitation involves a more detailed evaluation of collected data and information – eventually in accordance with exploitation tasking of other assets in other exploitation levels.

3.5.2. TTP E1: Source Evaluation

1. New and unfamiliar sources should be fully evaluated before use in the production of the OSINT result. OSINT personnel should build on the information collected during the Source Exploration stage to conduct source evaluation. The source evaluation should determine the reliability and credibility of a given source by looking at technical aspects, background of the publishing actor and content of the source. The result of the source evaluation is the overall rating of the source. In some cases, source evaluation could be an OSINT result on its own.

2. The reliability of a source indicates the potential added value to the intelligence community. While criteria such as financial and corporate background information should be considered, the credibility rating of the information provided by the source is an important factor. Verification of information provided by a source – regardless of an existing rating – should be undertaken. Source evaluation needs to be performed whenever collecting from a source, especially for the first time, and the source registry updated accordingly.

3. The information credibility rating indicates the credibility of one specific article, post or other piece of content. The credibility of the information has to be rated according to, but not limited to, the criteria as follows: whether the given information is original or duplicated from other sources; whether the content of the posted information is confirmed by facts over time; whether information is presented selectively or objectively; and whether the information can be verified by independent OSINT

sources. As credibility is directly linked to each individual piece of information from a source, a complete source cannot be given a single credibility rating. Evaluation of the credibility of pieces of information provided by the source over time contributes to an aggregated reliability rating of the source. The reliability of a source can vary with the veracity and accuracy of each piece of information collected in a collection activity. Therefore, the overall source rating does not necessarily include the numerical credibility rating after conducting a source evaluation for the first time.

4. Reliability and credibility in the information environment are important issues due to the vast number of sources and types of content, such as news media, grey literature and social media. The Overall Rating of a source should be adjusted from the preliminary reliability rating according to the credibility of information provided by that source over time. The Overall Rating of a source is expressed with the alphabetical value A through F (see Table 1). It should be accompanied by an assessment to provide a better understanding of the overall rating of the source. This helps to clarify if the source is especially (un-)reliable with regard to a certain subject matter. Thus: the overall rating for a source consists of that reliability rating combined with the credibility rating of that piece of information/content. The evaluation process is further explained in ANNEX C.

5. Evaluated sources should be added into a source registry that is maintained by OSINT capabilities. The source registry should include the name of the source, the evaluation rating (as per the NATO source reliability and information credibility matrix), the date of evaluation, and the contact information of the OSINT asset/capability who completed the evaluation. The evaluation of a source should regularly be revised to cover any changes which may occur in the source's reliability or credibility. The registry should be used to prioritize sources for further collection activities. The registry should be used with caution as sources may vary in reliability significantly by article, which will trend to an average rating that does not reflect them accurately.

6. Reliability and credibility ratings should always be determined on the grounds of a valid source evaluation. If operational requirements preclude conducting an immediate source evaluation, results should be included with a source rating of F, with a caveat as a comment that the source has not been verified. Follow up of the source should be conducted as soon as practicable, and if possible, within the time frame of the operation. A source rating of F does not exclude the source from use.

3.5.3 TTP E2: Assessment

1. To further enhance the value of the collected and processed data and information, additional comments and/or assessments may be added in order to provide background or alignment for the requester. It is strongly recommended that a source reliability and information credibility code be assigned and added to the OSINT result. A more in-depth assessment involves using the background or reach back database of the OSINT asset/capability. This level of exploitation often requires additional tools, processing power, and/or additional specific expertise. It can be time

consuming and may be conducted in the joint operations area (JOA) or via reach back capabilities.

2. Note that even if the underlying data and information is unclassified, the specialist's assessment may change the classification of the result.

3.5.4. TTP E3: Generate OSINT Result

Production within the exploitation step is concluded by the generation of an OSINT result: all and only relevant exploitation results are aggregated into a requested result (which can consist of several documents, annexes, etc.). The exploitation results are achieved by using a combination of qualitative and quantitative exploitation based on verified information. The relevance of the result is determined by reviewing the requirement. If and when necessary, the result is supplemented by an overall assessment. Caution and consideration should be given to the scope of assessments based on single discipline collection. OSINT personnel should endeavour to contain comments to their subject domain. If any personnel need to relay valuable information outside of his or her subject domain, this should be annotated in the comment. Intelligence gaps should be determined at this point so that they may be conveyed to the requestor, and/or IRM & CM in the dissemination step.

