NATO UNCLASSIFIED
Releasable to Australia and Sweden

29 April 2022

DOCUMENT
AC/343-D(2022)0001

NATO TECHNICAL EXPLOITATION GROUP (NTEG)

MARTIAL VISION 2021 Technical Exploitation Seminar Lessons Identified Report

Note by the Co-Chairs

1. Please find attached the MARTIAL VISION 2021 Technical Exploitation Seminar Lessons Identified Report.

2. This report represents a year's worth of concentrated study and analysis of existing NATO doctrine by the Alliances' foremost experts in the NATO Technical Exploitation Group, reinforced by Allied and Partner real-world experience of technical exploitation in operations and exercises.

3. Relevant communities across the Alliance are encouraged to consider the findings in this report to support the further develop and operation of the technical exploitation capability.

(Signed) Mr. Gabriele Cascone
Head, Counter-Terrorism Section
IS ESC

(Signed) COL Jose Vieira
Intelligence Capability Development
Strategy & Policy Unit/JISD

1 Annex

Action Officer: S. Henze
Original: English

ANNEX 1
AC/343-D(2022)0001

MARTIAL VISION 2021
Technical Exploitation Seminar
Lessons Identified Report

ANNEX 1
AC/343-D(2022)0001

TABLE OF CONTENTS

1 MARTIAL VISION 2021 TECHNICAL EXPLOITATION SEMINAR

1.1 BACKGROUND

MARTIAL VISION is a Flagship Activity conducted under Serial 2.4 of the NATO Technical Exploitation Group (NTEG) Technical Exploitation (TE) Programme of Work. MARTIAL VISION (MV) aims to identify and pursue opportunities for testing and/or validating concepts, doctrine and operational standards in NATO and/or national exercises and experimentation.[1] MV 2021-22 consists of a TE Seminar, which was held 13-14 December 2021, and a TE Experiment, which is to be held 13-17 June 2022.

The purpose of the MV 2021 Seminar is to promote a common understanding of TE focussing on the latest version of the Allied Intelligence Publication on Technical Exploitation (AIntP-10)[2], especially regarding command and control of TE operations and management of TE results, including Collected Exploitable Material (CEM) Collected and associated information flow[3] .

The follow-on MV 2022 Experiment assesses those TE concepts described at AIntP-10 and these lessons identified through the MV 2021 Seminar. This will be accomplished through practical application of scenarios and vignettes designed to highlight the diversity of applications of TE capabilities: Counter Unmanned Aircraft System (C-UAS), Maritime Interdiction Operations (MIO), Counter Improvised Explosive Device (C-IED), Chemical, Biological, Radiological, Nuclear Defence (CBRN)) and of their supported operational outcomes.

Together, the TE Seminar and TE Experiment aim to fill a gap in NATO's, and most Allies', approach to TE which has been heretofore almost exclusively focused on developing individual tactical capabilities and specific sub-capabilities within TE, such as Weapons Intelligence Teams (WIT) or Document and Media Exploitation (DOMEX) capabilities, rather than on the overall organization and management of such capabilities. MV intends to support the planning, preparation, execution and exploitation of results from TE capabilities deployed *together* by nations in a NATO or other coalition operation.

1.1.1 MARTIAL VISION 2021 TE Seminar Objectives and Scope

The objective of the MV TE 2021 seminar was to examine the TE framework and concepts presented in AIntP-10 and compare this doctrinal approach with the real-world experience of nations and NATO bodies. In doing so, the TE Seminar provided a better understanding of TE and activities undertaken

[1] PO(2020)0316 Practical Framework for Technical Exploitation, 15 October 2021 NATO UNCLASSIFIED

[2] Allied Intelligence Publication AIntP-10, Technical Exploitation, NSO, Edition B, Version 1, May 2021, NATO UNCLASSIFIED
[3] AC/343-DS(2021)0002 NATO Technical Exploitation Group, Report and Decision Sheet, June 2021, NATO UNCLASSIFIED

by practitioners in the field as well as the issues encountered. In particular, new concepts introduced in AIntP-10 regarding the command and control of TE in operations and the management of TE results were examined and clarified.

