NATO STANDARD

AIntP-10

TECHNICAL EXPLOITATION

Edition B, Version 1

MAY 2021

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

4 May 2021

1. The enclosed Allied Intelligence Publication AIntP-10, Edition B, Version 1, TECHNICAL EXPLOITATION, 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 6502.

2. AIntP-10, Edition B, Version 1, is effective upon receipt and supersedes AIntP-10, Edition A, Version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

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.

5. AIntP-10, Edition A Version 1, dated 2015, was focused on the technical exploitation (TE) of improvised explosive device (IED) weapon systems. The revision of AIntP-10, Edition A, Version 1, was prompted by the decision to cancel AJP-2.5, Edition A, Version 1, Allied Joint Doctrine for Captured Persons, Materiel and Documents in the future. The scope of AIntP-10, Edition B, Version 1, was expanded beyond its original counter-IED focus. This new edition of AIntP-10 redefines the TE process, includes relevant content from AJP-2.5 and provides a comprehensive framework that covers all TE capabilities used to process any collected exploitable material.

FOR

Zoltán GULYÁS
Brigadier General, HUNAF
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]
GRC	Hellenic Armed Forces will implement the subject STANAG taking into account all legal implications involved.
NLD	At the moment unknown NATO-standards prevent implementation of STANAG 6502. With the establishment of 108 TEXINTcie within Joint ISTAR Command (JISTARC), the NLD armed forces show their ambition to comply with NATO Technical Exploitation (TE) standards. However, NATO-standards for a TE-capacity are still unknown. The NATO Technical Exploitation Group (NTEG) will identify DOTPLMFI-factors in a 3-year Program of Work (POW) which will be completed in 2024. The goal of this program is the identification of clear NATO-standards for a TE-capacity.
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

References

AC/343-D(2020)0002	NATO Technical Exploitation Policy
AAP-03	Directive for the Production, Maintenance and Management of NATO Standardization Documents
AAP-06	NATO Glossary of Terms and Definitions
AAP-15	NATO Glossary of Abbreviations
AAP-47	Allied Joint Doctrine Development
AJP-01	Allied Joint Doctrine
AJP-2	Allied Joint Doctrine for Intelligence, Counterintelligence and Security
AJP-2.1	Allied Joint Doctrine for Intelligence Procedures
AJP-2.3	Allied Joint Doctrine for Human Intelligence (HUMINT)
AJP-2.4	Allied Joint Doctrine for Signals Intelligence (SIGINT)
AJP-2.7	Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance
AJP-2.8	Allied Joint Doctrine for Measurement and Signature Intelligence
AJP-2.9	Allied Joint Doctrine for Open Source Intelligence (OSINT)
AJP-3	Allied Joint Doctrine for the Conduct of Operations
AJP-3.1	Allied Joint Doctrine for Maritime Operations
AJP-3.15	Allied Joint Doctrine for Countering Improvised Explosive Devices (C-IED)
AJP-3.17	Allied Joint Doctrine for Geospatial Support
AJP-3.2	Allied Joint Doctrine for Land Operations
AJP-3.3	Allied Joint Doctrine for Air Operations
AJP-3.4.4	Allied Joint Doctrine for Counter-Insurgency
AJP-3.8	Allied Joint Doctrine for Comprehensive Chemical, Biological, Radiological and Nuclear Defence

AJP-3.9	Allied Joint Doctrine for Joint Targeting
AJP-5	Allied Joint Doctrine for Operational-level planning
AJP-6	Allied Joint Doctrine for Communication and Information Systems
AIntP-13	Human Network Analysis and Support to Targeting (HNAT)
AIntP-14	Joint Intelligence, Surveillance and Reconnaissance Support to NATO Operations
AIntP-15	Countering Threat Anonymity: Biometrics in Support of Operations and Intelligence
AIntP-16	Intelligence Requirements Management and Collection Management Procedures
AIntP-17	Joint Intelligence Preparation of the Operating Environment
ACIEDP-02	NATO Weapons Intelligence Team (WIT) Capabilities
AEODP-06	Explosive Ordnance Disposal Reports and Messages
AEP-66	NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA)
APP-11	NATO Message Catalogue
ATP-3.8.1 Volume 1	CBRN Defence on Operations
STANAG 4632	Deployable NBC Analytical Laboratory
STANAG 4715	Biometrics Data, Interchange, Watch Listing, and Reporting Standard

Preface

Context

1. Within the maritime, land, air and space, and cyberspace domains, there is an increase of emerging threats supported by adaptive adversary capabilities. Adversarial capabilities are continuously evolving and proliferating throughout operation areas and beyond. Adversaries continue to develop conventional and unconventional weapons at an accelerated rate, to include associated tactics, techniques, and procedures (TTP). These weapons range from improvised explosive devices to sophisticated weapon systems.

2. In countering these adaptive capabilities, the technical exploitation (TE) of collected material provides commanders an understanding of the threat and contributes to all-source intelligence and the conduct of operations. TE provides the knowledge needed to understand the adversary's capabilities and TTP and enhance force protection measures. TE also aids in identifying the source of the threat(s) within the operating environment by determining the identity of those responsible and the networks that are posing these threats.

3. This resultant situation highlights and reinforces the need to integrate and synchronise TE processes and capabilities across the NATO force. Commanders and staffs must be able to effectively communicate TE requirements, leverage existing NATO capabilities, and obtain timely results that will identify potential threats, prevent tactical surprise, and stay abreast of evolving technologies used by adversaries.

Scope

4. This document provides a TE framework enabling NATO commands and staff elements at all levels to plan and execute TE activities, that can vary based on the type, duration and environment of the commander's mission. The aim of the second edition of AIntP-10 is to expand beyond its original counter-improvised explosive device focus and provide a comprehensive framework to enable the TE of any collected material of interest.

Purpose

5. The purpose of AIntP-10 is to improve interoperability by providing guidance for commanders and staff on the employment of TE capabilities in support of NATO operations. Based on the combined joint task force concept, it establishes recommended standards and requirements to enable TE and facilitates effective communication of NATO TE processes and results through appropriate dissemination methods. AIntP-10 also serves as a foundational publication that can be used for the development of more detailed standard operating procedures.

Application

6. AIntP-10 applies to all NATO nations and stakeholders of NATO-led operations. It provides NATO forces, NATO headquarters, and subordinate organisations with a common framework for TE planning within the NATO operational architecture. TE activities and results provide vital information to commanders across the full spectrum of operations from expeditionary operations to homeland defence. In addition to military operations and homeland defence, TE results can also provide information and evidence for law enforcement activities and judicial proceedings. Although it is focused primarily at the operational level, this document could be applied at all levels of command and by other NATO organisations, member states and partners supporting their objectives, missions and activities.

Structure

7. This publication consists of four chapters and five annexes. Chapter 1 provides the fundamentals of the TE process and its relation to the intelligence cycle. Chapter 2 describes the TE process, capabilities and supporting activities. Chapter 3 outlines key command and staff element responsibilities. Key planning considerations for the conduct of TE are examined in Chapter 4. Annex A is an example of a TE memorandum of agreement. Annex B is an example of a TE management plan. TE capabilities and their potential intelligence value are described in Annex C. Annex D consists of a table comparing and contrasting the three levels of TE. Annex E includes three scenarios illustrating the TE process and the application of various TE capabilities.

Related documents

8. AIntP-10 is level-3 doctrine within NATO's AJP 2-series intelligence doctrine and is subordinate to AJP 2.7, *Joint Intelligence, Surveillance and Reconnaissance (JISR)* (Figure 01). AJP 2.7 is a level-2 joint functional doctrine publication that describes how collection requirements are satisfied by a JISR capability following five sequential steps: task, collect, process, exploit and disseminate. TE, as presented in AIntP-10, follows a similar five step process.

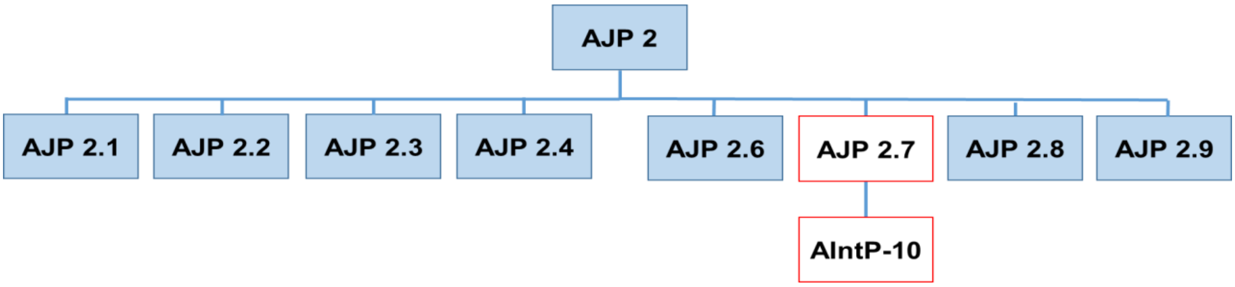


Figure 01: Allied Intelligence Publication for Technical Exploitation within the Hierarchy of Intelligence Doctrine and Publications.

TABLE OF CONTENTS

FIGURES

CHAPTER 1 TECHNICAL EXPLOITATION FUNDAMENTALS

1.1. INTRODUCTION

1. Technical exploitation (TE) is a process using scientific methods and tools to derive data and information of potential intelligence or operational value from collected data, information, materiel and materials. The aim of TE is to bring together a diverse set of capabilities and expertise to derive data and/or information from all types of collected material. For purposes of this publication, the term ‘collected exploitable material’ (CEM) is used and refers to any type of data, information, materiel and materials, which are collected, captured, or received by NATO forces which may have intelligence or operational value.[1]

2. Within a joint operations area (JOA), commanders will have access to large volumes of information relating to all aspects of the environment. This information influences decision making and provides the foundation for operations planning through the commander’s priority intelligence requirements (PIRs). As part of the commander’s intelligence collection plan (ICP) to satisfy PIRs, TE is a unique and valuable source of information providing commanders with greater insights regarding the adversary and the threat environment.

3. TE activities are integrated with operations employing capabilities that enable the combating of threats posed by an adversary across the spectrum of conflict. TE directly contributes to the full range of intelligence collection disciplines[2] and NATO focus areas, such as counter-unmanned aircraft systems, counter-intelligence, counterterrorism and counter-weapons of mass destruction, by exposing linkages between actors, objects and events.

4. TE capabilities can be assembled and formed into capability support packages that are tailored to meet joint force requirements. They can be task-organized depending on operational factors such as the commander’s critical information requirements, the operating environment (OE), as well as national laws and international agreements.

5. The fundamentals of TE include the relationship between TE and the intelligence cycle, the TE process, guiding principles, TE results and supported outcomes.

[1] Collected exploitable material (CEM) can include, but is not limited to: electronic media (computers, cell phones, flash drives) and the data and information they contain; documents; conventional and improvised weapons and their components; drugs; chemicals and precursors; explosives; chemical, biological radiological and nuclear substances; biometric information; tool marks and impressions; firearms; materiel (vehicles, marine vessels, aircraft, communications equipment, cryptologic gear, sensors); installations; fabric; fibres; and cordage.

[2] See AJP-2.0, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security,* for detailed information on intelligence collection disciplines.

a. **TE and the intelligence cycle.** TE integrates and synchronises a diverse set of capabilities to support the intelligence cycle by obtaining results from the TE of collected data, information, materiel and materials.TE is a component of the joint intelligence, surveillance and reconnaissance (JISR) process of the intelligence cycle. As a JISR component, TE contributes to the intelligence cycle as well as meeting time sensitive information requirements. TE results can be of direct interest for the all-source intelligence fusion cell and be directed to a command's intelligence staff element,

b. **TE process.** The TE process parallels the JISR process with a focus on the processing and exploitation steps.[3] TE results fused with JISR results contribute to the development of intelligence products that define the OE and supports the commander's decision making process at all levels. To ensure a unity of effort among multiple exploitation stakeholders, the TE process requires close coordination and a synchronized approach, especially in support of time-sensitive operations. Stakeholders may include government, industry, academia, joint forces, police/law enforcement agencies, international partners, non-government organizations and local civilian authorities.

c. **TE principles.** General principles to guide and govern how JISR results and intelligence is produced are described in AJP-2.7. These same principles apply to the conduct of TE activities but differ depending on the context.

d. **TE results and supported outcomes.** TE results could have an immediate tactical and operational impact as well as a strategic impact. TE results can contribute directly to all-source analysis including network analysis but can also be used to support other activities and outcomes. TE results support targeting; force protection; component and material attribution; countermeasures development; as well as research, development, testing and evaluation. Additionally, TE results could support law enforcement activities and legal proceedings; however, the priority for TE is to ensure military objectives are met.

[3] The JISR process consists of five steps: task, collect, process, exploit and disseminate and referred to as TCPED.

1.2. TECHNICAL EXPLOITATION AND THE INTELLIGENCE CYCLE

1. **Understanding the operational environment.** Commanders at all levels depend on timely, accurate information and intelligence on all aspects of the OE including an adversary's dispositions, strategy, tactics, intent, objectives, strengths, weaknesses, values, capabilities, and critical vulnerabilities. The intelligence staff element assists commanders in developing their understanding of the OE and situational awareness enabling commanders to make intelligence-based decisions.

2. **Joint intelligence preparation of the operating environment**. JIPOE is the continuous process through which the intelligence staff element produces analytical products enabling the commander and staffs to better understand the threat and the environment within a specific geographic area. JIPOE products include intelligence assessments and estimates that answer the commander's information requirements, focus intelligence collection at the right place and time and support planning and decision making processes at all levels.

3. In the course of defining and describing all relevant aspects of the OE, existing information may be insufficient. Information gaps are converted into new requirements and entered into the intelligence cycle. In response to validated collection requirements, intelligence collection capabilities are tasked to gather relevant data and information. In addition to JISR capabilities that are tasked to collect relevant data and information, TE assets are also tasked to collect data, information, materiel and materials. TE contributes to the JIPOE process by allowing intelligence communities to better "see the adversary" and understand the threat. For example, TE results from explosive ordnance disposal exploitation enable tactical characterization and technical categorization of adversary threats, such as improvised weapons, advanced munitions and first-seen ordnance. This TE-derived information enables intelligence analysts to better characterize the OE and produce intelligence assessments that include an evaluation of the threat's strengths, weaknesses, and vulnerabilities.

4. To address information gaps identified during the JIPOE process, all source analysts integrate and fuse TE results with JISR-derived results and other sources information and intelligence to produce detailed analytical products. (Figure 02). JIPOE analysts can then use these intelligence products to produce their assessments and estimates.

5. **Technical exploitation as a capability**. TE is a methodological, integrated and collaborative set of capabilities used to derive data and information from collected material. Within theatre, tactical level field exploitation teams (FETs) collect data, information, materiel and material of potential intelligence value. FETs gather material that is associated with or obtained directly from threat actors. Obtaining the material directly from an actor, a site or event may address a gap in collection that JISR collection capabilities cannot easily address. FET personnel, in general, must be in physical contact with the material or persons of interest. Due to the dynamic nature of all operations and the opportunities for collection that may arise, TE activities are dependent on an individual's ability to recognize and recover material that is deemed of potential value to satisfy intelligence requirements. Once the material of interest is detected, discovered and recognized, TE capabilities can be brought to bear wherever

and whenever there are collection opportunities which could include a battlefield (level 1), secured area (level 2), or outside the area of operations (level 3). Subject matter specialists, scientists and technicians apply scientific analysis using state-of-the-art capabilities to extract specific pieces of information from what is collected in the field. The results and the information derived from the collected material are then made available to intelligence analysts.

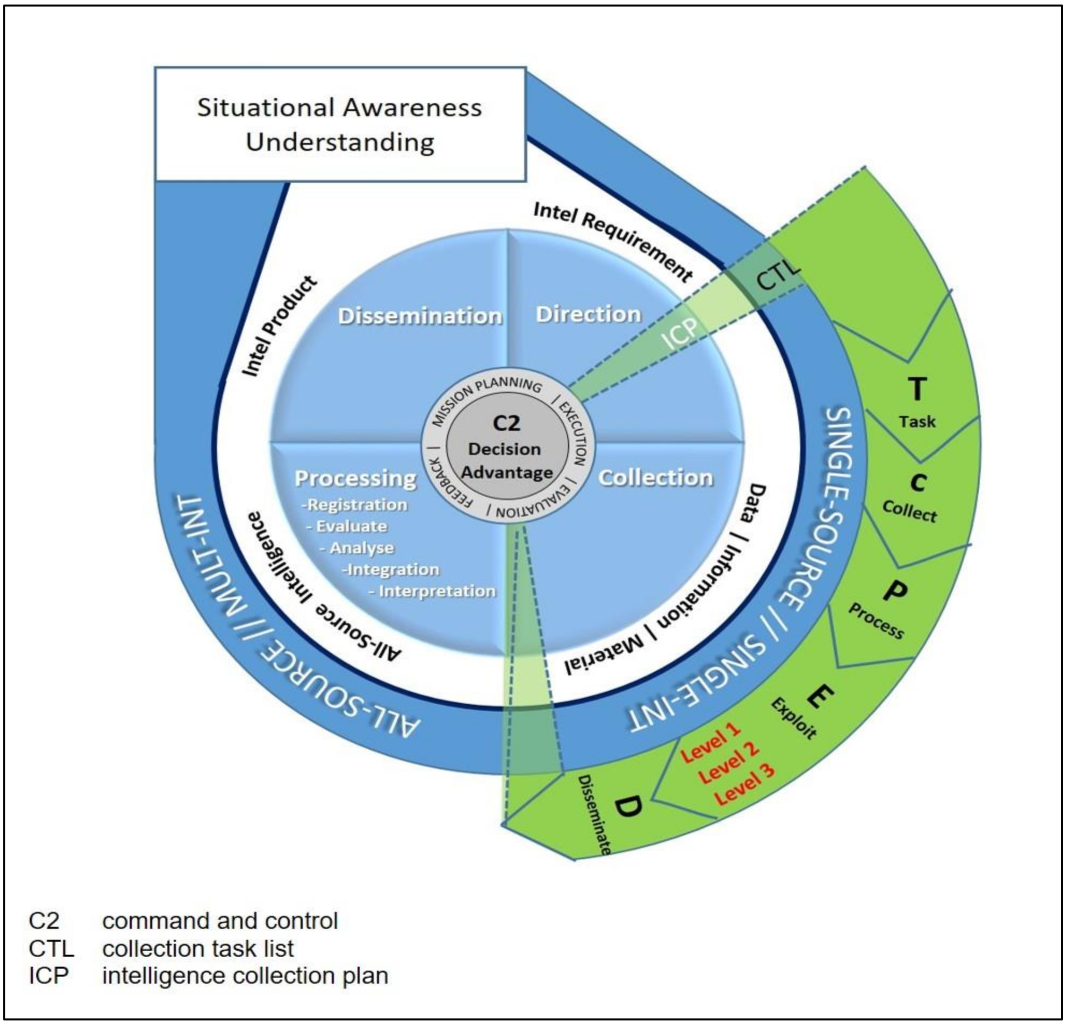


Figure 02: Technical Exploitation and the Intelligence Cycle.