3.5.5. TTP E4: Review

At the conclusion of the exploitation step, a mandatory review of the result is conducted. During the final review by the releasing authority, care should be taken to ensure that sensitive information is deleted in accordance with legal and policy constraints and that steps have been taken to protect sensitive sources.

3.6. DISSEMINATE

3.6.1. Introduction

The OSINT result is delivered to the IRM & CM function and transmitted to the requesters as specified by the original OSINT task. In accordance with theatre/exercise guidance, there may be additional dissemination paths. With appropriate consideration given to need to know, classification and copyright, OSINT should be disseminated as widely as possible.

3.6.2. TTP D1: Classify OSINT

Due consideration should be given to the potential for OSINT to require a higher classification because of the aggregation of information or the protection of OSINT methods, capabilities and sources. The OSINT specialist's assessment may change the classification and/or releasability marking of the OSINT result. Caveats may need to be included with unclassified results to ensure distribution is limited to those with the need to know, and in order to respect applicable copyright laws. The use of tearline

reporting is also a way to mitigate the distribution of sensitive information. The responsibility for classifying OSINT remains solely with the originating nation or NATO capability.

3.6.3. TTP D2: Disclaimers

1. In the case where the inclusion of graphic or offensive material is necessary to convey intelligence, it is advisable to include a warning at the beginning of the OSINT result and dissemination should be limited accordingly.

2. In the case where requested information mentions a NATO member or partner, it is advisable that a disclaimer be added to indicate that this is not the view of the OSINT asset/capability conducting the collection activity.

3. Where necessary, OSINT results should include a caveat or disclaimer that they should only be shared with the intended audience and not further disseminated without consultation with the originating asset/ capability. An example of disclaimer language is included in ANNEX E.

3.6.4. TTP D3: Approve OSINT

OSINT personnel with relevant release and disclosure training should verify that the classification and releasability of the OSINT result is in accordance with theatre/exercise guidance. At this time, the OSINT result should be sent to the releasing authority for final approval.

3.6.5. TTP D4: Disseminate OSINT

1. OSINT results should be released in the format specified by the tasker in accordance with theatre/exercise guidance that includes metadata completion. Due consideration should be given to the means by which OSINT is disseminated, including via appropriate classified domains.

2. A record should be kept as to when the OSINT result was disseminated, to whom, by what means, and whether or not receipt has been acknowledged.

3.6.6. TTP D5: Solicit Feedback

Once the result has been received and digested by the tasker, the OSINT asset/capability should actively solicit feedback through the client and/or stakeholders about the relevance, quality and usability of the delivered OSINT result in order to provide amplification if required, and to improve future collection and production efforts. The OSINT asset/capability should process/evaluate the received feedback, and, if desired, initiate the process to convert lessons identified (LI) into lessons learned (LL) and best practices.

3.6.7. TTP D6: Process Review

Questions, problems, and concepts applied during all steps are evaluated. They may lead to coordinated adaptions of the tasking, collection, processing, exploitation, and dissemination steps of the OSINT process.

INTENTIONALLY BLANK

CHAPTER 4 OSINT FUNCTIONS AND RESPONSIBILITIES

4.1. OVERVIEW

4.1.1. Introduction

1. The size and organization of an OSINT capability will vary depending on the level of command, the mission, and the available resources. As the size of the OSINT capability increases, function can be expanded and roles diversified.

2. As the focus of the OSINT capability is to collect, process and analyze data from open sources to produce intelligence results fulfilling the OSINT tasking, the position of collector/sensor in the appropriate role/environment is imperative. Collectors can be organized in a variety of different ways depending on the mission, available resources, and expertise of personnel. Options include, but are not limited to: division by theme, geography or type of source (e.g. social media, text, imagery, video, audio.)

3. In the case where insufficient resources exist to dedicate an individual to each role/function, a single individual can fill multiple roles. Other solutions to mitigate limited resources include: consulting external resources, such as legal/policy, or sharing resources with other assets, such as a common IRM & CM asset.