The TE Seminar was held at the San Marcial Spanish Army Division Headquarters, in Burgos Spain, 13-14 December 2021. The TE Seminar was conducted as a scholarly examination of TE as presented in AIntP-10 and reinforced by examples from practical experience. A number of panel members presented these experiences from a national and NATO perspective, which enabled discussion on specific topics associated with TE. These topics, included as seminar learning objectives, were:

- The NATO Technical Exploitation framework
- Combined Joint Task Force (CJTF) Staff Responsibilities for TE
- Level 2 Technical Exploitation Facility (TEF-2) – Capabilities, Operations and Management
- Technical Exploitation Laboratory – Level 2
- TE Collection
- Collected Exploitable Material (CEM) Flow
- Managing TE Results

1.2 LESSONS IDENTIFIED

Three persons were identified to support the development of the lessons identified for the TE Seminar. This involved extensive note taking during the various panel discussions as well as co-ordination amongst the note takers during and shortly after the seminar. This report was subsequently reviewed by the members of the NTEG's MV Tiger Team.

Although the Seminar topics discussed above were planned in terms of the learning objectives for the Seminar, the discussion during the Seminar covered a number of other overlapping topics and thus the lessons identified have been grouped in-terms of the key themes that arose during the Seminar rather than following the Seminar organization itself. These key themes are as follows:

- Technical Exploitation as a Single Source ISR Capability
- Command Joint Intelligence Staff (CJ2) vs Command Joint Operations Staff (CJ3) TE Tasking
- TEF-2 Provides Command and Control (C2) of Technical Exploitation in Support of Operations and Intelligence
- Collect Only vs Collect & Exploit Roles
- Levels of Technical Exploitation and the Processing, Exploitation and Dissemination (PED)
- Non-linear CEM flow

- Managing TE Results
- Technical Exploitation Conducted in Support of Intelligence vs Evidence-Based Operations

The rest of this report provides the lessons identified in the 2021 Martial Vision Technical Exploitation Seminar. The material presented in this report, including figures, were recorded as part of the discussions during the Seminar or were developed during its preparation. This report represents the views of the various participants of the 2021 MV Seminar and should not be considered as official NATO doctrine.

2 TECHNICAL EXPLOITATION SEMINAR LESSONS IDENTIFIED

2.1 TECHNICAL EXPLOITATION AS A SINGLE SOURCE ISR CAPABILITY

2.1.1 MV TE Seminar Learning Objectives

Addressed during the TE Framework seminar learning objective session.

2.1.2 AIntP-10 references

TE is discussed as part of the Joint Intelligence, Surveillance and Reconnaissance (JISR) cycle/process in the following areas of AIntP-10:

- Section 1.1, paragraph 5, item a, b & c
- Section 1.2, paragraph 3 & 4
- Section 1.3, paragraph
- Section 2.3.2, paragraph 3, item b.

2.1.3 Observations

NATO doctrine clearly places TE under JISR in the intelligence doctrine hierarchy. While this link is established in AINTP-10, it remains an underdeveloped concept in NATO doctrine. TE, or Technical Exploitation Intelligence (TEXINT), is not a recognized NATO intelligence collection discipline nor is TE's contribution of information into the JISR process clearly recognized or developed in NATO's intelligence doctrine. The legacy view that "TE is C-IED" remains pervasive. The TE Seminar demonstrated that this legacy view is changing more rapidly in nations than in NATO – approximately 50% of Seminar participants were from J2-related organizations.

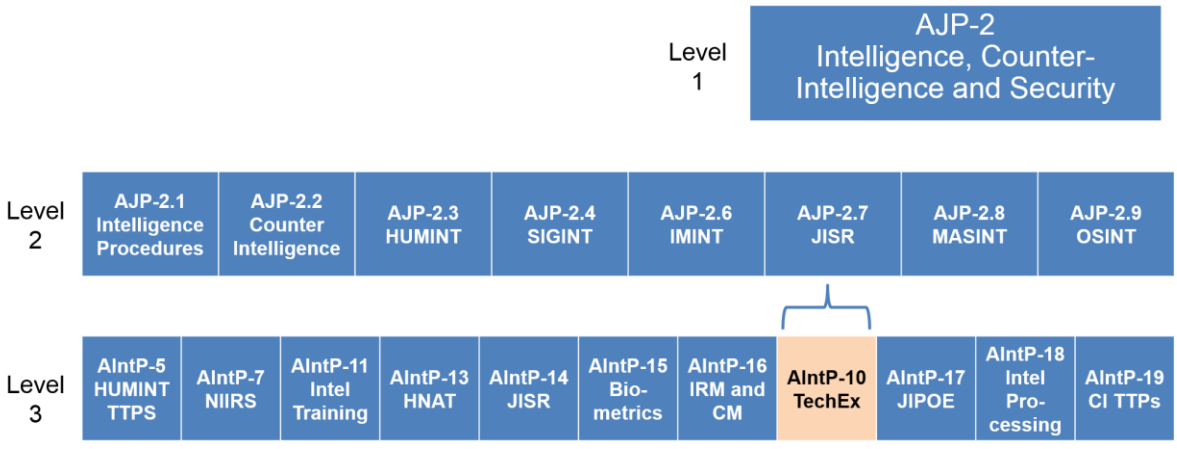

Figure 1 Technical Exploitation in the NATO intelligence doctrine hierarchy.