6. TE contributes to the intelligence cycle by:

a. informing the requirements and/or collection management activities within the direction phase of the intelligence cycle, and

b. providing results that can be used in conjunction with JISR results and fused into intelligence during the processing phase of the intelligence cycle.

7. TE collection activities are typically performed by conventional forces at the tactical and operational levels and can be complemented with special operations

forces (SOF). However, for any given mission, various types of specialised units within theatre also support TE collection activities. As the mission evolves, NATO forces could be used in other capacities to include support to stability operations. If NATO forces are used to support a stability policing (SP) mission, they can continue to support TE activities.

a. **Conventional forces**. Commanders conducting operations that include tactical level exploitation ensure subordinate unit missions are integrated by task and purpose and understand the exploitation scheme of manoeuvre. The availability of resources, such as time, forces, and specialized assets, allows commanders to synchronize subordinate exploitation actions in time, space, and purpose.

b. **SOF**. SOF provide a flexible and rapidly deployable capability that can reinforce, augment, and complement conventional forces across the range of military operations. They can also conduct independent operations especially when there is a time-sensitive need to obtain or verify information regarding adversary capabilities, vulnerabilities, intentions and activities.

c. **SP**. As the mission evolves over time within theatre, SP assets can continue TE activities. SP assets are specialised resources available to the commander that perform police activities in the mission area. SP tasks include, but are not limited to, support to: war crime investigations and assistance to international courts; forensic and biometric activities; counter-terrorism; and weapons intelligence teams.

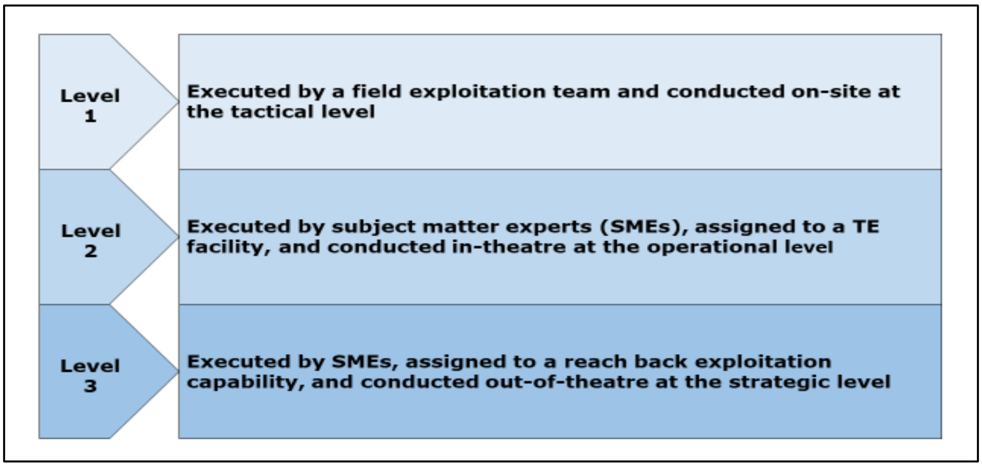
1.3. TECHNICAL EXPLOITATION ACTIVITIES

1. **Technical exploitation activities**. TE activities begin with the tasking outlined in the ICP that is prepared by personnel performing the intelligence requirements management and collection management function. Based on this tasking, deployed units start the TE process by collecting data, information, materiel and materials of interest. Due to the wide variation of items and objects that are of potential intelligence interest, an equally wide range of forensic, scientific and technical capabilities are required to support TE activities to produce optimal results. Subsequently, TE results are assessed and fused with other TE data that are then used to produce intelligence products to satisfy intelligence requirements.

2. **Technical exploitation process**. The TE process parallels the JISR process. In response to a TE task, material is collected, processed, exploited and disseminated at all levels of command. Dissemination of TE results and reporting is the final step in the process. However, as the CEM is processed at each level, TE results are disseminated and made available to meet time-sensitive strategic, operational and tactical requirements.

3. **Technical exploitation levels.** TE level 1 activities can occur: on-site at the point of collection; at a forward operating base, military installation, or laboratory; or at reach back facilities. Level 1 tactical TE and level 2 operational TE are typically conducted in-theatre as a synchronized set of activities. Once processed and exploited in-theatre, the material can then be transported to out-of-theatre facilities and laboratories to allow subject matter experts (SMEs) to conduct a further examination of the material.

4. Given that TE can be conducted at multiple locations and within different OEs, a geographically-based reference system is needed to facilitate TE activities. This reference system provides commanders with a basic awareness of where TE facilities are typically located and where TE activities are conducted. The three-level TE construct is appropriate and consistent with the three levels of command (Figure 03).[4] The boundaries between these levels are neither rigid nor impermeable but the levels can serve as a practical means to optimize TE activities.



Level 1 — Executed by a field exploitation team and conducted on-site at the tactical level

Level 2 — Executed by subject matter experts (SMEs), assigned to a TE facility, and conducted in-theatre at the operational level

Level 3 — Executed by SMEs, assigned to a reach back exploitation capability, and conducted out-of-theatre at the strategic level

Figure 03: Three-level Construct for Technical Exploitation.

5. At each of the levels, TE capabilities can be leveraged to derive data and information from CEM that can be processed and contribute to intelligence products. The degree of the TE effort conducted at each level will depend on the commander's priorities. In an operation, NATO nations can contribute to one or more of these levels depending on national capabilities and capacity to conduct TE.

[4] *Allied Joint Doctrine for Countering Improvised Explosive Devices (C-IED),* AJP 3.15, defines level 1 as field/tactical, level 2 as theatre/operational and level 3 as out-of- theatre/strategic exploitation. Similar construct can be found in *Allied Joint Doctrine for Comprehensive Chemical, Biological, Radiological and Nuclear Defence,* AJP-3.8, and *NATO Handbook for Sampling and Identification of Biological, Chemical and Radiological Agents (SIBCRA),* AEP-66,

6. TE activities are conducted at the tactical, operational, and strategic levels. Within theatre, an effective command and control structure should be established to ensure TE activities are integrated and synchronized in accordance with combined joint task force (CJTF) guidance/tasking. The intelligence staff is the CJTF staff element responsible for the management and coordination of TE activities at all levels. To effectively manage and coordinate TE activities, a combined joint captured materiel exploitation centre or an equivalent theatre exploitation centre should be established reporting directly to the CJTF headquarters (CJTF HQ). Tactical units and field exploitation teams begin the TE process by collecting material of interest. Level 1 TE tactical units can leverage multiple TE capabilities, depending on needs, location, security, training and availability of SMEs. For more in-depth TE, level 1 units (both land-based and sea-based) can forward the collected material to the nearest level 2 TE location or directly to a level 3 TE facility outside the JOA for further assessment (Figure 04).

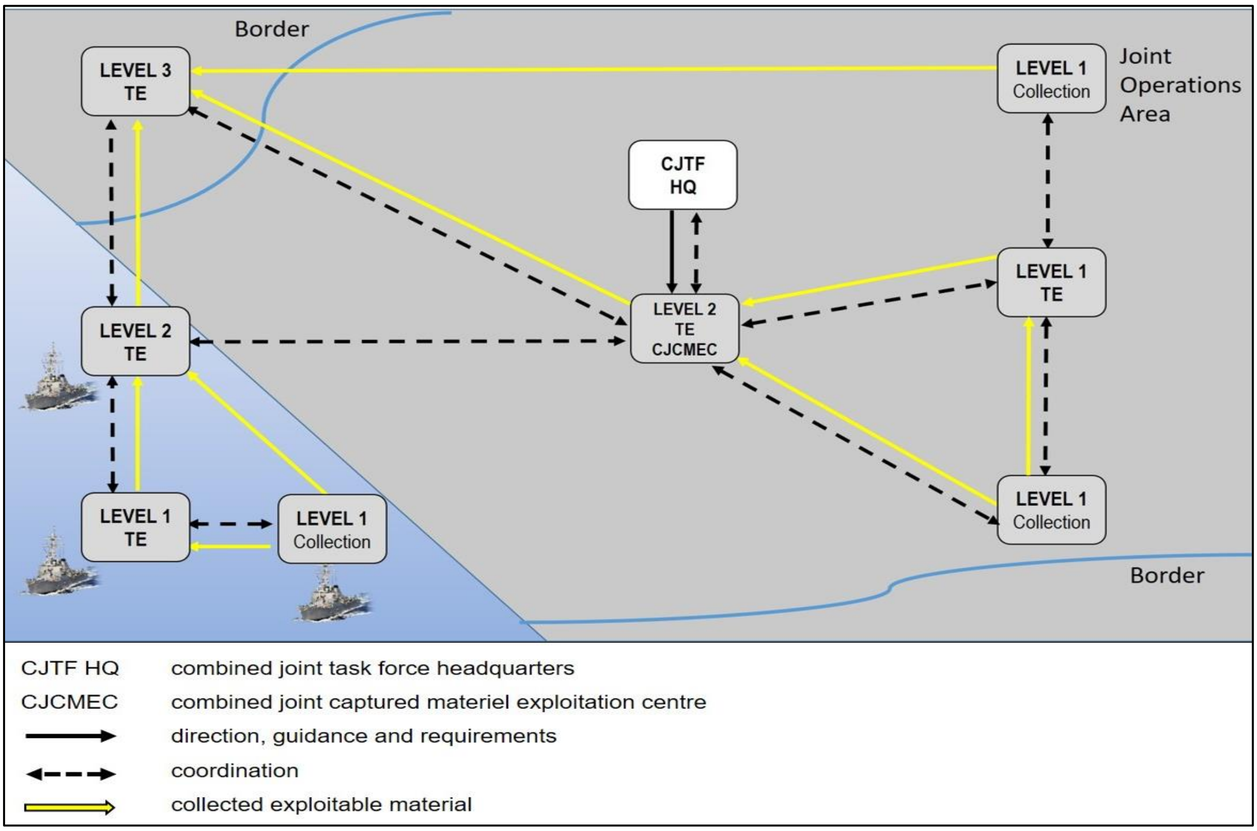

Border
LEVEL 3 TE
LEVEL 1 Collection
Joint Operations Area
CJTF HQ
LEVEL 1 TE
LEVEL 2 TE
LEVEL 2 TE CJCMEC
LEVEL 1 TE
LEVEL 1 Collection
LEVEL 1 Collection
Border
CJTF HQ combined joint task force headquarters
CJCMEC combined joint captured materiel exploitation centre
→ direction, guidance and requirements
←- - → coordination
⇒ collected exploitable material

Figure 04: Notional Operational View of Technical Exploitation.

7. The operational view:

a. visualizes TE as a geographically-based referenced system;

b. serves as a basic concept for the employment of TE capabilities;

c. recognizes that TE activities can be conducted in either a linear or non-linear sequence;

d. demonstrates that tactical commanders, who require reach back support, could transfer the CEM to level 2 or level 3 locations outside the JOA;

e. defines relationships between the TE elements and coordination between the level 1 tactical collection teams and the level 2 and 3 TE facilities.

f. recognizes sea-based TE capabilities in addition to land-based capabilities; and

g. identifies line of tasking between the CJTF HQ and intelligence staff elements.

8. Based on mission objectives, the commander will determine the required TE capabilities needed within the OE. In the event there are deployed formations supporting multiple mission objectives in different OEs, commanders and staff elements should develop a detailed TE management plan identifying their specific TE requirements and capabilities.[5]

9. **The advantages of a three-level technical exploitation construct.** Establishing a geographically-based 3-level construct ensures that any CEM is systematically processed and thoroughly exploited. (Figure 05). TE conducted at a level 1 site could produce immediate results to support time-sensitive requirements. However, as the CEM is transferred/transported from a non-permissive to a more permissive environment, TE SMEs and specialists can conduct further collection, processing and exploitation with specialized equipment. At each level over time, a higher degree of assurance, rigour, accuracy, and confidence may be achieved.

[5] See annex B for an example of a TE management plan.

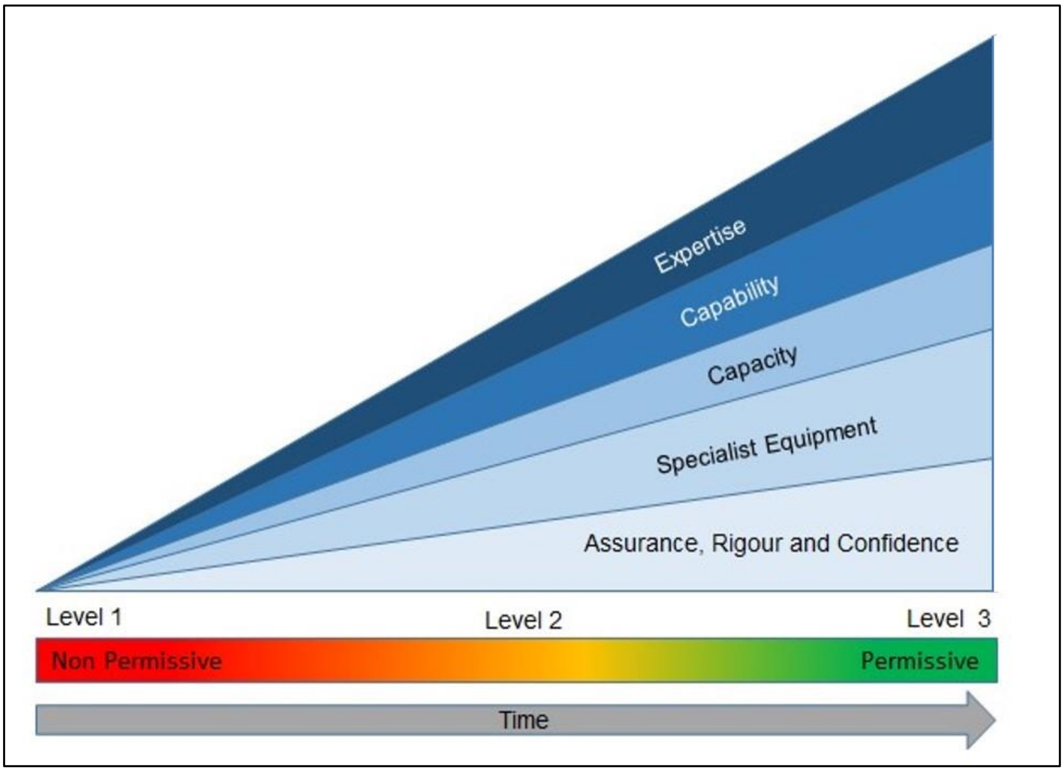


Figure 05: The Advantages of a Three-level Technical Exploitation Construct.

1.4. PRINCIPLES OF TECHNICAL EXPLOITATION

1. TE activities are governed by the following principles:

a. **Centralised command and control and decentralised execution.** Clear, consolidated command and control enables effective TE. TE activities involve close coordination with echelons of command and multiple organisations and personnel.[6] The commander has overall authority and responsibility for TE. However, the TE function is exercised through the intelligence staff element and executed in conjunction with the operations staff.

b. **Adaptability.** TE can begin with the rapid deployment of a small cadre of specialists with minimal equipment. Once the exact and enduring requirement is determined, the TE presence can then be expanded as necessary. TE supports the conduct of operations by providing capabilities that are both scalable and modular. Scalable TE capabilities should account for the volume and complexity of the CEM and the criticality of the potential information to be gleaned. In addition, TE capabilities should be modular to give commanders the ability to

[6] Personnel could include: task force commanders; on-site commanders; explosive ordnance disposal (EOD) technicians; forensic scientists; engineers; intelligence analysts; as well as host nation personnel.

employ and interchange elements based on the OE, need, availability and time.

c. **Continuous assessment.** TE activities should be continually monitored and assessed to ensure the TE process is responsive and satisfying information and intelligence requirements. TE should be performed in an expeditious, yet thorough manner. There should be sufficient TE capabilities available to the commander to provide information in a timely manner and where it is needed. The TE process and supporting capabilities should be based on efficient methods that allow for the rapid dissemination of critical information and the transport of material.

d**.** **Documentation and preservation of CEM.** During the collection and processing of material, proper documentation techniques and chain-of-custody procedures should be maintained from the time of discovery and throughout the TE process. This documentation should include a unique identifier using a standardised methodology that allows all items and objects from an event to be catalogued.