4. The table below outlines the roles and responsibilities of each function within an OSINT capability. Not every position needs to be filled in order to be considered a fully established OSINT capability. Suggested priorities are annotated; however, these will vary depending on mission and mandate.

4.2. ROLES AND FUNCTIONS

Priority	Function	Roles, Responsibilities, and Skills
1	Manager	• Implement process innovation • Constantly improve quality of OSINT results • Examine the IRs to ensure coherence and appropriately task available open source resources • Manage human and financial resources • Promote and represent OSINT department to commanders/beneficiaries • Plan & implement OSINT policy • Maintain permanent contact with customers • Explicitly solicit and acquire feedback for OSINT results to focus or redirect collection • Provide advice on releasability, in conjunction with foreign disclosure officer (FDO) • Maintain current understanding of OSINT

1	OSINT Collector/Sensor	• Deconstruct complex problems • Be aware of cognitive biases • Use scientific search methodologies • Use specific & technical collection tools • Identify, evaluate, and select sources • Perform exploitation of content • Draft reporting in relevant way • Have good understanding of technical domain in which they are collecting • Assess source credibility in context • Trained in collection tradecraft (as per STANAG 2555) • Build relations with the professional community inside and outside of NATO
1	Source Evaluation	• Identify new sources with an understanding of intelligence requirements • Evaluate sources to include subscription databases • Maintain standardized source registry • Good understanding of media landscape • Advise analysts on source reliability and limitations
1	Security	• Maintain network security • Evaluate and recommend managed attribution solutions • Monitor network activity to ensure policy compliance
2	OSINT Analyst	• Cooperate with open source collector to guide collection • Clarify intelligence requirement with collection manager • Deconstruct complex problems • Produce single discipline analysis of content using scientific analytical methodologies and critical thinking techniques with an awareness of cognitive biases • Ability to predict future outcomes based on analytical tradecraft • Possess advanced writing skills • Have a background in open source collection or in analysis in another collection discipline • Trained in analytical tradecraft (as per STANAG 2555)

		• Build relations with the professional community inside and outside of NATO
2	Linguist/Cultural Advisor	• Translate • Be proficient according to NATO standard Level 3 • Provide cultural context
2	Data Scientist	• Design and implement innovative ways to interpret and exploit collated data • Implement a data repository interoperable with other NATO systems • Structure data in a common format using agreed standards • Extract/add metadata to available information • Implement solutions for predictive analysis from big data repository based on intelligence requirements.
2	Trainer	• Provide OSINT familiarization training to organization • Attend and evaluate commercial and allied training sessions • Practical experience with OSINT tools and methods gained through working in a nation or in NATO as an OSINT collector
3	Software/application developer	• Ensure interoperability with other entities/systems • Write scripts and/or create tools to automate functions and processes • Advise commander on technical solutions • Software development • Design and develop platforms for online information sharing • Translate functional into technical requirements/technical writing • Express information and communications technology requirements • Proficient in at least one programming language • Strong understanding of OSINT information environment
3	Technical Innovation	• Keep abreast of emerging technologies • Recommend innovative technologies, taking interoperability into consideration • Assist analyst in the formation of technical requirements

		• Business processing analysis and information flows • Make new sources available to community • Liaise with the NATO Science and Technology Organization (STO)/NATO Allied Command Transformation Operational Experimentation (ACT OPEX) • Advise NATO to invest in up and coming data sources
3	Outreach Entity	• Liaise with academics, government organizations, non-government organizations (NGOs), research centers and commercial entities
3	Information Management	• Maintain OSINT portals • Tag OSINT information for future discovery • Airgap data between systems
4	IRM & CM	• Coordinate open source collection efforts • Participate in collection coordination • Facilitate dissemination • Maintain close connection to OSINT stakeholders
4	Legal counsel/Policy Advisor	• Provide advice on copyright issues • Provide advice on data protection and privacy • Provide advice on security & communication laws • Support procurement, licenses • Provide advice on use of social media accounts for open source collection purposes • Provide legal/policy advice about collection and retention of information
4	Procurement/Contracting Officer	• Write contract specifications • Support contract negotiations • Liaise with procurement agency • Data and services acquisition/procurement
4	IT Support	• Resolve issues with system access • Troubleshoot equipment problems