While the position of TE in JISR in NATO doctrine is not well developed, the Netherlands provided the Seminar with a much more developed view, and practical application, of TE as a multi-type, single source "sensor" capability within the intelligence cycle. Responding to a commander's information requirements, in the Dutch conception, TE will be tasked just like other sensors or Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) capabilities such as Unmanned Aircraft Systems (UAS) collecting imagery intelligence (IMINT) or troops collecting Human Intelligence (HUMINT). Recognizing that TE also includes a lot of "incidental", or non-tasked, collection, the TE process runs in parallel to the JISR process and needs to have an internal analysis capability to fuse TE results from multiple sub-capabilities or "types" (Chemical Exploitation [CHEMEX], electronic exploitation [ELEX], etc.) into a single-source product (TEXINT) for ingestion into the Intel cycle. The final step of the TE process disseminates TE results into the all source intelligence cell where TE results will be fused with information from other intelligence sources.

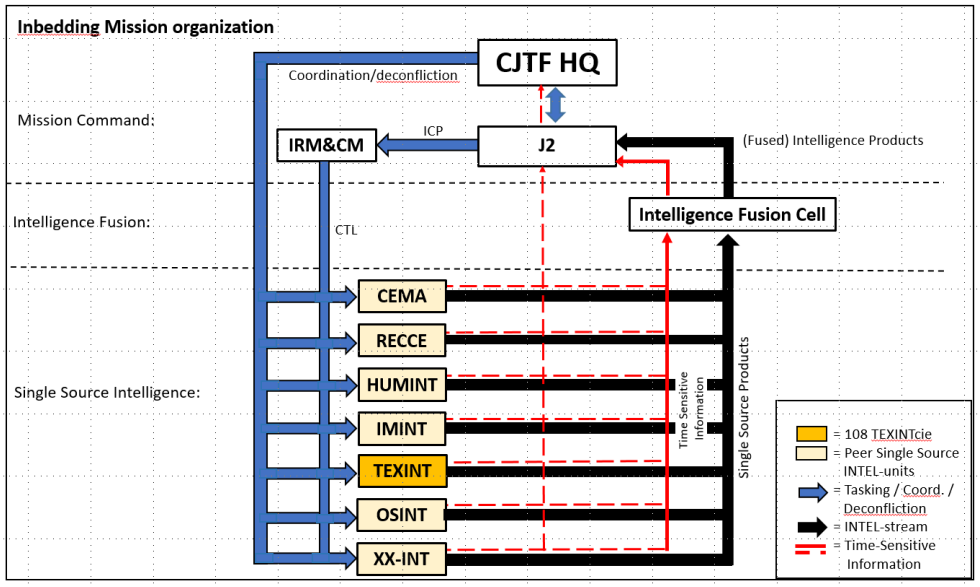

Figure 2 The Dutch concept of TE as a multi-type, single source sensor in the JISR system.

However, a key feature of TE that distinguishes it from the classic intelligence collection disciplines is that TE will typically disseminate to a wider array of "customers", not just Intel. These customers include operations, training, counter-measure development, Research, Development, Test & Evaluation (RDT&E) and, potentially, civilian law enforcement. There may even be cases of time sensitive information, such as technical information about an overmatching enemy capability, which needs to be assessed and disseminated immediately without passing through the all source intelligence fusion cell.