Personnel must be trained in rudimentary collection and preservation skills to ensure they do not degrade the CEM of potential intelligence value. Trained personnel should use standardised procedures when collecting and handling the material so as to preserve the maximum exploitation value. Specialists should use methods and techniques that are the least invasive and destructive to ensure an accurate and thorough analysis.

e. **Prioritization.** Each item and object that is collected needs to be prioritized.The commander's TE resources need to be applied to those items and objects with a high potential of intelligence and operational value. However, the sequence of applying TE capabilities (e.g., biometric characteristic analysis, mechanical exploitation, document and media exploitation) should also be prioritised to ensure that the material, or the potential data and information it may reveal, is not inadvertently altered, thus preventing any additional TE.

f. **Risk awareness.** Commanders and leaders at all levels should be cognizant of the risks associated with TE and weigh these risks against the value of the information to be gained. There may be instances in which collection, handling and processing of CEM may be of paramount importance and worth risking life and safety. Material (e.g., ammunition, chemical agents, radioactive material and and biohazards) and persons of interest encountered in the area of operations can pose a threat. For these types of threats, TE assets may require specialised tactics, techniques and procedures and specialists, such as security personnel, specialised chemical, biological, radiological and nuclear defence forces or medical personnel, to support their activities. While performing TE activities, collectors, exploiters and laboratory personnel must use appropriate individual protective equipment and exercise safe practices to minimize exposure to potential hazards.[7] Material that pose a threat to life or are unsafe to recover may need to be destroyed at the location where they are first discovered.

g **Systematic approach.** Collection occurs at all levels of TE. Using advanced collection techniques and processing capabilities at a level 2 or 3 TE facility, secondary collection and TE can result in the discovery of new material previously undetected. The TE framework employing a 3-tier construct helps to ensure all collected material of interest is thoroughly exploited and assessed.

[7] Specialists, such as EOD or CBRN defence personnel, may be required for a specific type of hazard.

INTENTIONALLY BLANK

CHAPTER 2 TECHNICAL EXPLOITATION FRAMEWORK

2.1. INTRODUCTION

An operational framework for technical exploitation (TE) provides the structure needed to understand, coordinate and execute TE activities in order to fulfil the commander's intent and satisfy information requirements. The TE framework, consisting of the TE process, capabilities and supporting activities, is designed to derive data and information from all collected exploitable material (CEM) in a systematic and efficient manner (Figure 06). TE results enable commanders and staff to gain an understanding of the operating environment (OE) and can also support tactical, operational and strategic requirements and outcomes.

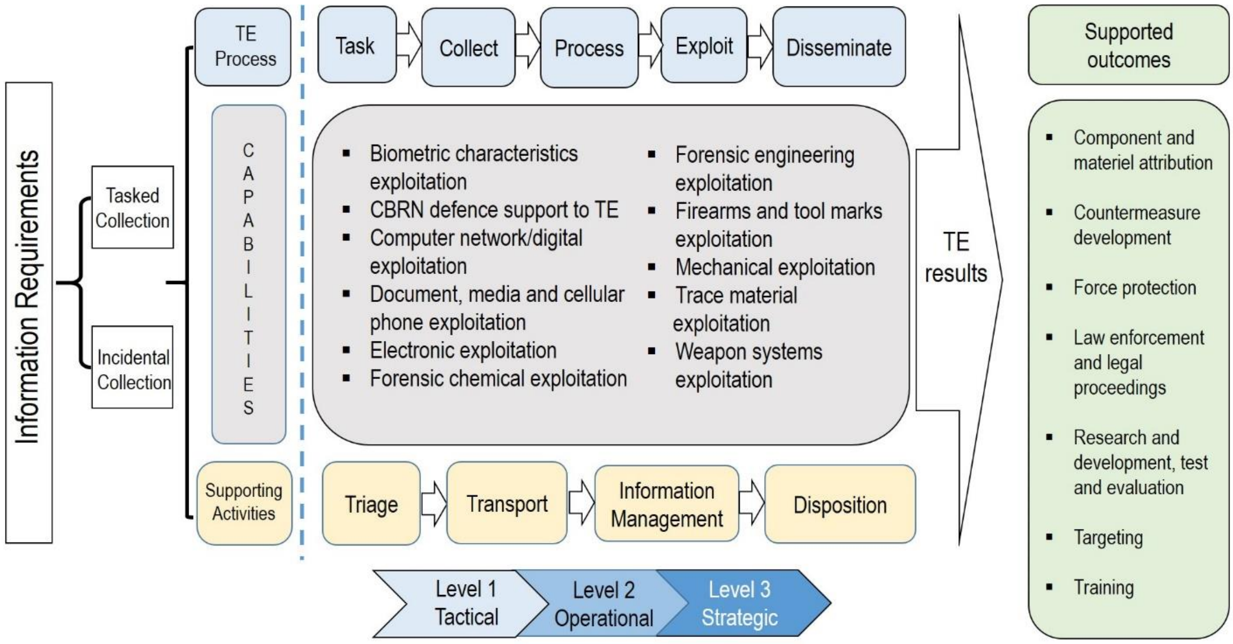

Information Requirements
Tasked Collection
Incidental Collection
TE Process
Task
Collect
Process
Exploit
Disseminate
CAPABILITIES
Biometric characteristics exploitation
CBRN defence support to TE
Computer network/digital exploitation
Document, media and cellular phone exploitation
Electronic exploitation
Forensic chemical exploitation
Forensic engineering exploitation
Firearms and tool marks exploitation
Mechanical exploitation
Trace material exploitation
Weapon systems exploitation
Supporting Activities
Triage
Transport
Information Management
Disposition
TE results
Supported outcomes
Component and materiel attribution
Countermeasure development
Force protection
Law enforcement and legal proceedings
Research and development, test and evaluation
Targeting
Training
Level 1 Tactical
Level 2 Operational
Level 3 Strategic

Figure 06: Technical Exploitation Framework.

2.2. TECHNICAL EXPLOITATION PROCESS

1. The TE process consists of five core steps: task, collect, process, exploit, and disseminate.

a. **Task**. Once TE capabilities are made available to the commander, the first step of the process is tasking. External tasking, conducted by the intelligence requirements management and collection management function inside the intelligence cycle, is based on the commander's validated intelligence and operational priorities. Within the TE process, the task step is initiated with the clear articulation of a collection requirement and consists of developing collection, exploitation and dissemination guidance/directives/orders to coordinate and effectively manage TE activities. TE tasking should be coordinated among all levels of command to enable mutual support between services/component commands and to make the most efficient use of available collection and exploitation capabilities.

b. **Collect.** Collection starts with the detection and recognition of material with potential intelligence and/or operational value and refers to the actual gathering of the material. TE assets collect the material and make it available for examination and assessment. Collection includes documenting the findings at the site and the physical collection, storage, security and transfer of information for further exploitation.

The security situation on-scene is of paramount importance and a critical factor which affects the freedom of movement and time on-scene of the collection asset. In a high threat/low secured environment, commanders need to prioritize collection activities. Given the likelihood of limited time on site, the goal for teams in the field is to secure as much essential material as possible.

When the security situation allows, chain-of-custody procedures need to be initiated and maintained to ensure the acquired material is handled in accordance with relevant policy, procedures, and applicable laws. In addition to establishing chain-of-custody procedures, all CEM must be protected and preserved by available and reasonable measures (marking, packaging, and tracking) to prevent contamination, loss, or inadvertent alteration.

c. **Process.** Processing is the preparation, development and conversion of the CEM into a form that enables exploitation. Processing leverages the results of the collect step and serves as a transitional activity prior to exploitation.
The first phase in the processing step is to sort through and organize the collected material by type. In some cases, data and information of potential value will need to be physically extracted from a device and converted into a readable format. For printed materials that require translation, a linguist will need to provide a gist of the document and determine its relative importance. During this step, all CEM should be prioritised, categorized and handled properly in an efficient manner. Advances in technology continue to change the manner in which data and information can be processed. TE assets with a near real-time data processing capability can rapidly convert collected data into exploitable information.

d**.** **Exploit.** The initial level of exploitation (level 1 TE) is the rapid and preliminary assessment of the collected material and forwarding the results immediately to the requester in support of current operations. For further exploitation and assessment, the CEM is transferred from a level 1 TE location to a level 2 or 3 TE facility. The time required to conduct exploitation will vary depending on the characteristics and limitations of the collection assets and the degree of exploitation required.

e. **Disseminate.** Dissemination is the timely delivery of TE results to the requester, commanders and staff, tactical field exploitation units, the all-source intelligence cell, and all stakeholders. The intelligence staff should be informed directly of any TE results that are time-sensitive and could impact future operations.

Effective dissemination management is needed to ensure requesters have access to the disseminated TE results that are posted, published, or transmitted. When TE results and material are transferred between the TE levels for further exploitation, it is critical that the results are made available to the originating organisation as well as the intended recipient/requester. In addition to providing an answer to a specific request for information, TE results should be systematically shared to support intelligence development and to improve the situational awareness of commanders and staffs. Dissemination is to be executed in accordance with classification and releasability guidance and procedures.

2.3. TECHNICAL EXPLOITATION LEVELS

1. TE can be conducted at the tactical, operational and strategic levels of command. TE capabilities and resources may vary from one level to the next, but there are specific actions that need to be accomplished at the initial point of collection and at each subsequent level to ensure requirements are satisfied.

2.3.1. Level 1 technical exploitation (field/tactical)

2. The processing and exploitation of the CEM can be initiated where possible and as the operational environment and tempo allow. The vast majority of the CEM that is discovered, recovered or seized are part of field exploitation activities.[8] Field exploitation is the initial stage of level 1 TE and includes activities performed at or near a specific location or event.

3. **Field exploitation.** Field exploitation is focused on any material of possible value for TE. Field exploitation not only involves detecting, recognizing and assessing the actual item of interest, it also involves understanding the way in which the item is used and employed. The degree of field exploitation conducted will be based on the operational situation and tactical imperatives. Field exploitation can consist of rapid photography and skim reading of exposed documents. In other cases, it may involve

[8] Field exploitation is a series of methodical actions taken to ensure that any findings at a site are detected, collected, and processed to preserve both intelligence and legal evidentiary value.

a systematic search to collect samples, extract computer hard drives, and remove building partitions. Field exploitation activities include:

a. **Recognizing potential sites.** Based on intelligence requirements, early recognition of collection rich sites within the joint operating area will support TE and the production of timely and relevant TE results.

b. **Establishing a field exploitation team.** The number of personnel assigned to a field exploitation team (FET), the degree of expertise, the equipment and the time on site can vary depending on the degree of examination and exploitation required. Depending on the objective and suspected contents at the site, TE specialists (e.g., media, communications, linguists, human intelligence collectors, weapons intelligence analysts and explosive experts) can augment the team providing immediate specialized support.

c. **Documenting the site.** Team members need to document all CEM. Documentation should include the location, time, and the details of the mission/objective. The context in which the material is first encountered should be thoroughly documented as well. Contextual documentation can be achieved by taking photographs and making sketches of the overall scene and of all items and objects prior to being moved. Statements should be taken from all persons/witnesses who can provide as much contextual data and information as possible relative to the item(s) in question. All relevant data and information regarding the items or information obtained from persons of interest should be recorded. When the situation allows, the team should initiate chain-of-custody procedures.

4. FETs can be part of a patrol, raid, or search mission and can take advantage of these events to collect material of intelligence interest. Field exploitation activities may, in turn, lead to immediate actionable information that can be used to plan and execute future operations. If the information derived from the collection is time-sensitive, it can directly support dynamic targeting. During targeting operations (deliberate and dynamic), valuable information can be collected by FETs. When this information is fused with other sources, the resulting intelligence could lead to the discovery of new sites for exploitation, such as locations containing high-value individuals, threat communication equipment and networks, weapon caches, or explosive production facilities. In addition to enabling follow-on operations, further exploitation may be needed that cannot be accomplished at a level 1 TE location due to operational tempo, limited capacity and throughput. In this case, the FET may need to forward the collected material directly to a level 2 or a level 3 TE facility for further exploitation and assessment.

5. **Level 1 technical exploitation activities.** Upon initial receipt of the CEM from the FET and a thorough debriefing of the team, level 1 personnel need to triage all collected items and objects to ensure the material can be handled safely and determine the significance and priority of handling. Personnel supporting level 1

TE consists of specialists trained in advanced collection and preservation techniques. Non-specialist personnel supporting level 1 TE are trained in basic collection and preservation techniques. Level 1 TE is employed to collect, process and exploit items, usually obtained at or near the point of collection, which may be in a non-permissive OE, using some or all of the available TE capabilities. Basic exploitation and presumptive testing may take place depending on time constraints and resource availability. Level 1 TE personnel typically apply non-invasive TE methods, document their findings and ensure all material is recovered and preserved for further processing and exploitation at a level 2 or level 3 TE. The intelligence staff should categorize and record information of intelligence value and provide intelligence reports to both the higher echelon and the capturing unit.

6. **Level 1 technical exploitation results.** Level 1 TE results are disseminated in minutes-to-hours from the point of collection. Level 1 TE activities may generate time-sensitive results, contribute to rapid follow-on operations and meet intelligence requirements. Level 1 TE results include, but are not limited to:

a. **Feedback.** Feedback on the level 1 TE results includes information regarding tactical threat tactics, techniques and procedures (TTP) and countermeasures.

b. **Reporting.** Level 1 personnel will complete a field exploitation report to catalogue collected material, provide a basic characterization and assessment and render an immediate assessment of threat capabilities and TTP. Level 1 TE results are focused on satisfying the tactical commander's requirements. The amount of information and level of detail obtained by level 1 TE will depend on the tactical situation and how much time can be spent on-site. The results from a level 1 TE tactical assessment[9] could include the following information:

- indications/warnings of adversary weapon systems;
- adversary intent;
- battle damage assessments;
- indication of new adversary TTP;
- tactical characterisation of how an adversary's activity was planned and executed;
- initial technical categorization of adversary weapon systems and associated components;

[9] Level 1 TE tactical assessments can enable TECHINT and other activities and inform their own reporting requirements.

- evaluation of signatures to intelligence, surveillance and reconnaissance priorities;
- trend analysis to identify possible future activity;
- biometrically enabled intelligence (BEI)[10] to support human network analysis;
- recommendations to friendly force TTP adaptation;
- support for dynamic/time-sensitive targeting; and
- information satisfying intelligence gaps.

c. **Disposition of collected material.** At this initial stage in the TE process, level 1 personnel should implement chain-of-custody procedures. All CEM should be properly documented, packaged, transported and secured to ensure viability for further exploitation at more advanced levels and for possible use as evidence in legal proceedings.

If the intelligence staff, in coordination with level 1 personnel, determines that the CEM needs to be transported from a level 1 TE location to a level 2 TE location, the intelligence staff will coordinate with the logistics staff to make the necessary transportation arrangements. For material that is deemed to be of high-level operational value, arrangements should be made to transport the material directly from the point of collection to the level 2 TE location. Level 1 TE ends when the level 1 TE results, along with collected material deemed appropriate for further exploitation, are transferred to a level 2 or 3 TE location.

2.3.2. Level 2 technical exploitation (theatre/operational)

1. **Level 2 technical exploitation activities**. Level 2 TE is typically conducted at the theatre/operational level using advanced capabilities, sophisticated equipment, and performed by personnel with greater technical, forensic and specialized skills than those at level 1. To meet combined joint task force (CJTF) requirements and support in-theatre

operations, the CJTF commander may establish a level 2 TE center to appropriately integrate, synchronize, and coordinate in-theatre TE activities.[11] The level 2 TE center should be equipped and staffed by appropriately trained and qualified, scientific and technical personnel to conduct a more thorough, deliberate, and detailed exploitation of the collected material. Level 2 TE activities may provide a greater level of assurance,

[10] BEI is intelligence information associated with and/or derived from biometrics data that matches a specific person or unknown identity to a place, activity, device, component, network or weapon of interest due to threat activity, homeland defense concerns and/or related analysis.

[11] An example of level 2 TE center is the Combined Joint Captured Materiel and Exploitation Center (CJCMEC).

fidelity and technical capability beyond level 1, due to the availability of advanced testing equipment and a greater number of subject matter experts. Level 2 TE capabilities should include or be co-located with an intelligence and targeting analytic capability where possible. If this capability cannot be established in theatre, the intelligence staff should ensure external analytic assets are available as a reach-back option to support level 2 TE activities.

2**.** **Level 2 technical exploitation results.** The TE results derived from these more advanced level 2 TE capabilities are processed and disseminated in hours-to-days from the point of collection. Level 2 TE activities may generate time-sensitive TE results, support rapid follow-on operations, and answer intelligence requirements.

3. The results of level 2 TE include, but are not limited to:

a. **Feedback.** Upon receipt of the collected material, level 2 TE personnel should provide immediate feedback to the level 1 TE element regarding the physical state of the material. In addition, they should also provide relevant lessons learned that might assist level 1 activities with the collection, preservation and handling of collected material. This feedback may be provided via voice communication or by a written report.

b. **Reporting.** Level 2 personnel prepare detailed TE assessments to include threat awareness trends and intelligence reports on adversary networks. Level 2 TE assessments and intelligence reports are fused with additional sources of information and other joint intelligence, surveillance and reconnaissance (JISR) results by intelligence analysts at an intelligence fusion cell. The types of reports, profiles, and documents produced at a level 2 facility include, but are not limited to:

- theatre threat occurrence summaries;
- BEI;
- alert and materiel source reports;
- adversary personnel and materiel profiles;
- law enforcement documentation;
- threat awareness reports; and
- new threat technologies or methods reports.

c**.** **Disposition of collected material.** If the collected material represents a new threat TTP, adversary capability or warrants additional exploitation to address knowledge gaps, a more detailed examination and exploitation should be performed within the level 2 center or forwarded to a level 3 TE location. Prioritisation of the collected material should be based on force protection and targeting considerations, time-sensitive information requirements and intelligence requirements. As level 2 TE personnel complete the TE process, the officer-in-charge or manager determines the need for disposal, archiving, temporary or indefinite storage, or forwarding to specified location in accordance with national, theatre and local commander policies.

2.3.3. Level 3 technical exploitation (out-of-theatre/strategic)

1. **Level 3 technical exploitation activities.** The collected material, which has been exploited at a level 1 location and/or a level 2 TE facility, can be further assessed and evaluated at a level 3 TE facility. At level 3 TE facilities, appropriately trained and qualified scientific and technical personnel apply their expert knowledge and techniques that are typically unavailable in theatre. Level 3 TE is usually a nationally-owned capability based in one of NATO's member nations.