LEXICON

PART I – LIST OF ACRONYMS

ACO	Allied Command Operations
ACT OPEX	NATO Allied Command Transformation and Operational Experimentation
AOR	area of responsibility
BDA	battle damage assessment
CR	collection requirement
DDoS	distributed denial of service
EEI	essential element of information
FDO	foreign disclosure officer
HUMINT	human intelligence
IP	Internet protocol
IR	intelligence requirement
IRM & CM	intelligence requirements management & collection management
JCMB	Joint Collection Management Board
JOA	joint operations area
JIPOE	joint intelligence preparation of the operating environment
JISR	Joint Intelligence Surveillance Reconnaissance
LI	lessons identified
LL	lessons learned
MA	managed attribution
NCS	NATO codification system
NGO	non-governmental organization
NSO	NATO Standardization Office
OPSEC	operations security
OS	open source(s)
OSINT	open-source intelligence
OSINTREP	open-source intelligence report

PAI	publicly available information
PIR	priority intelligence requirement
RFC	request for collection
RFI	request for information
SA	situational awareness
SIGINT	signals intelligence
SIR	specific intelligence requirement
SOP	standard operating procedure
STO	Science and Technology Organization
TCPED	Tasking, Collection, Processing, Exploitation and Dissemination
TTP	tactics, techniques, and procedures

PART II – TERMS AND DEFINITIONS

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

collation
In intelligence usage, an activity in the processing phase of the intelligence cycle in which the grouping together of related items of information provides a record of events and facilitates further processing.
(NATO agreed)

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.
(NATO agreed)

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.

data
Raw, discrete facts, such as measurements, statistics, or entities, used as a basis for analytic work. A single piece of data often has little meaning in isolation.
(AJP 2.0/AJP 2.9)

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)

discreet
Discreet activity is deemed to be generally passive, masked to the source owner or non-attributable identity.
(AJP 2.9)

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)

information
Unprocessed data of every description which may be used in the production of intelligence.
(NATO agreed)

information environment
An environment comprised of the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs.
(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)

Joint Intelligence Surveillance and Reconnaissance (JISR) asset
An individual, detachment, unit, sensor, or platform that can be tasked by respective authorities to achieve joint intelligence, surveillance and reconnaissance results.
(NATO agreed)

Joint Intelligence Surveillance and Reconnaissance (JISR) capability
An asset or set of assets, including supporting organizations, personnel, collectors systems, supporting infrastructure, processing, exploitation, and dissemination processes and procedures, used to achieve a designated joint intelligence, surveillance and reconnaissance result.
(NATO agreed)

Joint Intelligence Surveillance and Reconnaissance (JISR) result
The outcome of the joint intelligence, surveillance and reconnaissance process disseminated to the requester in the requested format.
(NATO agreed)

Joint Intelligence Preparation of the Operating Environment (JIPOE)
The analytical process used to produce intelligence estimates and other intelligence products in support of the commanders' decision-making and operations planning.
(NATO agreed)

joint operations area (JOA)
A temporary area within a theatre of operations defined by the Supreme Allied Commander Europe, in which a designated joint force commander plans and executes a specific mission at the operational level.
(NATO agreed)

open-source intelligence
Intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access.
(NATO agreed)
It is derived from the systematic collection, processing and exploitation of open sources of information and data of any form in response to specific intelligence requirements.

sensitive information
Information that, as determined by a competent authority, must be protected because its disclosure, modification, destruction, or loss will cause perceivable damage to someone or something.
(NATO agreed)

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

INTENTIONALLY BLANK

ANNEX A COLLECTION PLAN

This annex does not represent standard NATO procedure, but is intended only as a collection of best practices.

The following format provides an example of how to Operationalize the OSINT Task (T4) and develop the collection strategy (C1).

The purpose of this annex is to:

1. Assist the operator in refining their requirements;
2. Keep a record of where and what was searched for legal purposes, or to assist in tracking the sources used for the collection activity over time. Populating the queries field below with search strings used in a database or search engine could be used for this purpose.