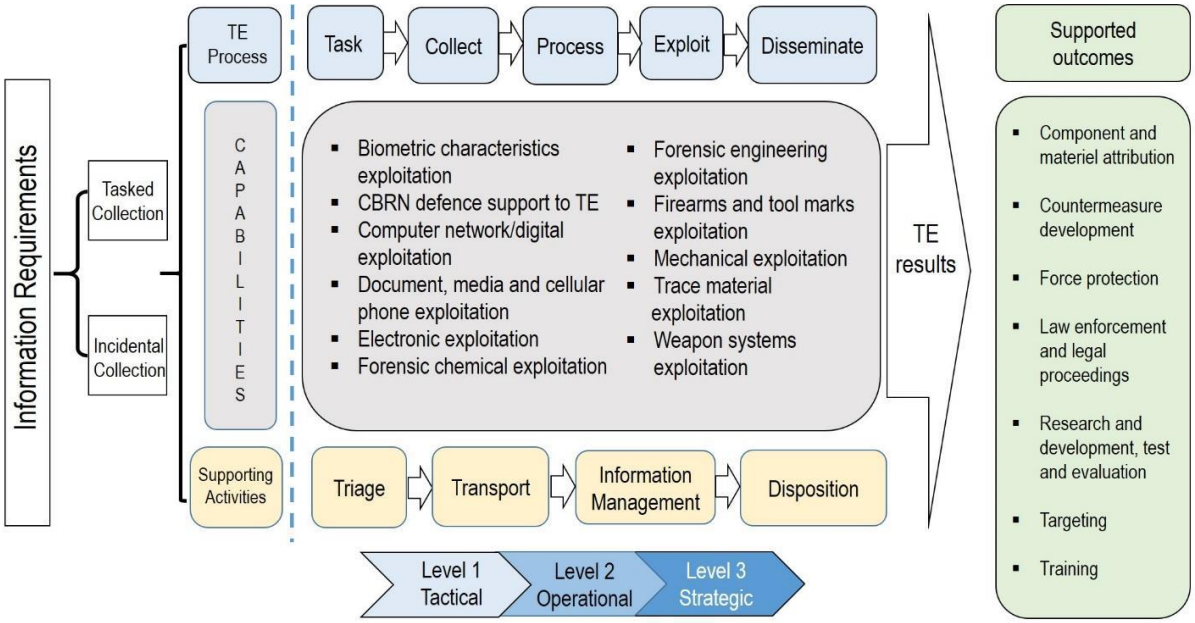

Figure 3 This presentation of TE as a multi-type, single source ISR capability is very useful to inform further integration of TE into the overall intelligence architecture.

2.1.4 Conclusions

AINTP-10 presents TE as capable of responding to JISR collection requirements and the Netherlands is implementing TE according to a practical vision of that concept. This view represents the future of TE, yet much work remains to integrate TE into JISR while preserving TE's role in supporting outcomes beyond intelligence.

2.1.5 Recommendations

2.1.5.1 NATO doctrine

- Further develop the concept of TE as a multi-type single source sensor within the JISR process[4] and its implications on tasking/reporting of TE results into the Intelligence Cycle[5] .
- Review related intelligence doctrine to ensure integration and harmonization of TE with other intelligence sources.

2.1.5.2 Experimenting and exercising TE concepts

- Experiment and exercise TE as a JISR single source capability.

[4] Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance, NSO, Edition A, Version 1, July 2016, NATO UNCLASSIFIED
[5] Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security, NSO, Edition B, Version 1, July 2020, NATO UNCLASSIFIED

2.2 CJ2 VS CJ3 TE TASKING

2.2.1 MV TE Seminar Learning Objectives

Addressed during the CJTF Staff Responsibility for TE seminar learning objective session.

2.2.2 AIntP-10 references

Referenced in AIntP-10 explanation of TE-related CJ2 and CJ3 staff roles and responsibilities in chapter 3.

2.2.3 Observations

AIntP-10 establishes that CJ2 is the joint staff lead for TE. However, it is difficult to plan for TE in the intelligence collection plan (ICP) if there is a lack of awareness and understanding of the TE capabilities that are available and how they can support response to the commander's Information Requirements (IR). It is important to leverage Joint Intelligence Preparation of the Operational Environment (JIPOE) and JISR information when planning for TE. For TE to be effective, there needs to be good co-ordination between CJ2 and CJ3 as CJ3 is the joint staff lead for operations, which includes tasking. TE gaps need to be identified, including those that can and cannot be addressed by TE. Currently, NATO doctrine for TE is a little confusing concerning the co-ordination between CJ2 and CJ3 for TE. To confuse matters more, there is almost no reference to TE in other NATO intelligence publications. There need to be clearer lines of delineation between CJ2 and CJ3 and better understanding of TE's relation with JISR.