2. Level 3 TE is conducted at specialised scientific and technological facilities and laboratories that apply rigorous procedures and operate in accordance with stringent accreditation standards.[12] Generally, they are equipped with sophisticated equipment that cannot be easily transported and deployed in theatre. These types of facilities provide the capability and capacity needed to conduct in-depth scientific testing, detailed component exploitation and the ability to reverse engineer an adversary's technology. Level 3 TE may use more invasive and possibly destructive methods than the methods and techniques used at a level 2 TE location.

3. Depending on the prioritisation of the collected material and the transit time to transport the material to a level 3 TE facility, level 3 TE personnel may need days-to-months to process and exploit the material and produce a TE result. Level 3 activities may generate results to support future operations and answer intelligence requirements. In delivering full-spectrum TE results, level 3 TE activities provide the highest level of assurance, fidelity and technical capability.

4. In NATO-led operations, level 3 TE capabilities and facilities may be provided by a single nation or by a group of NATO nations and coalition partners. Out-of-theatre level 3 TE activities may be distributed between different facilities and/or nations that may be requested to support the mission. If a nation does not maintain a national-level TE capability, a nation may be able to coordinate on a bi-lateral basis with those nations that possess such capabilities.

5. **Level 3 technical exploitation results.** Actions and results of level 3 TE include, but are not limited to:

[12] International Organization for Standardization (ISO) is an independent, non-governmental international organization with a membership of 162 national standards bodies. ISO 17025 is the international standard used by testing and calibration labtories to ensure their ability to consistently produce valid results.

a. **Feedback.** Level 3 TE results provide feedback to level 1 and level 2 counterparts for their awareness. Specifically, level 3 personnel should provide feedback on lessons learned that might assist level 1 or 2 in the preservation of collected material during collection and processing.

b. **Reporting.** The data and information derived from level 3 TE activities need to be shared with in-theatre personnel and allies to the greatest extent possible based on the need-to-share principle. Level 3 TE reports may include, but are not limited to:

- countermeasures to adversary TTP;
- support to intelligence;
- alert reports (e.g., high threat technologies /methods)
- genetic profiling;
- support to BEI;
- materiel and signature profiles;
- support to law enforcement activities; and
- technical assessments of electronic components.

c. **Disposition of collected material.** Following level 3 TE, collected material may be returned to theatre to support future operations. Alternatively**,** the collected material may be investigated further for strategic attribution, securely retained for judicial proceedings, distributed for training purposes, or destroyed.

2.4. CAPABILITIES

1. TE capabilities enable the systematic exploitation of all CEM in support of military operations. TE capabilities are a critical part of the TE framework and collectively can make a significant contribution to understanding the OE. However, each capability is unique. For any given capability, there are knowledgeable experts, trained personnel, specialized equipment, standard operating procedures, internal processes, databases, reporting requirements and unique report formats. TE capabilities and their potential intelligence value are summarized in annex C.

2. The commander assembles the available capabilities appropriate to meet the operational need. However, TE capabilities and the availability of specialists may vary between the three TE levels. Typically, there is no single level 1 TE location, level 2 facility, or level 3 facility that includes every available TE capability. To meet the

operational needs of the commander, the intelligence staff should prepare a TE management plan enabling commanders to manage the distribution of available capabilities and resources within the 3 level TE construct.

3. TE capabilities can involve complex and time-consuming procedures and require specialized equipment. The personnel needed to support TE capabilities, such as linguists, interpreters, technicians, materiel exploitation specialists, or liaison personnel, must be considered at the earliest stages of the planning process. Commanders need to be aware of these considerations and requirements and how best to employ them. While some capabilities may be readily available and used on-site at the point of collection, other capabilities require specialised structures. Within a chemical, biological, radiological
and nuclear (CBRN) environment, CBRN defence support to TE activities can include a deployable analytical laboratory consisting of CBRN detection, identification and monitoring capabilities. Other capabilities may have environmental constraints that require enclosed facilities with adequate power and environmental controls. Additionally, some capabilities may have limited use on-site and/or in-theatre and may require follow-on examination and assessment in a separate, controlled environment.

2.5. SUPPORTING ACTIVITIES

1. Supporting activities enabling the TE process include, but are not limited to:

a. **Triage**. Triage is the evaluation of CEM to determine exploitation value. Triaging is a key activity in the TE process and consists of three steps; 1) triage personnel screen the CEM for explosive, chemical, biological, radiological and physical hazards to determine whether they are safe to handle prior to any exploitation activity; 2) triage personnel determine which CEM might be relevant for TE and identify the capability/capabilities needed to fully exploit it; and 3) triage personnel prioritize the CEM based on priority intelligence requirements (PIRs). Selected items of interest that meet PIRs should be forwarded to the appropriate facility and exploited immediately. Prioritization also includes timely reporting and the sharing of information. Triage, as a supporting activity, is a continuous process and repeated each time an individual handles, transports or examines the collected items.

b**.** **Information management.** The management of information derived from CEM is essential to the TE process, Information management allows information to be collected once and used many times over.[13]

Within NATO, information management consists of two key elements; 1) information sharing and; 2) data archiving. Information systems and

[13] Information management is the means through which an organisation maximizes the efficiency with which it plans, collects, organises controls, disseminates, uses and disposes of its information, and through which it ensures that the actual value and the potential value of that information is identified and exploited to the fullest extent.

data repositories must be managed such that all who have a right and a need to the information and data can easily access it, and that the contents of the repositories are safeguarded from willful or negligent disclosure, loss, damage, or corruption. The system must have built in redundancies and data recovery plans. The system and data that resides on the system must also be secure, so that it cannot be accessed by those without proper authorization.

The use of common and shared databases is essential for an effective and functioning collaborative TE network. Accessible databases support the TE core activities enabling the exploitation and dissemination of information; greatly enhance the ability of coalition nations to share information; and afford opportunities to follow new lines of investigation. For example, software applications can compare data and information collected from a series of improvised explosive device detonations to determine similarities between events and identify commonalities in support of link and pattern analysis.

Data exchange standards should be based upon existing NATO standards.[14] Furthermore, a theater exploitation database needs to be coordinated and synchronized with other data storage and management systems.

c. **Transportation of collected material.** Successful TE is dependent on the safe and timely physical movement of material from the point of collection to a level 1 site and onward to a level 2 and/or level 3 facility if required. TE activities must be supported by a responsive joint transportation system, from the tactical through to the strategic levels, to ensure that exploitable data, information, materiel and materials are processed rapidly and efficiently. NATO, national and commercial resources may be used to meet transportation and logistical requirements depending on the type of material and desired delivery time. Shipments may require prioritised handling that necessitate the use of non-routine transportation methods. Arrangements can be made to use available ground transportation, but for high priority cases, air transportation may be required. Special considerations and subject matter expert advice may be needed for the transportation of hazardous items. Each transportation movement and transmittal of data and information should be documented to ensure compliance with legal requirements and associated intelligence needs.

d. **Disposition, storage and disposal of collected material.** Nations and NATO commanders will develop and implement procedures to ensure that any CEM that is transferred within and out-of-theatre and any data and/orinformation that is shared will be discoverable and traceable through to, and including, final disposition. Special consideration will be

[14] See AIntP-3, *Military Intelligence Data Exchange Standard*.

given to long-term storage, disposition and retention. These procedures will be developed as early as possible and managed with appropriate oversight to ensure compliance with applicable international and national law, agreements and policy.

The level 2 TE case manager will determine the need for disposing, archiving, temporary or indefinitely storing, or forwarding material for further exploitation. Considerations in determining the disposition of CEM include:

- significance of the material;
- resource availability/capacity at the TE location; and
- availability of national and strategic TE capabilities.

Based on the nature of the collected material, construction techniques, or other criteria, personnel may need to forward the material directly to national and strategic level 3 TE facilities. Whether the material is expeditiously forwarded to level 3 out-of- theatre location or is processed and exploited in theatre, the intelligence staff in coordination with the logistics staff needs to ensure there are appropriate storage facilities for each TE level in accordance with NATO policy, national policy and applicable regulations. To safely secure the CEM, all TE locations should have a storage facility attached to the triage location as well as a separate long-term storage area.

2.6. RESULTS AND SUPPORTED OUTCOMES

1. The TE process is designed to produce results and outcomes that contribute to answering the commander's critical information requirements, which consist of priority intelligence requirements and friendly force information requirements.[15]

2. **TE results.** The results from TE can support tactical, operational and strategic activities. At the tactical level, TE results can have an immediate impact on the OE to minimize, neutralize and/or defeat threats. The intelligence staff at a level 2 TE facility should ensure TE results are sent back to FETs and level 1 locations to support their capabilities and activities, as well as to re-focus their collection and TE priorities as required. At the operational level, TE results can directly support forces within the joint operations area and enable the cueing of JISR collection assets to locate and track high value individuals and refine targeting information. At the strategic level, TE results could have international implications or involve long-term effects, such as the disruption of international supply chains used by an adversary.

[15] For more information on intelligence requirements and intelligence requirements management see AJP-2.0, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security* and AIntP-16, *Allied Intelligence Publication for IRM&CM.*

3. The intelligence collection disciplines derive data and information from human sources, sensors and/or technical systems.[16] TE supports human intelligence (HUMINT) collection through technical and forensic examination of material obtained from captured persons or persons of interest. TE results can inform HUMINT by providing biometric signatures such as iris images, facial photographs, genetic samples,[17] fingerprints and other identifying information as well as captured or seized documents and media that can link individuals to events, locations, equipment, materials, and threat networks. The results of the TE process can also support counterintelligence personnel, for example, in the vetting of local staff, thus enhancing force protection. TE results can also be used in conjunction with measurement and signature intelligence (MASINT) sensor results providing an additional source of scientific and technical data and information. The type of information that is collected and extracted via the TE process can inform any of the MASINT sub-disciplines and supplement MASINT results.[18]

In addition to informing the intelligence collection disciplines, TE results support intelligence sub-disciplines such as technical intelligence (TECHINT). TE results can enable TECHINT analysts to assess the technical sophistication of adversary weapon systems to include their capabilities, limitations, vulnerabilities and countermeasures.

The integration and fusion of TE results with JISR results and other sources of information and intelligence enables analysts to produce detailed analytical products that can contribute to:

- an understanding of adversary networks, adversary TTP and the social cultural environment;
- human network analysis and support to targeting; and
- standing strategic intelligence requirements.

4. **TE outcomes**. In addition to TE results and findings that are used to support on-going analytical efforts, TE results can support a variety of other activities. Key supported outcomes can include, but are not limited to:

- component materiel attribution;
- countermeasures development;
- force protection;

[16] See AJP-2.0, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security,* for detailed information on intelligence collection disciplines.

[17] Genetic samples refers to deoxyribonucleic acid (DNA) testing and profiling.

[18] MASINT is divided into eight sub-disciplines: biometrics, radio, geophysical, electro-optical, nuclear, materials, multi/hyper-spectral, and radar. MASINT results, derived from ground-based, airborne and acoustic sensors, are typically used in conjunction with the data and information gathered from overhead and airborne imagery intelligence and signals intelligence collection capabilities.

- law enforcement investigations and legal proceedings[19];
- research and development, testing and evaluation;
- targeting; and
- training.

[19] The use of TE results for legal proceedings will depend on international and national laws. If CBRN substances are used as evidence, the collected samples must be analysed and confirmed by independent, accredited laboratories.

CHAPTER 3 COMMAND AND STAFF MANAGEMENT RESPONSIBILITIES

3.1. INTRODUCTION

1. A combined joint task force (CJTF) command structure may be established for a theatre of operations. The CJTF provides a flexible and efficient means to enable the Alliance to generate forces at short notice, providing deployable, multi-national, multi-service task forces (TFs) with appropriate command and control arrangements. Although the organizational structure elements and supporting units may differ for each operation to meet mission requirements, the basic concept, process and activities for technical exploitation (TE) can be applied to all entities at all echelons to varying degrees and level of detail.

2. The member Nations should have a common understanding what constitutes collected exploitable material (CEM) and the procedures regarding its handling prior to forming a CJTF. NATO, in conjunction with the troop-contributing nations supporting a CJTF, develops rules of engagement applicable to the particular operation or mission. Although the commander bears the overall responsibility for the handling of CEM, the commander delegates responsibility for the management of TE activities to staff elements.

3. The deliberate planning of TE activities requires extensive coordination with the CJTF staff elements, TFs and other specialised organizations and units. Staffs should familiarise themselves with the timelines, prioritization and logistical requirements associated with TE activities. TE activities should be conducted in accordance with recognised theatre standards as these activities are normally included as part of any combat operation. Furthermore, to ensure unplanned TE opportunities are not lost, the combined joint staff for intelligence (CJ2) and the combined joint staff for operations (CJ3) should develop standard operating procedures to guide the units or headquarters (HQ) when relevant CEM of potential intelligence or operational value is discovered during routine operations and patrols.

4. The following command and staff elements play key roles in managing the application and execution of the TE process to meet operational objectives and desired end states.

3.2. COMBINED JOINT TASK FORCE COMMANDER

1. The CJTF commander has overall authority and responsibility for TE, which is exercised through the CJ2. The CJ2 is the staff lead for TE and responsible for coordinating TE activities with other staff elements and echelons. TE elements should be fully integrated within the HQ with a full vision of the process and authorised to coordinate

and plan TE activities within the joint operations area (JOA), theatre or region. Therefore, TE elements should be closely linked to operational and intelligence staff elements, as the nature of TE operations require close and continuous cooperation.

2. Commanders must ensure that TE activities are conducted within the authorities, constraints and restraints of applicable national and international law, rules of engagement (ROE), and the orders, policies, and directives from higher authorities. Commanders must also ensure the forces under their command understand their roles and responsibilities and can comply with the relevant provisions in applicable laws, orders, policies, and directives related to the conduct of TE.

3. In conducting TE, NATO forces may require cooperation with the host nation (HN) military as well as civilian entities such as law enforcement and border security authorities. The relationships and responsibilities between these various entities should be included in a memorandum of agreement.

3.3. COMBINED JOINT TASK FORCE STAFF ELEMENTS

1. **Combined joint staff for personnel and administration (CJ1).** The CJ1 is responsible for providing, in coordination with the CJ2, qualified personnel and the expertise needed to support TE activities. For example, if a document exploitation capability is required in theatre, the CJ1 should provide interpreters and linguists for translation services.

2. **Combined joint staff for intelligence (CJ2).** As the commander’s staff element for intelligence, the CJ2 is responsible for prioritizing TE activities and ensuring information is produced and disseminated in accordance with the commander’s critical information requirements (CCIRs). The CJ2 staff element:

a. establishes and maintains the TE architecture in accordance with operational requirements;

b. in coordination with the CJ3, integrates and tasks TE activities in accordance with the intelligence collection plan (ICP);

c. develops and coordinates a TE management plan as a standardised appendix to the CJ2’s intelligence annex that addresses capabilities, resources, procedures, ROE, and training requirements;[20]

d. leverages the joint intelligence preparation of the operating environment and the joint intelligence, surveillance and reconnaissance (JISR) tasking processes to identify events and locations suitable for deliberate TE activities;

e. ensures the information derived from TE activities is shared with all TE teams to enhance subsequent TE activities, situational awareness and all-source intelligence production;

[20] Refer to annex B for an example of a TE management plan.

f. ensures information gaps that cannot be addressed by TE are fed back into the intelligence cycle for effective re-tasking via the JISR process;

g. plans and coordinates with the CJ3 and with subordinate and/or superior units and formations to integrate their deliberate TE collection activities;

h. coordinates with the combined joint staff for logistics (CJ4) to logistically sustain TE activities within theatre and ensures safe handling, packaging, and physical movement of material between TE facilities;

i. coordinates with the combined joint staff for communications and information (CJ6) to ensure the TE communications and information systems operate as required; and

j. develops and oversees information classification, disclosure, and security policies.

3**.** **Combined joint staff for operations.** Collection can be based on incidental/opportunistic collection tasking or deliberate collection tasking. In conducting tactical actions within the JOA, the CJ3 is often the first staff element to become aware of opportunities to collect and exploit material of interest. As these collection opportunities present themselves, the CJ3 should inform the CJ2 so that specialist support can be arranged and provided, in accordance with the tactical situation. When opportunities for deliberate TE collection activities arise, the CJ3 is responsible for the detailed planning and execution of the tactical actions undertaken to seize any material of interest.

4. **Combined joint staff for logistics (CJ4).** The CJ4 is responsible for:

a. providing logistical support to sustain TE activities within theatre and ensuring the safe handling, packaging, and physical movement of material between TE facilities (TEFs);

b. procuring and providing construction materials and stores for the establishment of collection points; and

c. recovering or disposing of collected material after it has been examined.

5. **Combined joint staff for communication and information (CJ6).** The CJ6 is responsible for ensuring TE information management systems are incorporated within the information sharing architecture within the operation. In addition, the CJ6 ensures TE communications and information technology systems operate as required.

3.4. TECHNICAL EXPLOITATION FACILITIES

1. The integration and synchronisation of the data and information derived from TE activities are essential to support intelligence requirements and operations planning. To support TE activities, the CJTF commander should establish a level 2 TE facility that serves as the central location in theatre for the collection, safeguarding,

identification, exploitation, reporting, and evacuation of collected material with potential intelligence value. The combined joint captured materiel exploitation centre (CJCMEC) is used in this publication as an example of a TEF-2 serving in this capacity. The CJCMEC should be established at a location within a permissive environment that is best suited for performing TEF-2 activities. In planning for TE, communication and logistical requirements need to be carefully considered to ensure the CJCMEC can effectively coordinate TE activities in theatre and out-of-theatre. If additional TE support is required, commanders can request TE support from out-of-theatre specialised facilities and laboratories.