Before creating the collection plan, the operator should consult with the requestor/customer to better understand the requirement and define the parameters, including, but not limited to, geographic boundaries and historic range.

This collection plan should be updated throughout the search process as new information is discovered.

In building the collection plan, due consideration should be given to the amount of time and the number of resources available to be dedicated to the collection activity.

According to standard procedure, the aggregation of the data in the collection plan below may make this document classified and create the need to store it on a system other than the one the operator is using to conduct the collection activity.

A collection plan should be prioritized to allow optimal usage of limited resources. It should aim at putting the topic into a comprehensive context, capturing the spectrum of relevant and plausible facts and opinions from a full range of sources, and uncovering patterns and inconsistencies. This helps to mitigate bias inherent in every source.

It is not a requirement to fill all of the fields below. This is a guideline to focus thinking before commencing the collection activity.

Intelligence Requirement
Concept/Topic/Question:
RFI #/PIR/SIR/EEI
Client: Name: Email: Phone: Mail:
Due Date:
Dissemination Format: Report, Briefing, Other

Can the topic be broken down in sub-topics?
Sub-Topic 1:
Sub-Topic 2:
Sub-Topic 3:
Sub-Topic 4:
Sub-Topic 5:
Sub-Topic 6:
Sub-Topic 7:
Sub-Topic 8:
Sub-Topic 9:
Sub-Topic 10:

What is already available?

Topic Semantics	
Spelling	
Language	
Singular - Plural	

Technical Language/Jargon	
Popular vs Scientific	
Acronyms	
History	
Synonyms	
Quasi Synonyms	
Antonyms	
Homonyms	
Heteronyms	
Specific - General	

Viewpoint	

Who might produce this information?	
Publishers	Commercial
	Free Websites
	Databases
News Services	Radio
	TV
	Internet
	Press Releases
Known Experts	Interview
	Social Media
Organizations	Conference Paper
	Conference Proceeding
Academic	Abstract
	Article
	Book
	Dissertation
Social Media	Chat Room
	Discussion Group
	Blog
	Video Sharing
Government	Official Gov't Docs
	Official Gov't Records
Company	Company Reports
Reference	Bibliography
	Catalogue
	Dictionary
	Encyclopaedia
	Index
	Taxonomy
Graphics	Infographics
	Images
	Maps
	Forms (Ephemeral)

Grey Literature	Leaflet
Other	

What are the Search terms/Queries already used	
Search Terms	
Queries	

ANNEX B RISK MANAGEMENT STRATEGY

This annex does not represent standard NATO procedure, but is intended only as a collection of best practices.

A Risk Management Strategy consists of two components:

ANNEX B1: A Risk Assessment; and,

ANNEX B2: A Risk Mitigation Strategy.

ANNEX B1 is intended to address considerations to determine the level of risk. If the risk is assessed to be low, additional risk mitigation beyond normal OPSEC may not be required. ANNEX B2 is intended to assist the OSINT practitioner in determining the best strategy to mitigate the risk.

Note that not all of the considerations are applicable in every scenario. It is up to the individual practitioner, in conjunction with the responsible security officer or team lead, to determine which aspects are relevant based on the assessed risk and the assigned task.

B.1. RISK ASSESSMENT

Legal and Policy Considerations

- Outline the nexus between the activity you will carry out and the authorized mission or defence mandate it will support (include under what national or international law information will be collected).
- Ensure the proposed activity is not in violation of any approved regulations, policies or guidance.
- If the objective of the collection activity includes the collection of personal information, ensure that this is elaborated in the mission mandate. Determine what measures will be put in place to track/monitor collection of personal information and its subsequent use. The collection, storage of personal data must be consistent with applicable national and international law.
- If the collection of personal information is unintended, ensure that the OSINT personnel understand the procedure to record, report, and consult. Ensure the personnel understand what constitutes unintended collection in this context.
- Consider any oversight mechanism(s) planned for the activity.

Identify Threat in Context of Collection Requirement

- Outline the activity and the operational effects the IRM & CM element has indicated are to be achieved through the collection (e.g. Force protection, targeting/battle damage assessment (BDA), situational awareness (SA), joint intelligence preparation of the operating environment (JIPOE), surveillance). Include conditions or time based end state.

- Identify the threat(s) and its intent with relevant statements to its capability & intent in the digital environment.
- Consider both the risks of conducting the proposed activity, and the risk of not conducting the activity.
- Explain in detail how the information collected will be processed into intelligence.
- Identify potential conflict with other agencies' open source information collection and communicate with the IRM & CM element.
- Consider with whom will you collaborate/share/disseminate open source information.

Information Security

- Consider the nature of the keywords/selectors/data against which you are collecting. A best practice is to query the originator of the intelligence (i.e. HUMINT/SIGINT) to determine if releasing it into the open source domain constitutes an OPSEC concern. Bear in mind that the release of data in aggregate may present an unacceptable level of risk, even when the individual data components are unclassified.

B.2. RISK MITIGATION STRATEGY

Training

- Ensure that the operator(s) are trained on all tools and systems required to carry out the collection activity IAW NATO standards. Good tradecraft is a component of a robust risk mitigation strategy.

Technical

- An approved managed attribution solution should be employed for all queries with some level of risk, as required by policy. In developing the IT infrastructure used for managed attribution the following criteria should be considered, based on the risk assessment:
  - Unfettered, non-attributable internet access
  - A virtual machine and/or virtual private network
  - Methodology for data transfer and retention
- All users should be appropriately trained on system functionality and have signed a user agreement for the system
- Experienced personnel should be charged with regular system maintenance and to periodically conduct penetration testing to ensure that there is no risk of data spillage or contamination
- System usage should be monitored and violations addressed as appropriate.

Sources

- Describe the tools you will be using to gather information on the Internet (i.e., third-party service provider, application programme interface (API), purchase of data, etc.).

- Identify functionality/utility of all proposed collection sources, and Methods of Access (including access software). It is often useful to illustrate in a diagram the authorities, flow of information, as well as the physical location of network infrastructure and virtual location of the activity.
- All third-party sources, including vendors of commercial tools, which are acquired or engaged by the OSINT function should be vetted in order to determine how much information about the government agency/NATO body will be collected, retained and shared.

Information Management

- Information collected should be stored on the appropriate system as per its classification, with due regard to the potential for increased classification related to data aggregation.
- Information should be retained IAW NATO and/or local policies.

INTENTIONALLY BLANK

ANNEX C SOURCE EVALUATION

Part I Introduction

This annex does not represent standard NATO procedure, but is intended only as a collection of best practices.

For further clarification and amplification refer to the OSINT Handbook (to be promulgated)

To the greatest extent possible the methodology of source evaluation should be in accordance with standard NATO procedures based on the NATO source reliability and information credibility matrix and rating system.

The Source Evaluation Process aims at assessing the value of a given open source and the information provided by it for usability within intelligence in general (i.e. PAI) and OSINT specifically. For every open source used within an OSINT activity a Source Evaluation should be conducted.

Source Evaluations should be revised periodically. A revision is also recommended if the environment and situation of an open source are deemed to have significantly changed since the last evaluation.

Source Evaluations are primarily conducted by OSINT exploitation personnel specialized in Source Evaluations. Reliability and credibility ratings follow the NATO source reliability and information credibility matrix as defined by AJP-2. In case a source is reliable and/or credible on a certain subject but unreliable and/or not credible on other subjects, care should be taken to indicate this clearly in the source evaluation.

Only evaluated sources should be included in the OSINT capability's Source Registry. Inclusion, however, is conducted regardless of the result of Source Evaluation: reliable sources are to be included as well as unreliable sources or sources assessed to be misinformation or disinformation.

A Source Evaluation consists of three parts: (I) Source Reliability, (II) Credibility of Information, (III) Overall Rating.

Reliability of the source		Credibility of the information	
A	Completely reliable	1	Confirmed by other sources
B	Usually reliable	2	Probably true
C	Fairly reliable	3	Possibly true
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged

Table 1: Evaluation and Rating[12]

[12] AJP-2, Chapter 4.4.2, Figure 4.