2. As the operational-level focal point for TE activities in theatre, the CJCMEC should coordinate with the CJ2 to receive guidance and direction on TE priorities and obtain threat/situational updates within the operating environment (OE) impacting TE activities. The CJCMEC should guide level 1 TE activities conducted by FETs and coordinate directly with TEF-2s in theatre, as well as TEF-3s out-of-theatre (Figure 07). If additional TEFs are introduced within the theatre of operations, the TEF-2 managers should coordinate with the CJCMEC to ensure their activities are properly integrated within the TE construct.

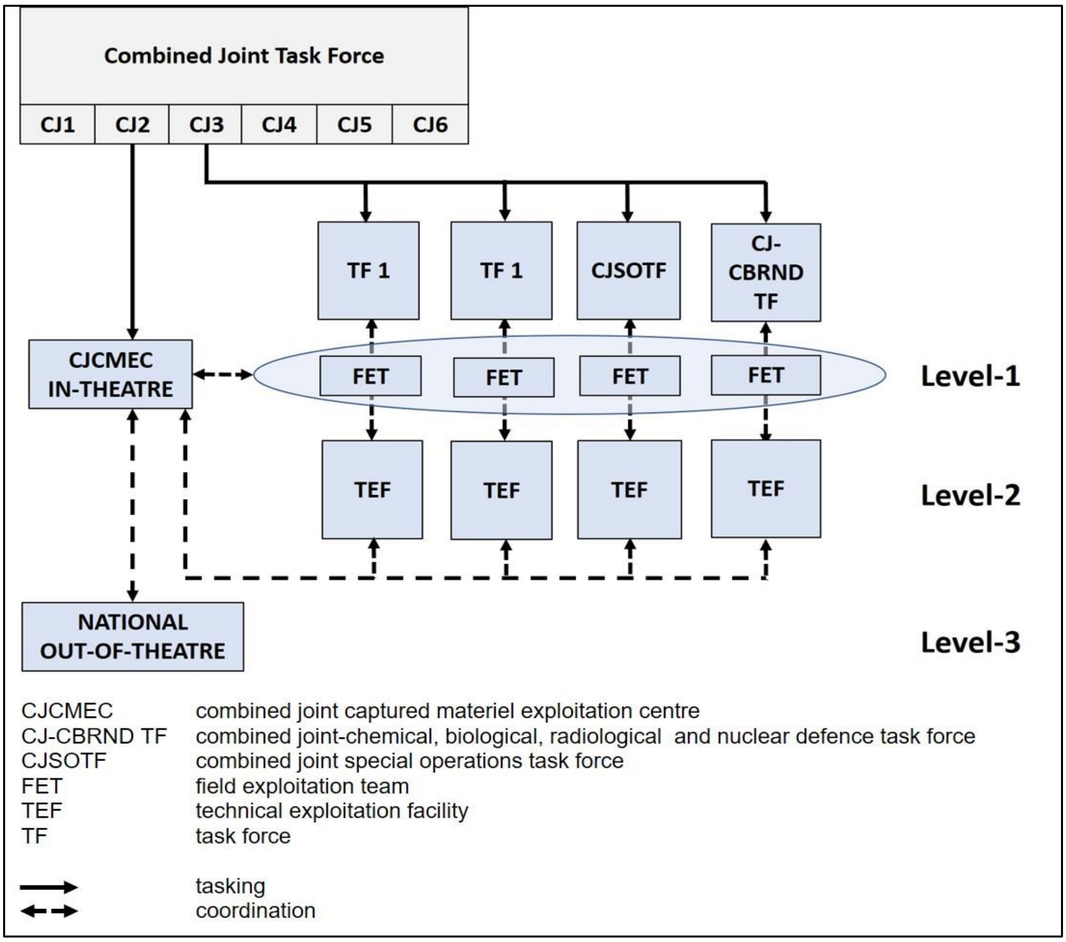

Combined Joint Task Force
CJ1
CJ2
CJ3
CJ4
CJ5
CJ6
TF 1
TF 1
CJSOTF
CJ-CBRND TF
CJCMEC IN-THEATRE
FET
FET
FET
FET
Level-1
TEF
TEF
TEF
TEF
Level-2
NATIONAL OUT-OF-THEATRE
Level-3
CJCMEC combined joint captured materiel exploitation centre
CJ-CBRND TF combined joint-chemical, biological, radiological and nuclear defence task force
CJSOTF combined joint special operations task force
FET field exploitation team
TEF technical exploitation facility
TF task force
tasking
coordination

Figure 07: Notional Command and Control Structure for Technical Exploitation.

3. **Combined joint captured materiel exploitation centre components**. CJTF commander determines how the CJCMEC will be integrated within the overall

command structure. As an intelligence function, the CJCMEC is aligned under the CJ2 and may consist of the following four sections:

a. **Operations.** The operations section is responsible for the planning and coordination of all CJCMEC operations and maintaining the current intelligence situation.

b. **Support.** The support section is responsible for providing administrative and logistics support to all CJCMEC elements and personnel.

c. **Communications.** The communications section is responsible for providing communications, automated information systems, and related maintenance support to all CJCMEC elements.

d. **Processing, exploitation and dissemination.** The processing, exploitation and dissemination section processes validated requirements; exploits CEM; and produces and disseminates TE results.

4. **Field exploitation teams.** The CJCMEC can form field exploitation teams from its organic assets to meet the immediate needs and requirements of echelons without a TE capability. These teams may be attached to units and can deploy forward or support rear area units as required. A document exploitation team or technical intelligence team could be formed to carry out complementary TE activities on site as the tactical situation allows. To take advantage of incidental collection opportunities, these teams should possess a broad range of technical expertise and should be trained in the use of specialized equipment and automated information systems. A sufficient number of teams should be organized and ready to deploy when needed within the JOA.

5. **Specialised technical exploitation teams.** In certain situations it may be necessary to form TE teams to carry out highly specialised technical analysis of a particular object or item. These specialised teams are formed in accordance with the task at hand and may be dissolved when they complete their mission. They may carry out their work in rear area facilities such as main workshops or outside the JOA at research and development facilities with highly advanced test equipment.

6. **CJCMEC functions.** The establishment of a CJCMEC will ensure TE activities are conducted in an efficient, coherent and structured manner. To achieve this aim, the CJCMEC must have a clear C2 structure with appropriate lines of authority delegated by the commander to the intelligence staff and through the CJCMEC's staff element. A key role of the CJCMEC is to ensure that there is a unity of effort and effective coordination amongst all stakeholders and partners, including HNs, in producing and disseminating TE results. The CJCMEC is comprised of a staff element and augmented with technical advisors to coordinate TE activities to satisfy intelligence requirements. The staff element:

a. serves as the functional manager and coordinating authority for all TE activities;

b. receives and processes CEM, including the ability to handle and store chemical, biological, radiological and nuclear substances if warranted by threat levels;

c. maintains a case open/close tracking tool for all CEM;

d. develops and coordinates a TE management plan as an appendix to the CJ2's Annex B to address NATO and CJTF guidance regarding the employment of TE activities;

e. when directed by CJTF, provides TE support to emerging priority TE requirements;

f. prioritises and tasks TE activities in a timely manner to meet the intelligence requirements in accordance with the ICP;

g. coordinates and deconflicts TE activities with other staff elements;

h. establishes procedures for the exploitation and evacuation of CEM in coordination with CJ4 and other organizations as required; and

i. produces and disseminates preliminary/complimentary technical reports and intelligence reports.

7. **Technical exploitation management plan.** During the operational planning phase, the CJ2 should develop a TE management plan to satisfy the CJTF CCIRs. If new CCIRs emerge during the operation, the J2 may need to revise the TE management plan as required. Any modifications to the plan could result in the re-distribution of level 1 and/or level 2 TE capabilities within the OE.

a. A detailed TE management plan ensures TE capabilities can be introduced in theatre and applied in an effective and efficient manner. The management plan should include relevant policies and authorisations, operational restrictions, terms of reference, command relationships, specific tasks and special instructions, as well as a matrix indicating the status of all available TE capabilities.

b. The TE management plan facilitates the planning, execution, and assessment of TE capabilities. The plan should be published as a standardised appendix to the CJ2's intelligence annex, which outlines intelligence requirements to meet the CCIRs during each phase of the operation. The plan should be considered as an authoritative planning document, approved and tasked by the CJ3, and applicable to all NATO nations and partners supporting the CJTF commander.

c. The TE management plan should be flexible and adaptable to the changing dynamics of the OE, the phasing of operations, and resultant changes to respective intelligence requirements. It should identify all TE capabilities that are available to the CJTF commander. Because some TE capabilities may be out of-theatre and/or supporting multiple operations, it is imperative that command relationships and requisite authorities be identified as early as possible in the planning process. The CJ2 should maintain close coordination with the CJ3 to prioritise and align TE capabilities as required in support of intelligence requirements.

3.5. TECHNICAL EXPLOITATION INFORMATION MANAGEMENT STRUCTURE

1. In response to CJTF direction, guidance and information requirements, the CJ2 staff element, in coordination with the CJTF staff, should establish an information management structure. The aim of this structure is to maximize efficiencies that will support TE tasking, coordination, and reporting activities in order to produce and disseminate results in a timely manner. The CJCMEC, or its equivalent, should play a central role within the TE process, serving not only as a TEF-2 but also as the coordinating authority to ensure there is an effective information flow between all TE levels (Figure 08).

2. At the point of collection, the tactical TE team lead and/or on-site commander will prepare a field exploitation report based on the findings and forward recommendations regarding the CEM to a level 1 site. The material exploited at a level 1 site is then typically transported to a TEF-2 for further examination.[21] Case managers at the CJCMEC or a nearby TEF-2 will then assign the material to the appropriate TE subject matter expert (SME) or a team of SMEs. Based on level 2 TE findings and results, the CJCMEC prepares TE reports that are coordinated and shared with all TE stakeholders. The CEM is then forwarded to a TEF-3 for further exploitation, final disposition, or long-term storage. As the CEM is transmitted/transferred throughout the TE chain, all material should be carefully documented. To maintain visibility on the material, an end-to-end TE reporting and tracking system is required.

3. Feedback and results should be provided to those units that contributed to level 1 tactical exploitation and to the intelligence requirement management and collection management staff element. Feedback gives commanders the ability to better assess their information requirements and adjust their collection plans accordingly. Intelligence analysts can use the feedback for link and pattern analysis to discern connections among activities that can result in further level 1 collection activities.

4. The criteria for assessing TE activities includes measures of performance (MOP) and measures of effectiveness (MOE). MOPs are criteria used to assess friendly actions tied to measuring task accomplishment. They are associated with objectives rather than end state conditions. An example of an MOP is the capture of a high-value target on the biometric-enabled watch list. MOE, on the other hand, assess end state conditions. Examples of MOE are a decrease in insurgent improvised

[21] In certain situations (e.g., time sensitive requirement for dissemination of TE results), CEM can be transferred directly from a level 1 to a TEF-3 for immediate examination.

explosive device activity or an increase in the disruption of bomb-making activities resulting from tactical site exploitation. When developed, MOE indicators provide the appropriate guidelines for developing intelligence collection plans and form the basis for assessing them.

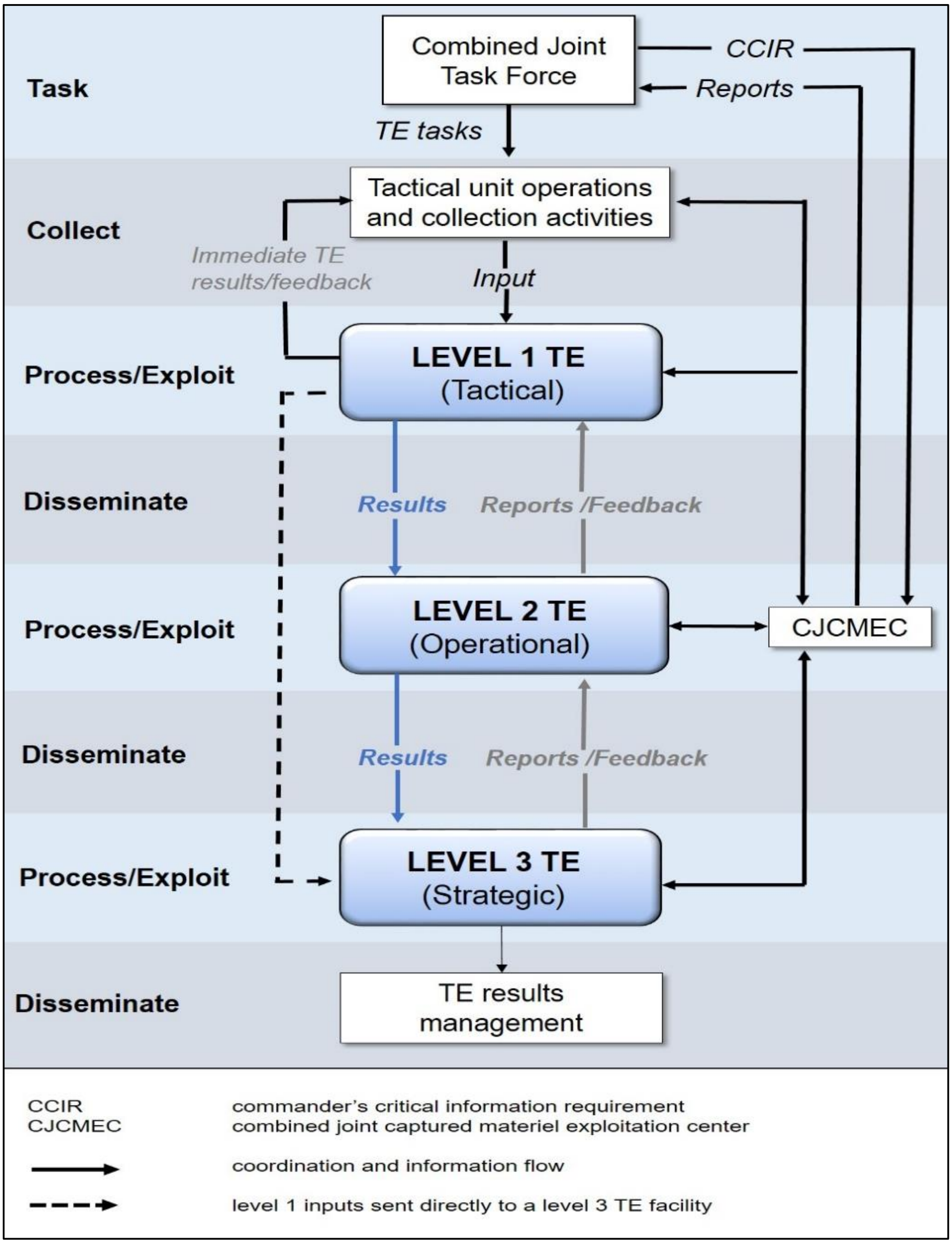

Task
Combined Joint Task Force
CCIR
Reports
TE tasks
Collect
Tactical unit operations and collection activities
Immediate TE results/feedback
Input
Process/Exploit
LEVEL 1 TE (Tactical)
Disseminate
Results
Reports /Feedback
Process/Exploit
LEVEL 2 TE (Operational)
CJCMEC
Disseminate
Results
Reports /Feedback
Process/Exploit
LEVEL 3 TE (Strategic)
Disseminate
TE results management
CCIR commander's critical information requirement
CJCMEC combined joint captured materiel exploitation center
coordination and information flow
level 1 inputs sent directly to a level 3 TE facility

Figure 08: Information Management Structure for Technical Exploitation.

CHAPTER 4 TECHNICAL EXPLOITATION CONSIDERATIONS

4.1. INTRODUCTION

1. In establishing the technical exploitation (TE) framework, key planning considerations include, but are not limited to:

- ensuring compliance with applicable international and national laws and standards;
- preparing a memorandum of agreement (MOA) and determining rules of engagement (ROE);
- establishing reporting standards; and
- developing training opportunities.

4.2. LEGAL CONSIDERATIONS

1. TE activities are constrained by laws, policies, agreements and rules. The conduct of TE activities, as part of a NATO operation, will follow NATO policies and directives and must be in accordance with international law, MOA and ROE including applicable host nation (HN) law. Commanders and the intelligence staff should consult with their legal advisors if they have any doubt or question regarding the legal standing of their planned TE activities.

a. **Law of war and international law**. The law of war is that part of international law that regulates the conduct of armed conflict. The law of war encompasses all international law for the conduct of conflict binding on the state or its individual citizens, including treaties and international agreements to which the state is a party, and applicable customary international law.

b. **Customary international law.** Customary international law results from a general and consistent practice of states that is adhered to from a sense of legal obligation. Customary international law is an unwritten form of law in the sense that it is not created through a written agreement by states. Customary international law is generally binding on all states, but states that have been persistent objectors to a customary international law rule during its development are not bound by that rule.

c. **National laws.** The national laws of troop-contributing nations (TCNs) may impose greater restrictions on troops from those nations, but they must not give them greater latitude than those imposed by NATO. Nations must inform the NATO command staff when their forces will be operating under restrictions greater than those imposed on the force as a whole.

d. **MOA.** The capabilities required to completely exploit all collected exploitable material (CEM) encompasses a broad range of scientific and technical skills. Lead capability nations may be identified to provide a NATO-led force with the necessary expertise, organisation and facilities for the employment of TE in support of NATO missions. The responsibilities of these lead capability nations and the procedures for the employment of TE may be set out in a specific MOA. At a minimum, a MOA, in support of a combined joint task force, must comply with the provisions of the Geneva Convention and other applicable international law. A MOA should identify the standards participating nations agree to follow with respect to TE. These standards should cover, but are not limited to, the following procedures:

(1) Collection, handling, preservation, and documentation of CEM.

(2) Handling, storage, transportation and disposal of hazardous CEM.

(3) Emergency mitigation measures to be used in the event of an accident.

(4) Final disposition of the CEM, including legal ownership as well as the financial and logistical responsibility for their final removal or destruction.

(5) Handling of hazardous material and samples used for legal proceedings.

e. **ROE.** When conducting TE, commanders must abide by clearly articulated ROE. At the outset of an operation, and in conjunction with all TCNs, NATO develops a common set of ROE. The ROE that are derived under the authority of the North Atlantic Council are applicable as the minimum standard for all participating forces.[22] At a minimum, these rules must be compliant with applicable international law. The ROE will provide the authorisation for, or limits on, the use of force and the conduct of intelligence collection operations and activities, including TE activities. Based on a clear understanding of the operational requirements and ROE, nations agree to commit TE capabilities and personnel under the control of the NATO commander. Nations may impose more restrictive ROE on their forces committed to NATO, but national ROE may not be more permissive.[23]

[22] For more information on ROE, see MC362/1.

[23] The conduct of national forces operating in the same area of operations as NATO, but which have not been declared or transferred to under NATO command, are beyond the scope of this doctrine.

f. **Command and individual responsibilities.** Observance of international laws and NATO orders, policies, and directives is both a command and an individual responsibility. In accordance with the mission mandate and as the applicable international law allows, personal property, including that found in pocket litter, may be taken and examined for intelligence purposes. However, any collected personal property must be protected and safeguarded and returned to the owner at the earliest time and as operations allow. When the property cannot be returned to the lawful owner, policy and agreements with the HN must be in place to waive this right, or compensation provided in accordance with legal considerations and local custom.

TE applies methods and techniques that are least invasive and destructive to ensure the maximum use of all exploitation capabilities, accurate and thorough exploitation, and possible future support to legal proceedings. The commander should decide the balance of exploitation activities conducted in support of intelligence vice legal proceedings based on the nature and the phase of operations.

NATO forces may be used to replace the indigenous police force and assume a stability policing mission. In this capacity, NATO forces can continue to collect material provided the collection and exploitation activities are conducted within the legal framework, including applicable HN law.

4.3. INFORMATION MANAGEMENT

1. **Chain-of-custody documentation.** When collecting and handling CEM, personnel should use proper procedures to preserve the material that may have intelligence value. Detailed reporting and labelling enable further collection and processing activities in accordance with standard procedures.[24] It is paramount that chain-of-custody documentation is maintained from the point of collection and throughout the TE process. In some cases, chain-of-custody records may be needed for judicial proceedings.

2. When CEM is transferred from one location to another, a chain-of-custody report should be attached and forwarded along with the shipment. Chain-of-custody reports typically consist of four sections:

a. **Section 1: Administrative.** The administrative section includes the reason, time, location, and date the CEM was obtained.

b. **Section 2: CEM description.** This section includes an accurate and detailed description of the CEM to include its composition, condition, dimensions and weight if applicable.

[24] For more information on the intelligence collection process and intelligence processing, see AJP-2.7, AIntP-14 and AIntP-18.

c. **Section 3: Change-of-custody.** When a change-in-custody occurs, the custodian in control of the CEM notes the change-of-custody. The signature, printed name, and rank or title of the individual who initially accepted receipt of the material is noted.

d. **Section 4: Rationale for change-of-custody.** In this section, the custodian provides the rationale as to why the CEM was transferred from one custodian to the next.

3. **TE reporting.** TE reporting provides detailed information about the CEM and should be submitted in accordance with relevant reporting procedures. Within the joint operations area (JOA), TE specialists assigned to a task force and conducting initial field exploitation activities typically have their own initial reporting requirements.[25] Initial level 1 TE reporting may include, but is not limited to:

a. **Initial field exploitation report.** The initial field exploitation report is a written or verbal report prepared by the field exploitation team (FET) upon the discovery or seizure of material believed to be of intelligence interest. The FET transmits the report through the chain of command to the first echelon with a TE capability. At a minimum, this initial report should contain facts that answer the six basic interrogatives: who, what, when, where, why and how.

b. **Level 1 TE report.** At the level 1 TE site, intelligence analysts and/or TE subject matter experts (SMEs) prepare a level 1 TE report. The level 1 TE report is based on the compilation of information derived from other field exploitation reporting. Additionally, TE SMEs initiate chain-of-custody procedures, categorizing and recording the CEM.

After extracting the relevant information to meet the tactical commander's immediate information and intelligence requirements, level 1 personnel will then send the level 1 TE report along with the material to a level 2 facility for further exploitation and assessment.As there are unique reporting requirements and formats for each TE capability, a standardized level 1 TE reporting format should be considered. A standardized TE report format provides TE SMEs the means to document and record their assessments and evaluations as the material is transferred from one TE facility to the next.[26]

4**.** **Information sharing.** TE results should be shared with NATO, coalition and other partners, and may need to be shared with civilian and other organisations, such as law enforcement. This may require a robust, scalable, open system architecture

[25] Examples of initial TE-related reporting include: preliminary technical reports (PRETECHREPs), complimentary technical reports (COMTECHREPs), explosive ordnance weapons intelligence team task order and level 1 exploitation report (EO 400 WIT TASK L1 EXPL REP), explosive ordnance level 2 exploitation report (EO 500 L2 EXPL REP), intelligence reports (INTREPs), SPOT reports, CBRN and MASINT reports.

[26] Refer to AAP-11, *NATO Message Catalogue*, for TE-related message formats.

that enables widespread information sharing. It is vital to have a robust, collaborative, data-sharing architecture established that can rapidly communicate raw data/information and TE results. Considerations for sharing TE results include, but are not limited to:

a. **An end-to-end system architecture.** Data and information may be collected at any level and stage throughout the TE process. Therefore, there is a requirement for a robust end-to-end system to ensure that data can be collected and transmitted in austere conditions. This data should be collected and transmitted in a standardised manner to maximise sharing, replication and data basing. Information systems should reach to the lowest tactical level so that FETs can be supported during their tactical collection activities. TE results of immediate tactical value, collected and produced co-incident with the initial collection effort, should be immediately passed to the supported tactical commander. In addition to the tactical level, all levels of the TE architecture should be connected to this network, including national level facilities and laboratories.

b. **Standardized format and methodology.** The distribution of information resulting from TE should be presented in a standard format and vocabulary, using appropriate forms and electronic capabilities. To ensure effective information sharing, reports should be standardized to include the assignment of a unique identifier/case number. A standardised TE methodology and report format provides TE personnel the means to catalogue all items that are an integral part of each case. The identifier/case number provides a lifetime affiliation method to associate all related items through an established workflow, enabling coordinated current and future exploitation.

c. **Writing for release.** Mechanisms are required whereby TE data and information can be gathered and shared in a timely manner within NATO and with non-NATO entities. TE reporting and production should be guided by the responsibility-to-share concept in accordance with NATO´s existing security policy. The source of the information may need to be protected and the information itself may need to be sanitized to protect the source in order to share information with others. If applicable, the product may have to be written at a different classification level to ensure that the information will be available to those who need it. This "writing for release" is a key concept of coalition operations.

5. **Data archiving.** Data at all levels needs to be archived to support future operations. Archived data, consisting of TE results and reporting, can be a valuable source of information that may aid future targeting, intelligence analysis and/or support to legal proceedings. In addition, archived data can provide historical context to current and future operations and enhanced opportunities to respond to time-sensitive requests for information. To be useful, the data should be managed to retain its integrity and authenticity by applying standard handling and processing methods. The

stored information must also be readily accessible and retrievable by the NATO nations through common information sharing tools. Any personal data that is collected must be processed in accordance with national laws and international treaties.[27]

4.4. TRAINING REQUIREMENTS

1. TE activities require personnel that are SMEs or highly skilled support personnel. The fundamentals of the TE process should be covered during pre-deployment training. However, depending on conditions within the JOA, SMEs and support personnel may require specialized training and equipment prior to their arrival in theatre. Deployed units, SMEs and support personnel must be able to operate in a work environment that is suitable to triage, process, exploit, and store hazardous material. Commanders and staff need to be aware of the types of training and equipment required and should consider these requirements early in the planning stage.

2. Given the wide spectrum of activities that are conducted within the TE framework, personnel with diverse backgrounds and extensive analytical training are needed. While most of the scientifically-focused functions are performed by civilian SMEs, there are many tasks that can be performed by deployed military units. Tactical manoeuvre units deployed on the battlefield will often encounter high value CEM during the conduct of their specific missions and operations. Whilst it is advantageous to have specialists assigned to these manoeuvre units to assist them with level 1 TE, such specialists will seldom be available to support all units. Tactical units should therefore be trained by specialists to conduct rudimentary level 1 TE.

3. To achieve the aim of TE, there needs to be an awareness that any physical material that is used, discarded or handled by an adversary is of potential value and could contribute to answering intelligence requirements, if properly preserved, processed and exploited. FETs need to understand the basic principles of TE and the ability to detect, recognise and identify items of interest. At a minimum, personnel should be trained in:

a. basic collection and material preservation skills;

b conducting systematic and thorough searches;

c. non-destructive collection procedures and techniques;

d. recognising various documents, media, and other types of CEM that may be of potential intelligence value;

e. assessing and documenting the tactical context in which the CEM was obtained; and

[27] Refer to Biometrics Framework Policy, PO (2018)0235), for information on the archiving of personal data derived from biometrics characteristics analysis.

f. identifying potential witnesses and conducting interviews.

4. Training considerations for TE include general training, highly specialized individual training, collective training and training for personnel supporting the intelligence staff.

a. **General training.** Where TE is expected to be used widely within an operation, general training for deploying units should include familiarization with the TE process and activities, basic detection and collection methods and safety awareness. Planners need to determine if these basic skills are included as part of the unit’s pre-deployment training regime or whether this training can be accomplished in-theatre using mobile training teams.

b**.** **Individual training.** Most TE skills require highly specialised training and levels of competency. The training needed to conduct level 2 TE may only be available at civilian training facilities on an individual basis.

c**.** **Collective training.** Given the complexities and timelines associated with conducting exploitation activities, it may be necessary to establish specific courses to develop a cadre of specialists conversant with the various processes and activities required to conduct TE. Within the JOA, multiple TE teams, units and SMEs will need to effectively coordinate and interoperate with each other especially within contaminated areas and within a chemical, biological, radiological and nuclear environment. Pre-deployment training opportunities should include an interoperability component.

d**.** **Specialised training.** Within the intelligence cycle, all-source analysts fuse TE results with information derived from the intelligence collection disciplines and other sources. To support the all-source analyst, personnel assigned to the intelligence staff at an in-theatre TE site or facility may require specialized training in one or more intelligence collection disciplines. This specialised TE-oriented training for in-theatre personnel would ensure that analysts receive the TE results in a timely fashion and in the proper format.

INTENTIONALLY BLANK

ANNEX A SAMPLE TECHNICAL EXPLOITATION MEMORANDUM OF AGREEMENT

A.1. In the event a NATO nation agrees to be the lead nation for technical exploitation (TE), a memorandum of agreement (MOA) will be developed in coordination with other participating nations. The aim of the TE MOA is to:

- describe the scope of the TE effort and how it will be organised and commanded;
- identify internal and external TE facilities, laboratories, and units; and
- establish information sharing arrangements between participating nations and stakeholders.

A.2. The TE MOA should provide detailed information regarding the capabilities to be provided by each of the participating nations. In particular, it is important to confirm:

- the nations participating in the MOA and the extent to which they are participating;
- the types and levels of TE capabilities the participating nations will be committing to multi-national facilities, laboratories, and units;
- the types and levels of TE capabilities participating nations will be committing to the NATO operation, but that will remain under national control;
- the identification of all participating national-level TE facilities and laboratories, and the designation of which of these facilities and laboratories will lead the level 3 TE effort for which types of collected material;
- the extent to which personnel, from participating nations, assigned to multi-national level 2 TE facilities, laboratories, and units may be tasked to conduct level 1 TE collection activities;
- the extent to which personnel, from multi-national level 2 TE facilities, laboratories, and units may be attached to other facilities, laboratories, and units;
- the extent to which personnel, from nationally-controlled TE facilities, laboratories, and units may be attached to multi-national facilities, laboratories, and units; and
- the expected troop rotation schedule, for each nation committing personnel to multi-national facilities, laboratories, and units.

A.3. The TE MOA should identify the standards participating nations agree to follow with respect to any collected exploitable material (CEM). These standards should cover, but are not limited to, the following procedures:

- collection, handling, preservation, and documentation of CEM;
- handling, storage, transportation, and disposal of hazardous material;

- emergency mitigation measures to be used in the event of an accident or mishap; and
- final disposition of the CEM, including final ownership of the material and financial and logistical responsibility for its removal or destruction.

A.4. The collection and use of biometric information are a significant concern for many nations. As such, any MOA that is developed should include a discussion of the standards and procedures to be used for the collection, processing, identification, recording, storage, retention, and disposal of biometric data and information. These biometric standards and procedures should not be focused solely on persons of interest. These standards and procedures should apply to members of the coalition as well. The standard needs to address how the biometric information associated with these members will be collected, stored, used, and disposed of, so that the data can be used for exclusion purposes if coalition personnel inadvertently contaminate the material.

A.5. Standards for a multi-national communications and information system (CIS) should also be included in the MOA. As with all NATO-led operations, common NATO systems and standards should be used to the greatest extent possible. When this is not feasible, the lead nation should provide the appropriate system to support TE activities. The responsibilities of the participating nations with respect to the provision of computers and network connectivity should be clearly articulated in the MOA, so that the CIS network can be operational as soon as possible as units are deployed to the joint operations area.

A.6. Nations have specific legal responsibilities concerning the handling of persons detained by their military forces. When nations agree to collect and exploit material obtained from or associated with persons of interest, the TE MOA should address:

- procedures and standards for the handling and safekeeping of personal property, information, and biometric data; and
- the rights of each participating nation with respect to observing and confirming that the other participating nations are maintaining the agreed standards.

A.7. The use of TE results for legal proceedings will depend on international and national laws. This aspect of TE should be addressed in the TE MOA as well. For example, if samples of chemical, biological, radiological and nuclear substances are used as evidence, the MOA should stipulate that the collected samples must be analysed and confirmed by independent and accredited laboratories.

ANNEX B TECHNICAL EXPLOITATION MANAGEMENT PLAN

B.1. **Technical exploitation management plan outline.** The following outline serves as a starting point for developing a comprehensive technical exploitation (TE) management plan with instructions to complete the outline.

a. **Annex "X" to the operations plan (OPLAN)**
Provide title of annex and linkage to supporting plans, as applicable.

b. **Planning guidance**
Provide NATO guidance to the combined joint task force (CJTF) and reference existing NATO policies affecting management and conduct of TE activities.

c. **CJTF strategy and guidance**
Guidance may include lines of effort, end states, commander's critical information requirements, host nation agreements and coordination.

d. **CJTF objectives**
Objectives should be clear, concise, and attainable. CJTF objectives may cover TE capabilities; organizational structure; process and disposition of collected exploitable material.

e. **Operational restrictions**
Address limitations and constraints on the use of TE capabilities in accordance with NATO policies (e.g., international law) and CJTF guidance (e.g., protection of civilians).

f. **Terms of reference**
List relevant terms and definitions applicable to performing TE activities.

g. **Command relationship/authorities**
Identify tasking authorities and command relationships designated by CJTF.

h. **Tasks**
Provide specific tasks to CJTF staff elements and components/task forces.

i. **Asset command relationships**
Identify command relationships between the CJTF and supporting components/task forces that have TE assets. Example relationships may include operational and tactical control (TACON) of in-theatre TE assets and establishing direct liaison authorities.

j. **Special instructions**
Provide any specific guidance and direction involving unique aspects

of TE activities. Examples may include planning and executing TE activities in coordination with a combined joint-chemical, biological, radiological and nuclear defence-task force or special operations forces task force.

k. **Named areas of interest (NAIs)**
Identify one or more geographical areas or systems (e.g., theatre ballistic missiles) as an NAI where collected exploitable material (CEM) will satisfy specific information and intelligence requirements.

l. **OPLAN directive/guidance**
Provide additional guidance on TE activities that directly support OPLAN requirements. This may result in NAIs or CEM having a higher TE priority.

m. **Organization**
Develop an organizational chart that shows TE-assigned positions and associated subject matter experts (SMEs).