Part II Process

Overview

During source evaluation OSINT personnel should combine information on technical aspects of the source, background of the publishing actor and the content of the source. The information on these three elements is then used to assess reliability of the source and credibility of the information.

The element(s) to emphasize within an individual Source Evaluation depend(s) on the source being evaluated and the specific Collection Task.

Technical Analysis

Technical Analysis aims to provide a comprehensive description of the technical parameters of a digital source. While evaluating technological aspects OSINT personnel should attempt to identify as much technological background information on the source. This includes – but is not limited to – internet protocol (IP) address, Domain Name System (DNS), shared servers, frameworks used, server hardware used, possible use distributed denial of service (DDoS) protection services and integration with other services.

As the technical domain is evolving rapidly, OSINT personnel should be aware of the evolving changes and conduct technical analysis of technical elements in the current information environment.

Background Analysis

Background Analysis aims to provide a comprehensive description of the background of the actor publishing the source. During the Background Analysis OSINT personnel should attempt to create a clear source description.

Among other background information found, the following should be included: a general description, information on ownership, affiliation to other sources or entities, revenue streams, stated purpose, stated target audience, (geographical) coverage and history of the source.

Content Analysis

Content Analysis aims to provide a comprehensive description of the content published on the source. OSINT personnel should attempt to analyse the overall content of the source, not a single published item.

The comprehensive description should include – but is not limited to – accuracy, authority, objectivity, relevancy, currency, topical coverage, target audience, tonality, purpose and type of content.

Determine Credibility

A thorough verification against other available open sources, conducted with the specific focus of the IR/EEI during the exploitation phase, is required to rate the credibility of collected information.[13]

Determine Reliability

As information is collected from a given open source over time, an aggregation of that source's reliability can be developed. In order to do so, credibility of information has to be rated and recorded every time an individual source is used in a collection activity.

Part III Assessment of the OSINT Result

For the description of the assessment inside an OSINT result, standardized probability statements and confidence levels are to be used.[14] The credibility rating of a specific result can differ from the overall credibility assigned to a source, e.g. a normally reliable and credible source publishes an article that is clearly false.

[13] AJP-2, Chapter 4.4.2, Figure 4.
[14] AIntP-18, Chapter 2.4.4, Figures 7 and 8.

INTENTIONALLY BLANK

ANNEX D OSINT REPORT (OSINTREP) FORMATTING

The OSINTREP is a NATO open source reporting structure to be created by the NATO asset/capability. This report, in turn, becomes an artifact and should be logged in an OSINT repository according to data storage regulations. STANAG 4559 should be adhered to in the compilation of the report.

The OSINTREP

Purpose

The purpose of the OSINTREP is to be able to transmit OSINT results in accordance with the NATO message catalogue APP-11.

Producers of OSINTREPs

The responsibility of generating OSINTREPs will be with the OSINT exploitation systems.

Consumers of OSINTREPs

The consumers are IRM & CM systems, OSINT/Multi-INT exploitation systems.

OSINTREP Content

Fields of an OSINT report are:

Category in OSINTREP	XML Field Name	Description	Required Y/N	Comments
Security	Security	Security parameter for: • Releasibility • Classification	Y	
PIR/RFC/RFI	NA	Will be added in IntelFS to link to the appropriate PIR/RFC/RFI	N	Automated in the reporting system
Precedence	NA	Priority classification of the report	N	Routine, Priority, Immediate or Flash

Title	NA	Short description of the collected result	Y	
Document ID	DocumentUUID	Unique identifier of the document	Y	UUID should be generated by applications.
Document Version	DocumentVersion	Version of the document	Y	Republished reports have new version numbers
Document Series	NA	Series number	N	For regularly published reports
Creation Date Time	CreationDateTime	Date and time the result was created	Y	
Information Cutoff Date	NA	Date information collection terminated	Y	
Event/Content Date	NA	Date of the event or activity being reported	N	Could be a date range
Validity Date	NA	Date the information is valid until	N	
Countries Associated with report	NA	NATO Codification System (NCS) code of the countries associated to the event	N	Can include multiple
Geographic Location	GeographicLocationOf CollectedInformation	Location of the information collection	N	UTM, MGRS, Lat/Long
ACO designator	NA	NATO AOR	N	
Subject	NA	Free text/free form	Y	
Originator	Creator	Creator of the document • (Unique) Platform Identification • Author	Y	Also consider specific requirements for exercise/operation