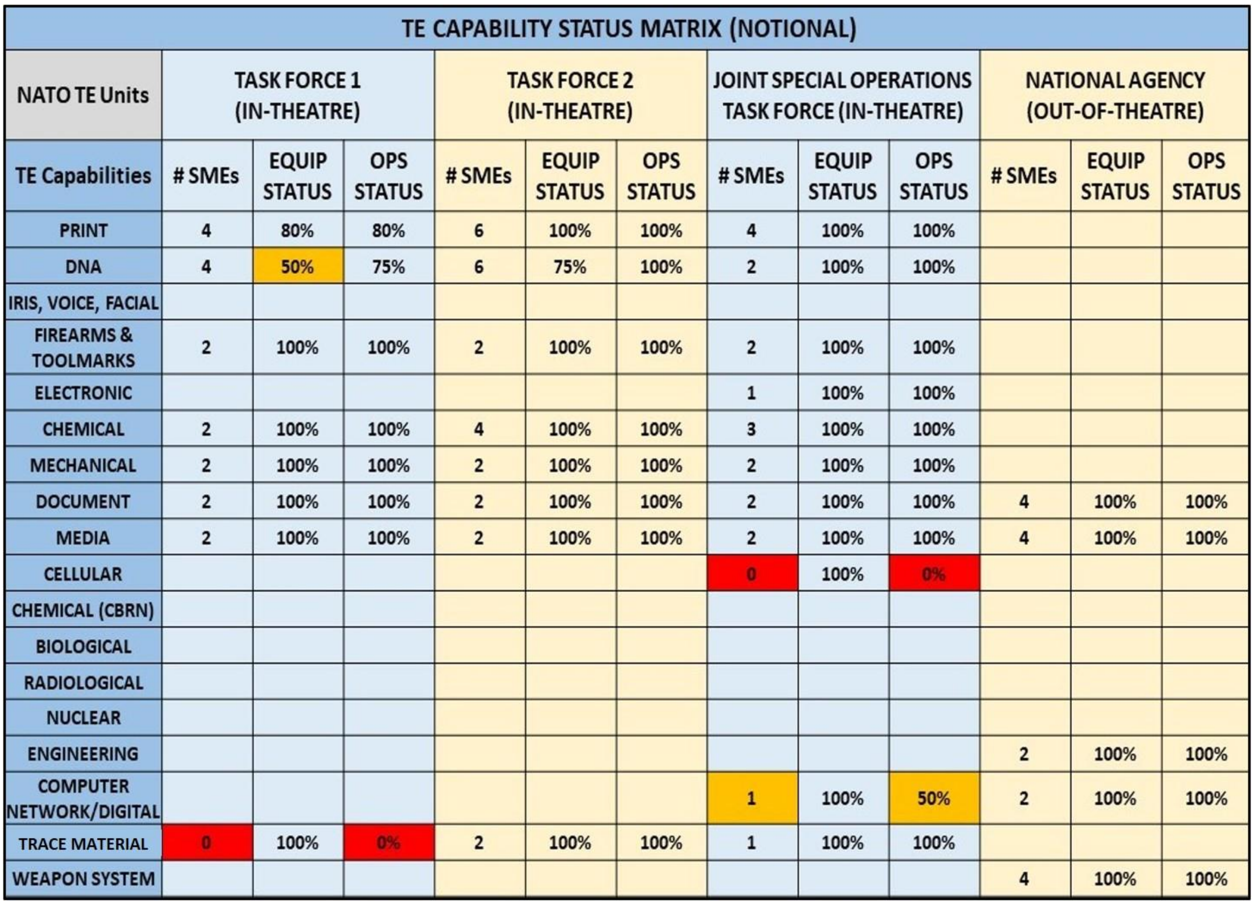
n. **Communications**
Provide contact information to include phone and email information for TE SMEs operating on both unclassified and classified networks. Information should also include classified/unclassified video teleconferencing capabilities and chat room access.

o. **Systems**
Provide information and graphics (e.g., system architecture) outlining primary information management systems used to perform, produce and communicate activities. Classification guidance on communications regarding TE activities should be provided as well.

p. **Activities**
Outlines specific information on TE assets, to include:

- Organizational identification
- Geographical location (i.e., in-theatre, out-of-theatre)
- Task organization (e.g., TACON to task force 2)
- Dissemination and reporting
    - System of record
    - Reporting formats and products

B.2. **Example of a technical exploitation capabilities status matrix**. The TE capabilities matrix supplements the TE management plan allowing commanders and staff elements to maintain visibility on the operational status of all TE capabilities (both in-theatre and out-of-theatre). The matrix can also be used as a resource/asset planning tool to allocate and realign TE capabilities and personnel as required.



TE CAPABILITY STATUS MATRIX (NOTIONAL)

NATO TE Units	TASK FORCE 1 (IN-THEATRE)			TASK FORCE 2 (IN-THEATRE)			JOINT SPECIAL OPERATIONS TASK FORCE (IN-THEATRE)			NATIONAL AGENCY (OUT-OF-THEATRE)		
TE Capabilities	# SMEs	EQUIP STATUS	OPS STATUS	# SMEs	EQUIP STATUS	OPS STATUS	# SMEs	EQUIP STATUS	OPS STATUS	# SMEs	EQUIP STATUS	OPS STATUS
PRINT	4	80%	80%	6	100%	100%	4	100%	100%			
DNA	4	50%	75%	6	75%	100%	2	100%	100%			
IRIS, VOICE, FACIAL												
FIREARMS & TOOLMARKS	2	100%	100%	2	100%	100%	2	100%	100%			
ELECTRONIC							1	100%	100%			
CHEMICAL	2	100%	100%	4	100%	100%	3	100%	100%			
MECHANICAL	2	100%	100%	2	100%	100%	2	100%	100%			
DOCUMENT	2	100%	100%	2	100%	100%	2	100%	100%	4	100%	100%
MEDIA	2	100%	100%	2	100%	100%	2	100%	100%	4	100%	100%
CELLULAR							0	100%	0%			
CHEMICAL (CBRN)												
BIOLOGICAL												
RADIOLOGICAL												
NUCLEAR												
ENGINEERING										2	100%	100%
COMPUTER NETWORK/DIGITAL							1	100%	50%	2	100%	100%
TRACE MATERIAL	0	100%	0%	2	100%	100%	1	100%	100%			
WEAPON SYSTEM										4	100%	100%

Figure 09: Example of a Technical Exploitation Capability Status Matrix.

INTENTIONALLY BLANK

ANNEX C TECHNICAL EXPLOITATION CAPABILITIES

C.1. The capabilities required to exploit collected material encompass a broad range of scientific applications, methods and techniques. The following table includes a list of the various capabilities, a summary description, and their relative intelligence value. New capabilities can be included and descriptions for existing capabilities modified as methods and techniques improve over time.

Capability	Description	Intelligence Value
Chemical exploitation	▪ Chemical exploitation, also referred to as forensic chemical analysis, is focused on the detection and identification of substances by determining their chemical signatures. ▪ Chemical exploitation specialists use presumptive testing methods to determine the chemical signature of explosives, explosive precursor elements, improvised explosive device (IED)-related material, as well as other substances such as illicit narcotics and pharmaceuticals. Handheld spectrometers or colorimetric reactive kits enable personnel to rapidly determine the presence of hazardous substances and provide timely reporting and alerts.	▪ Comparison between collected chemical substances and reference compounds or databases helps to provide a better understanding of the chemical threat and can provide critical information about the operational environment. ▪ Link analysis. Detailed chemical analysis to determine the makeup and characteristics of the collected substances is completed at a reach-back facility for chemical element comparisons and trend analysis. Based on the chemical analysis of homemade explosives used in an IED event, chemical exploitation results can aid in the link analysis among multiple IED events.
Chemical, biological, radiological, and nuclear (CBRN) defense support to technical exploitation (TE)	▪ CBRN defence support to TE is focused on the sampling and identification of biological, chemical, radiological and nuclear substances, CBRN weapons and means of delivery, and devices employed in CBRN incident or materiel suspected to be contaminated ▪ On the presumption of an adversary's use of CBRN substances, or by discovery of suspected CBRN substances and/or a positive alarm of detectors, the commander may order sampling teams to gather information and determine the identity of the CBRN hazard in conjunction with specialized	▪ CBRN defense support to TE provides unambiguous identification of CBRN substances and contributes to determining attribution for a CBRN incident.

	CBRN laboratories. Sampling can be either tactical, operational or forensic sampling. ▪ Commanders should be aware that not all TE activities are safe to perform with organic forces and equipment. Based on CBRN threat assessments, some TE missions may require specialised CBRN defence support capabilities and protective measures.	
Digital network exploitation	▪ Digital network exploitation is the application of computer science methods and techniques to detect, extract, and analyze data obtained from computer network systems. ▪ Digital network exploitation specialists extract data and information from networked systems and data repositories. Activities can include identifying router data/wireless access points and detecting evidence of offensive attacks on websites such as distributed denial of service attacks.	▪ Digital network exploitation results can contribute to network characterization, vulnerability assessments, indications and warning alerts, and the development of countermeasures.
Deoxyribonucleic acid (DNA) analysis	▪ DNA analysis is an automated method of biometric identification based on the genetic material obtained directly from an individual or object. ▪ DNA specialists can establish an individual's genetic profile and match previously produced DNA profiles retained in existing DNA databases. ▪ When handling DNA samples, appropriate personal protective equipment should be used to avoid contact that might contaminate the samples.	▪ DNA specialists can provide a biological link between individuals, objects and events. DNA matches enable identity management, verification, linkages to threat networks and attribution. ▪ DNA analysis often overlaps with latent fingerprint; trace material, firearms and tool marks capabilities.
Document and media exploitation (DOMEX)	▪ DOMEX is focused on the processing, translation, analysis and dissemination of collected hard copy documents and electronic media. TE may require the application of several DOMEX capabilities including document exploitation, media exploitation and cellular phone exploitation. ▪ Within the context of TE, a document refers to any type of recorded information regardless of its physical form or characteristics. Media refers to objects on which data can be stored magnetically, optically, chemically, mechanically, electronically, or digitally. Cell phones are portable communication devices that can store data and information. Smartphones are mobile devices that combine cellular and mobile phone computing functions into one unit.	▪ DOMEX may provide information on the strategies, plans, operations, activities, tactics, weapons, personnel, contacts and relationships, finances, and logistics of adversaries, terrorists, and criminal networks.
Electronic exploitation	▪ Electronic exploitation is focused on the rapid characterization and assessment of electrical/electronic systems and components.	▪ Electronic exploitation results enable specialists to: develop capability

	▪ Electronic exploitation specialists conduct a functional analysis of electronic devices to determine basic signaling characteristics; voltage levels; electrical connections; operating frequencies; component configuration identification and operating profiles/modes.	profiles; assess trends; determine vulnerabilities; and develop countermeasures.
Facial recognition	▪ Facial recognition is an automated method of biometric identification that applies a technology capable of verifying an individual's identity based on a digital image or video source. ▪ This technology examines parts of the human face that do not change significantly over time such as the distance between the eyes, the length of the nose, or the angle of the chin. ▪ Automated facial recognition analysis produces results based on probabilities. Once the sample is collected and compared with the template database, positive identifications are made according to the level of accuracy set in the system.	▪ Facial recognition results enable identity management, verification, link analysis and attribution.
Fingerprint recognition	▪ Fingerprint recognition is an automated method of biometric identification confirming the identity of an individual. Fingerprints are impressions of the friction ridge of human skin and are unique to an individual. ▪ Fingerprints may be collected through the biometric enrollment of a subject using a specialized collection device. These devices may automatically search a larger database, or a smaller "on-board" sampling of fingerprints, to confirm the identity of an individual.	▪ Fingerprint matches enable identity management, verification, link analysis and attribution. ▪ Fingerprint recognition often overlaps with DNA and trace material analysis.
Firearms and tool marks examination	▪ Firearms and tool mark specialists examine firearms, ammunition components, ordnance fragmentation, bullet trajectories, and tool marks. ▪ Firearm specialists can determine the rifling characteristics and specifications of a firearm, its country of origin and manufacturing details. ▪ During the manufacture of a firearm, the machining process leaves unique and microscopic marks on some of the firearm's parts. When most firearms are fired, these tool marks are transferred to the discharged ("spent") cartridge casings and bullets. This allows examiners to establish a link between the firearm and the ammunition.	▪ Firearm and tool mark examiners can determine the relationship of a firearm or tool to an individual or event. Results can be used for link and trend analysis, threat assessments and support force protection (FP). ▪ Results can overlap with DNA, trace material and fingerprint analyses
Forensic engineering	▪ Forensic engineering exploitation is a capability that assesses the design of	▪ Forensic engineering exploitation provides key

exploitation	adversary facilities, personal and collective equipment, materiel, vehicles, and buildings. ▪ Forensic engineering specialists conduct design and effects analysis. Assessments can be conducted to determine the effects weapon systems and detonations have on structures (e.g., bridges, buildings, and tunnels) and materiel, as well as the effects on the environment. ▪ Specialists apply reverse engineering methods to determine the component's physical dimensions, design features, manufacturing methods, and material properties.	information and assessments to support engineering design and survivability improvements to weapon systems and other areas, such as combat equipment, personal protection, and military construction. Forensic engineers may coordinate with weapon system exploitation specialists to collaborate on vulnerability assessments and the development of countermeasures.
Iris recognition	▪ Iris recognition is an automated method of biometric identification. High quality images of the human eye focused on the iris is a means of identifying persons of interest. ▪ Once the image is captured and converted into a digital biometric framework, a trained/certified examiner uploads the file to an existing database for comparative analysis and vetting.	▪ Iris recognition technology provides near-instant, highly accurate identity verification.
Mechanical exploitation	▪ Mechanical exploitation is the examination and evaluation of the functioning components of mechanical devices. ▪ The types of material appropriate for mechanical exploitation may range from improvised threats (e.g., IEDs, unmanned aircraft systems, mines) to state-of-the-art weapons systems. The mechanical components and devices of interest could include switches, relays and other similar devices. ▪ Mechanical exploitation specialists examine and assess component actuation, configuration, and the required forces/inputs for the device to function. Specialists also reconstruct and reverse engineer the mechanical components of the device and assess their potential connection and functional relation to similar devices.	▪ Mechanical exploitation results can contribute to understanding the operation, employment and configuration of the device, as well as its potential vulnerabilities. ▪ Mechanical exploitation can support counter-intelligence, counter-facilitation, and FP operations. Specialists may be able to determine the origin of the material and the manufacturing methods used to build them.

Trace material examination	▪ Trace material examination is the analysis of any additional types of materials recovered at a collection site such as hairs, fibers, cordage, fabric, powder, paint, glass, pollen, soil or other residues. ▪ Trace material specialists detect, collect, process and analyse collected material and items in order to establish associations between objects, individuals or locations.	▪ The results derived from trace material exploitation can provide valuable device-manufacturing location linkage information for use in analysing threat networks and supply chains. Trace material analysis can also contribute to device attribution.
Voice recognition	▪ Voice recognition is a method of biometric identification and authentication. Voice recognition is useful for the identification or linking of individuals, whose speech has been captured on sound recordings using analogue or digital recording devices. ▪ Voice technology works by digitizing a profile of an individual's speech to produce a stored model voiceprint or template. Biometric technology reduces each spoken word to segments. Each segment has several tones that can be captured in a digital format. The tones collectively identify the speaker's unique voiceprint. ▪ Voiceprints are stored in databases in a manner similar to the storing of fingerprints or other biometric data.	▪ Voice recognition and identification technologies can be used to verify a person's claimed identity against voice enrollments or to link a particular voice as having come from the same individual. It is often used where voice is the only available biometric identifier, such as over the telephone.
Weapon system exploitation	▪ Weapon systems exploitation is any activity that includes the technical analysis, testing, evaluation and documentation of the characteristics of weapon systems or subsystems; the capabilities and vulnerabilities; and the evaluation of operational performance against other systems and countermeasures. ▪ Weapon systems include, but are not limited to: rifles, tanks, aircraft, vessels, computer networks, space networks, rockets, missiles, mines, armored vehicles, and munitions as well as the components of the materiel such communication systems, signaling or control systems, information technology materiel and cryptographic components of any kind. ▪ In addition to the TE of weapon systems that are obtained intact or seized in a near-peer conflict, post-strike TE can also provide vital information regarding the technical characteristics and vulnerabilities of a particular weapon system.	▪ Weapon systems exploitation results can shape and influence strategy and guidance at all command levels. ▪ The information and intelligence gained from the TE of weapon systems are primarily used to: prevent technological surprise; assess scientific and technical capabilities; identify vulnerabilities and component sourcing; and develop countermeasures that are designed to neutralize an adversary's technological advantage.

Figure 10: Technical Exploitation Capabilities

INTENTIONALLY BLANK

ANNEX D THE LEVELS OF TECHNICAL EXPLOITATION IN COMPARISON

D.1. The table below compares each level of technical exploitation (TE) relative to a set of criteria.

CRITERIA	LEVEL 1 TE	LEVEL 2 TE	LEVEL 3 TE
Processing time from point of collection	- Minutes-to-hours	- Hours-to-days	- Hours-to-months
Exploitation time upon receipt at the TE site or facility	- Minutes-to-hours	- Minutes-to-days	- Days-to-months
Supported functions and activities	- Force protection - Targeting	- Force protection - Targeting - Component and materiel sourcing - Support to prosecution//criminal investigations	- Force protection - Targeting - Component and materiel sourcing - Judicial proceedings - Law enforcement activities - Signature and observables - Research, development, testing and evaluation
Environment	- On-site non-permissive or permissive	- In-theatre semi-permissive or permissive; or as reach back out-of-theatre permissive	- Out-of-theatre permissive
Available expertise	- Basic/intermediate	- Intermediate/advanced	- National agencies - Academia
Command and control	- Operational control in the joint operations area (JOA)	- Operational control in or near the JOA	- National agencies outside The JOA
Volume of information processing	- High tempo collection - Low volume processing	- Low tempo collection - Intermediate volume processing	- Minimal tempo collection - Flexible, high volume processing

Figure 11: Technical Exploitation Comparison Table.

INTENTIONALLY BLANK

ANNEX E TECHNICAL EXPLOITATION SCENARIOS

E.1. Anti-ship missile and associated radar technical exploitation.

During a NATO-led joint operation in a littoral area, signals intelligence identifies a new radar signature at an adversary coastal missile site. Imagery intelligence confirms that new equipment has recently been added to the site. In an effort to determine how to defeat the new radar and to determine what other changes have been incorporated into the site, the combined joint task force tasks the combined joint special operations task force (CJSOTF) to conduct a raid. The CJSOTF raiding force includes radar and missile specialists to identify and collect critical material for exploitation.

While securing the site, the troops use non-destructive means, including non-lethal weapons, to secure the radar and missile equipment to ensure that it cannot be tampered with or destroyed. Technical exploitation (TE) begins at once, searching and mapping the entire site, photographing the equipment to show how it was emplaced and recovering all documents and media. Biometric data is collected from the captured adversary soldiers. They are quickly questioned to confirm the location of the new components and to identify their leaders and those most knowledgeable about the new systems. The specialists on the team identify and remove critical radar and missile parts for further detailed exploitation.

Once the raiding force is extracted, the seized material is handed over to an in-theatre, multi-function laboratory to facilitate TE by a wider range of experts. The in-theatre laboratory collects fingerprints from the radar and missile components and then prepares the components and the related documents for transport to the national laboratories of two NATO nations. One laboratory specializes in anti-ship missiles and the other in radars. The other seized material, such as cell phones, are kept in-theatre for further TE. Information regarding the missile that was gathered from the captured soldiers is forwarded to a national-level missile laboratory.