		• Military unit or organization		
Published Status	PublishedStatus	Status of the document	N	Draft, Approved, Current or Obsolete
Exercise or Operation Name	ExerciseName/ Operationname	Use either “ExerciseName” for exercise (nick-)name or “OperationName” for operation name.	N	
Disclaimer	NA	Graphic and/or offensive material	N	
Summary	NA	Free-text description of the exploitation results as summary.	Y	Would be the 1-2 sentences that would be translated into NATO working languages
Table of Contents	NA	To navigate through a multi-page document	N	
Content	NA	Result of collection	Y	Will include imagery or graphics if applicable
Comment	NA	Comment on the information or the source	N	Include machine translated if applicable
Assessment	NA		N	
Sources	NA	Author, Title, Publication, Date, URL	N	
Source Rating	SourceInfoRatingType	As per the source information grading matrix	Y	Leaving the field empty corresponds to a rating of “F”

OSINTREP Example

UNCLASSIFIED

ROUTINE

(U) TITLE: Something Important Happened to Somebody

(U) Document ID: OSINTREP 0021-2021
(U) Creation Date: DD Mmm YYYY (ie. 07 Mar 2020)
(U) Information Cutoff Date: DD Mmm YYYY (ie. 07 Mar 2020)
(U) Country: Name (trigraph ABC)
(U) Subject: free text keywords that assist in document retrieval
(U) Originator: NATO command structure or national OSINT capability

(U) Summary

- The main points that cover what your report states (U)
- Can be in bullets or sentences (U)
- Will be translated into NATO working language(s) (U)

(U) Content

(U) Main aspects of the collected information, why was it collected. ie. No transcript or translation is available for this video at this time. This video was posted on DD Month year (ie. 07 March 2020).

(U) Figure 1: Screenshot from source X picture of ABC

(U) Sources

(U) Author, Title, Publication, Date, Source Rating

ANNEX E DISCLAIMERS

Note: The inclusion of disclaimers is not standard NATO procedure and are in no way required with the OSINT result. The following textual examples are provided as options for inclusion, if deemed necessary by the respective OSINT asset/capability. The disclaimers need not be used in their entirety, but relevant aspects can be selected at the discretion of the OSINT asset/capability.

Graphic Content Disclaimer

CONTENT WARNING! This product contains GRAPHIC and potentially DISTRESSING MATERIAL, viewer discretion is advised.

View/Opinion Disclaimer

The views and/or opinions expressed in the information used to produce this OSINT result are, unless expressly stated otherwise, not that of the OSINT asset/capability. They do not in any way constitute endorsement or reflect an official position.

OSINT Handling Disclaimers

This Open-Source Intelligence (OSINT) Report was produced by and is the property of [*name of asset/capability*]. Should you have any questions or wish further information, please contact the OSINT team [*contact information*]. This document is provided under the authority of [*name of authority*] and must be protected in a manner consistent with its overall security classification and releasability markings. It is provided to your department in confidence, for official purposes only. It is not to be used in affidavits, court proceedings, subpoenas or for any other legal or judicial purpose without the consent of the originator. The intelligence contained herein must not be reclassified, renamed, or altered in whole or in part without the consent of the originator. Text may be quoted or paraphrased as long as the classification and any handling codes or dissemination control markings are respected and the context is faithfully reproduced. Graphics can be embedded into third party reporting only if the graphic is unaltered and the banner and classification are visible and legible.

Liability Disclaimer

Data furnished by third parties is supplied in the format and condition provided and is licensed for the purpose specified in the release conditions. The originator accepts no liability for any error or omission in the data, or for any loss, damage, claims, proceedings or costs arising from the recipient's use of, or reliance on, the data or from any modification or alteration of the data or its format, to the full extent permitted by law.

Imagery Disclaimer

All graphics produced by [*name of asset/capability*] are for planning/briefing purposes only and are not intended for precision positioning or navigation. Boundaries are not considered authoritative.

INTENTIONALLY BLANK

AIntP-22(A)(1)