During the examination of the internal radar components at the other national laboratory, a set of fingerprints is identified as belonging to one of the captured soldiers, who had not been connected to the radar. This information is shared with the other national and the in-theatre laboratories. The biometric data eventually leads to the identification of the radar specialist’s cell phone. Eventually it is determined the new missiles and radars were provided by a third country in contravention of a United Nations embargo, which, in turn, leads to the interdiction of additional new missiles and radars by NATO warships.

E.2. Technical exploitation of an improvised explosive device.

At 1800, a motorized patrol departs a NATO main operating base and travels along a route toward another operating base. Engineers have previously cleared mines and improvised explosive devices (IEDs) on the route from the main operating base to release point (RP) ALPHA. The route from RP A to the destination has not been swept for mines/IEDs. Leading the patrol are two armored personnel carriers (APCs), with the patrol commander occupying the second APC. The rest of the patrol consists of 23 trucks, one medical squad and two light armored vehicles in the rear.

At 1930 hours, the patrol passes a few houses and a small creek. The first APC passes the creek, but when the second APC passes the creek there is a large explosion. The second APC is hit by a large IED. The commander is severely wounded but is able to call and request immediate support from explosive ordnance disposal (EOD) units, the military police, medics, engineers and recovery units.

The task force (TF) overseeing this operational area assigns a mission manager (MM), an EOD team and a field exploitation team (FET) to the incident. In cooperation with the unit and military police, the MM directs the EOD team to perform render safe procedures on-site for other possible IEDs and APC secondary munitions. The EOD team determines the site is safe and then contacts the MM and advises it is safe for the FET to conduct TE activities. The APC and the attack site are then exploited by the EOD and FET teams.

Remnants of the IED are collected, along with the recovery of the APC. Both are relocated to a level 2 TE facility (TEF-2) for follow-on TE. Casualties are transported to the field hospital and treated. The deceased are officially declared dead at the field hospital and later transported back to the unit´s homeland where autopsies are performed.

Upon arrival at the level 1 TE site, the EOD and FET teams finalize their reporting and coordinate transfer and disposition of the collected material retrieved from the site for further TE and storage at a TEF-2. The military police collect statements from all involved personnel and coordinate their findings with EOD/FET and the TF chain of command. The collected exploitable material (CEM) from the incident is assigned to a TEF-2 case manager, who oversees the triage, processing, exploitation and dissemination of TE results to the TF. The immediate lessons identified are forwarded to tactical units to update route and threat layers.

At the TEF-2, subject matter experts (SMEs) are tasked to identify and lift latent prints from the IED remnants and enter their findings into the automated biometric identification system (ABIS). The ABIS data is made accessible to all allied/coalition partners supporting the TF, as well as TE specialists operating at a reachback level 3 TE facility (TEF-3). Meanwhile at the TEF-2, chemical analysis is performed on the possible homemade explosive (HME) substance to determine composition and identification of precursors to support counter-facilitation operations. The HME substance is found to contain ammonium nitrate and number 2 diesel fuel oil (ANFO), with a 94/6 mixture ratio. Electrical and mechanical exploitation are performed on the IED remnants which are assessed to be a victim-activated pressure plate IED. The

APC is transported to a TEF-3 that has the capabilities and expertise to perform a vulnerability analysis. Additionally, the HME substance is forwarded to the TEF-3 for further analysis and confirmation as ANFO. The biometric and chemical reports are consolidated into a TEF-2 report and uploaded into a networked, information management system and disseminated accordingly to the TF.

Personnel at the TEF-3 receive and triage the CEM, including the damaged APC. Biometric characteristics exploitation specialists review the ABIS data/reports and perform link and network analysis to search for potential print matches and to validate data findings. Further chemical analysis of the HME substance confirmed the TEF-2's assessment as ANFO. Additional TE, via X-ray diffraction and chemical synthesis, identified pre-cursor substances. These pre-cursor substances were then compared to other archived HME samples. Resultant findings show that the original HME substance used pre-cursor substances originating within the TF's area of responsibility.

Derived information is disseminated to the technical analysis cell for single-source/multi-type analysis and generation of a technical analysis report that will be fused with all-source intelligence in support of counter-facilitation strategies and targeting. TEF-3 SMEs specializing in engineering exploitation and weapons effects vulnerability analysis, examined the APC, assessing combat damage effects to interior and exterior structural components. Resultant data were uploaded into a modeling database, containing like or similar APC vehicles, in order to ascertain and determine vulnerabilities. The information gleaned from this engineering and weapons effects exploitation, coupled with autopsy results, is sent to the technical analysis center for single-source/multi-type analysis. The resultant report was then fused with all-source intelligence and translated into standing requirements to support future APC force protection upgrades and development of countermeasures against improvised threats.

A few weeks later, NATO patrols encountered the perpetrators and identified them based on data from the biometric watch list delivered from the TEF-3. Persons who supplied the electronic components and raw materials for the IED were arrested four months later on charges of terrorism. One perpetrator was identified and arrested when he applied for asylum in Europe.

E.3. Technical exploitation of an aircraft crash site.

An aircraft, from an adversarial country, crosses into Allied airspace and crash-lands inside the NATO joint operations area. An on-scene commander (OSC) is assigned by the combined joint task force (CJTF) commander to oversee the crash site investigation. The OSC immediately sends out a multi-function team (MFT) consisting of security personnel, an explosive ordnance disposal (EOD) unit, and first responders via air-lift to the crash site. Airborne intelligence, surveillance and reconnaissance (ISR) collection is conducted over the crash site while the MFT is in transit.

Upon arrival at the crash site, the EOD and security teams confirm the pilot is alive and injured, but able to communicate. The pilot states that he wants to defect and requests political asylum. The EOD team performs an initial reconnaissance of the crash site and determines there are no imminent hazards present. The EOD team leader calls in first responders to remove the pilot and perform first aid, while the security team provides force protection (FP). Following render safe procedures for the live munitions and hazardous areas of the aircraft (e.g., fuel and ejection systems), the EOD team leader informs the OSC that the crash site is rendered safe for further investigation.

The EOD team initiates incidence reporting and level 1/field exploitation of the first-seen ordnance. They identify four radar-seeking air-to-air missiles and six precision guided munitions (PGMs). Other than standard adversary markings, they note that the air-to-air missiles have no unique visible characteristics when compared to existing adversary inventory. The six PGMs are assessed to be 250lb class conventional weapons and appear to have new/or modified guidance kits (nose and tail) and fuze enhancements. Markings on the guidance kits and fuzes indicate they could have originated from another foreign adversary. Via satellite communications (SATCOM), the EOD team leader contacts an out-of-theatre facility, specializing in research, development, and engineering of ordnance and warheads, to discuss initial findings. The reachback facility confirms the EOD team's assessment and provides additional guidance on collection and triage of the PGMs and air-to-air missiles.

While the OSC inspects the crash site and communicates their initial report to the respective command post, the EOD team records and collates their initial findings into respective EOD reporting formats (explosive ordnance (EO) 100-400 reports). In addition, previous airborne ISR full motion video, coupled with on-scene SPOT reports issued by the security team, indicate the crash site area is safe from potential hostile threats.

The OSC transmits the reports to the level 1 TE commander. The commander reviews and forwards the reports to the nearest level 2 TE facility (TEF-2), the combined joint captured materiel exploitation centre (CJCMEC) and the CJTF commander, recommending immediate TE support, given the significant intelligence to be gained from the 5th generation aircraft, ordnance, and the captured pilot. CJTF concurs and directs the operations staff (CJ3) and intelligence staff (CJ2) to coordinate and provide TE support of the crash site, as well as initiate coordination with out-of-theatre level 3 TE facilities (TEF-3s)t. CJ3 notifies TF1 (Task Force 1) to provide TE support and to coordinate with CJ2.

Upon arrival at the crash site, the TE team, in coordination with the MFT, continues level 1 TE support at the crash site, performing visual observations/recordings and closer inspection of visible aircraft components. A preliminary technical report is generated, confirming it is a 5th generation aircraft that closely resembles existing adversary order of battle inventory. However, the TE team discovers a small protrusion emanating from the rear tail section and they note that the entire aircraft has an opaque coating. Via SATCOM, the TE team coordinates with an out-of-theatre facility that specializes in the exploitation of 5th generation aircraft, and informs them of their preliminary findings. The reachback facility confirms that the two key findings from the TE team are new for this aircraft, with no supporting intelligence. They recommend removing the protrusion from the tail section and extracting samples of the opaque coating for further exploitation. The protrusion is removed and samples of the opaque coating are taken from various areas of the aircraft.

Meanwhile, the EOD team triages the four air-to-air missiles and six PGMs. Initial findings are translated into complimentary technical reports type "A" and "B," which are transmitted to the TEF-2, CJCMEC and respective level TEF-3s. The CJCMEC forwards these reports to the CJ2, who in turn, relays it to TF1 and the CJTF commander and staff. Logistics and security support arrive at the crash site to provide transportation of the collected material and FP, while in transit to the nearest in-theatre TEF-2.

Using a NATO-approved information management system (IMS), the TEF-2 case manager initiates level 2 TE by creating a new case file for exploitation of the 5th generation aircraft and its rendered-safe ordnance. Reports from level 1 TE activities are uploaded to the case file to highlight initial/significant findings and provide background and context for the level 2 subject matter experts (SMEs). The TE SMEs are alerted by the IMS of the new case file and priority exploitation requirements.

As aircraft components and the rendered-safe ordnance are brought into the TEF-2, triage and chain of custody procedures are performed and the material is assigned to appropriate SMEs. Per CJ2, in coordination with the CJCMEC and TEF-2, the protrusion from the tail section, the coating samples, and the PGMs have priority exploitation over all other collected material.

Electronic exploitation (EE) and weapon system exploitation (WSE) SMEs, whom specialize in aircraft and air defense capabilities, assess that the protrusion appears to be a highly advanced electronic countermeasure (ECM) capability. Examination of the internal components reveal complex and highly modern circuitry designed to defeat modern radar-guided air-to-air missiles. The protrusion's relatively small size and configuration indicate its power source for jamming is likely provided internally by the aircraft, which may limit the ECM's effective range and duration and affect aircraft performance. The EE and WSE SMEs coordinate with TEF-3 SMEs to discuss findings. Resultant analysis and information by the EE and WSE SMEs are entered into the IMS and recommendations are made to expedite chain-of-custody transfer of the protrusion to a TEF-3 for further TE and assessment of both, aircraft and ECM limitations/capabilities.

Meanwhile, the opaque coating samples are assigned to a chemical SME. The chemical exploitation SME determines that the coating contains chemical properties and crystalline structures that closely match existing radiation-absorbent material (RAM). RAM is used to improve aircraft stealth capabilities when exposed to radio frequency emissions. The chemical exploitation SME, in turn, notifies the TEF-3 of these initial findings and requests further analysis to confirm the chemical characterization and determine RAM effectiveness. The TEF-2 TE report sent from chemical SME is uploaded into the IMS.

At the TEF-2, the case manager assigns the PGMs to a team of mechanical, EOD and chemical experts. Mechanical assessment of the guidance kits indicates improved weapon standoff range and delivery accuracy. EOD and mechanical exploitation of the fuze points to void-sensing capabilities, indicating a munition penetration and effectiveness against multi-story facilities. Additionally, precise construction and use of quality alloy materials suggest high fuze functioning reliability and low void-sensing error rates. Finally, EOD and chemical exploitation of the warhead construction and explosive material indicates a very high-strength, steel alloy casing, coupled with a high density and more energetic explosive. Preliminary results for both suggest a nickel-cobalt steel alloy composition for the casing and containing a polymer bonded explosive (PBX). The level 2 team of experts deems it necessary to transfer the PGMs to a TEF-3 to confirm their findings. Level 2 analysis and reporting (EO 500) are uploaded in the IMS.

As level 1 TE and TEF-2 TE reports are produced, they are forwarded to human intelligence (HUMINT) and counterintelligence officials to aid their interviews with the pilot. Information and analysis gleaned from the pilot interviews are forwarded to the TEF-2 and CJTF commander and staff. Additionally, they are coordinated with respective level 3 facilities to help ascertain and confirm aircraft and munitions limitations and capabilities. In accordance with established MOAs and classification guidance, the resultant information and intelligence (HUMINT, counterintelligence) obtained from the pilot interviews are disseminated across the NATO force for situational awareness and fusion by all-source intelligence analysts.

Following level 2 TE of the priority materiel (ECM capability, opaque coating samples, and PGMs), the TEF-2 notifies the CJCMEC and CJ2 that the priority materiel is ready for transport to TEF-3s. CJ2 informs CJTF commander/staff and recommends priority materiel transfer to TEF-3s. CJTF commander concurs and directs the logistics staff to coordinate and expedite materiel transfer from the TEF-2. Simultaneously, CJTF informs the host nation (HN) of this planned action and references standing agreements for foreign materiel transfer, return, and storage.

TEF-3 personnel receive the priority materiel and the SMEs are assigned accordingly. An ECM capability is confirmed and evaluated against existing ECM systems. ECM analysis and raw data are compiled by the SMEs and subsequently fused by intelligence analysts into finished intelligence products. Level 3 analysis and findings of the opaque coating samples confirm presence of RAM and indicate RAM effectiveness equal to, and in some cases, less than, current 5th generation aircraft. Level 3 exploitation of the PGMs confirms improved standoff and penetration performance, delivery accuracy, and lethality. Warhead casing analysis yields a nickel-

cobalt steel alloy, while explosive analysis confirms high density, PBX material. Analysis of the fuze confirms void-sensing capability, however, further testing reveals high fuze functioning error rates, thus, degrading fuze reliability and overall weapon reliability. Analysis of guidance kits confirms improved standoff range and delivery accuracy, as well as a limited, terminal area modeling capability. In accordance with NATO classification guidance, these TEF-3 results are disseminated to appropriate NATO stakeholders and the CJTF.

In compliance with NATO and HN agreements, the materiel is returned and stored at a HN-specified facility. CJTF directs CJ2 to integrate all level 1, 2, and 3 information and intelligence reports into a technical intelligence study. This study includes all HUMINT and counterintelligence reporting associated with the pilot. Lessons-learned and recommendations with respect to TE activities are also captured. Finally, the study is shared across NATO and partner nations.

INTENTIONALLY BLANK

.

Lexicon

Part 1 - Acronyms and abbreviations

ABIS	automated biometric identification system
AEP	allied engineering publication
AIntP	allied intelligence publication
AJP	allied joint publication
ANFO	ammonium nitrate-fuel oil
APC	armored personnel carrier
BEI	biometric-enabled intelligence
C2	command and control
CBRN	chemical, biological, radiological and nuclear
CCIR	commander’s critical information requirement
CEM	collected exploitable material
CIS	communications and information system
CJ1	combined joint staff for personnel and administration
CJ2	combined joint staff for intelligence
CJ3	combined joint staff for operations
CJ4	combined joint staff for logistics
CJ6	combined joint staff for communications and information
CJ-CBRND-TF	combined joint chemical, biological, radiological and nuclear defence task force
CJCMEC	combined joint captured materiel exploitation centre
CJTF	combined joint task force
CJSOTF	combined joint special operations task force
COMTECHREP	complimentary technical report
CR	collection requirement
DNA	deoxyribonucleic acid
DOMEX	document and media exploitation
ECM	electronic countermeasure
EE	electronic exploitation
EO	explosive ordnance
EOD	explosive ordnance disposal
FET	field exploitation team
FP	force protection
HME	homemade explosive
HN	host nation
HQ	headquarters
HUMINT	human intelligence
ICP	intelligence collection plan
IED	improvised explosive device
IMS	information management system

ISO	International Organization for Standardization
JIPOE	joint intelligence preparation of the operating environment
JISR	joint intelligence, surveillance and reconnaissance
JOA	joint operations area
MASINT	measurement and signatures intelligence
MFT	multi-function team
MM	mission management
MOA	memorandum of agreement
MOE	measure of effectiveness
MOP	measure of performance
NAI	named area of interest
NATO	North Atlantic Treaty Organization
OE	operating environment
OPLAN	operations plan
OSC	on-scene commander
PBX	polymer bonded explosive
PGM	precision guided munition
PIR	priority intelligence requirement
PRETECHREP	preliminary technical report
RAM	radiation-absorbent material
RDT&E	research, development, testing and evaluation
ROE	rules of engagement
RP	release point
RSP	render safe procedures
SATCOM	satellite communications
SME	subject matter expert
SOF	special operations forces
SP	stability policing
TACON	tactical control
TCN	troop contributing nation
TCPED	task, collect, process, exploit and disseminate
TE	technical exploitation
TECHINT	technical intelligence
TEF	technical exploitation facility

TF	task force
TTP	tactics, techniques and procedures
WSE	weapon system exploitation

Lexicon

Part 2 - Terms and definitions

exploitation
Taking full advantage of any information that has come to hand for tactical or strategic purposes.
(NATO Agreed)

information requirement
In intelligence usage, information regarding an adversary or potentially hostile actors and other relevant aspects of the operational environment that needs to be collected and processed to meet the intelligence requirements of a commander.
(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
An integrated intelligence and operations set of capabilities, which synchronises and integrates the planning and operations of all collection capabilities with the processing, exploitation, and dissemination of the resulting information in direct support of the planning, preparation, and execution of operations.
(NATO Agreed)

joint operations area
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)

material
The physical substance, elements or constituents of which something is composed of or can be made.

(Oxford English Dictionary)

materiel
The items used to equip, maintain and support military forces in their activities.
Notes: Materiel includes software, but excludes real estate, installations and utilities.
(NATO Agreed)

operating environment
A composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander.
(NATO Agreed)

rules of engagement
Directives to military forces, including individuals, that define the circumstances, conditions, degree, and manner in which force, or actions which might be construed as provocative, may be applied.
(NATO Agreed)

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

technical exploitation
A process using scientific methods and tools to derive data and information of potential intelligence or operational value from collected data, information, materiel and materials.
(This term and definition only applies to this publication)

technical intelligence
Intelligence concerning foreign technological developments, and the performance and operational capabilities of foreign materiel, which have or may eventually have a practical application for military purposes.
(NATO Agreed)

AIntP-10(B)(1)