AIntP-10 describes support for TE under Combined Joint Logistics Staff (CJ4) (logistics for transportation of CEM), Combined Joint Staff Communications and Information Systems Staff (CJ6) for computer and information systems (CIS) to manage TE results, which also includes releasability in-terms of classification, disclosure and security policies.

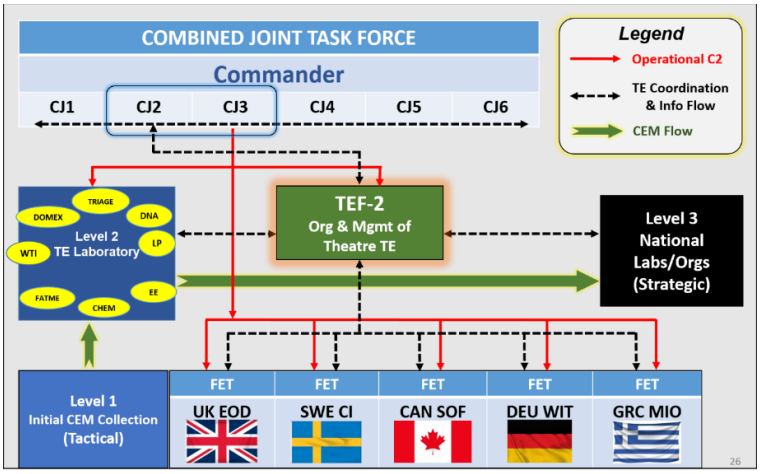

Figure 4 A visual representation of the relationship between the CJTF and subordinate elements of the TE system, noting the close relationship between CJ2 and CJ3.

The TE Seminar noted that AIntP-10 states that CJ3 informs CJ2 of the TE opportunities. However, in practice, this is normally the reverse, where CJ2 informs CJ3 of the TE opportunities in the concept of operations (CONOPS) for a theatre of operations, but it should be noted that this is not a one-way conversation, but more like a discussion. This recognition that there exists a variety of approaches was reinforced by national experiences related by panel members and audience participants.

Romania stated that they are tasked by CJ3 in-order to satisfy CJ2 requirements, but this will depend on the who has Operational Control (OPCON) or Tactical Control (TACON).

In the Netherlands' construct, there are two different situations. CJ2 tasks if TE is in the intelligence collection plan, while CJ3 tasks otherwise, to support outcomes such as force protection or as a reactive activity. The Netherlands has adapted their TE capabilities, previously focused on C-IED, to be integrated into ISTAR as a TE Company. This organization enables linkages throughout the TE chain and of course with JISR. C2-TE liaises with CJTF CJ2/3; a TE Quality Manger (QM) liaises with CJTF Legal Advisor (LEGAD); TE logistics and Material management co-ordinates with CJTF CJ4 and Base Commander. This fully integrated TE organization is a promising model for others, including for NATO, as it ensures effective coordination amongst all joint staff and especially CJ2/CJ3.

The United States' experience of operating multiple TE capabilities across a wide theatre of operations demonstrates that effective C2 of TE is required *at theatre level* in order to properly co-ordinate amongst the different stakeholders and capabilities. This is a pre-requisite to support the commander's situational awareness and understanding concerning TE and is a concept captured to a degree in AIntP-10 in the "TEF-2" concept that is the subject of the following section. US experience also highlights the need for adaptation of C2 relationships across the different phases of an operation or as priority IRs change. Everything needs to be co-ordinated at the CJ2/TEF-2 and C2 from CJ3.

The Netherlands, describing their experience in Mali, noted that higher commands need to understand what TE can provide and, equally importantly, what TE cannot provide, in order to manage expectations of TE capabilities and the time it takes to produce TE results. Higher commands are also responsible for providing the appropriate environment and security in which to conduct TE, which includes consideration of sustainability and legal constraints on what TE can and cannot as captured in Memorandums of Understanding (MOUs) elaborated at CJTF level.

2.2.4 Conclusions

CJ2 and CJ3 will co-ordinate the planning and tasking of TE capabilities, possibly through the TEF-2 (see next section). CJ3 will normally provide the tasking of the TE capability, assuming they have OPCON or TACON, while what is to be collected and by whom will be through the Collection Task List (CTL) and the TE management plan developed under CJ2 and the TEF-2. While different nations may have different ways of operating, what is essential is that these arrangements be decided during the planning phase of the operation so that C2 of TE is effective and efficient.

The consensus in the TE Seminar is that chapter 3 of AIntP-10 concerning tasking of TE capabilities is a little confusing and perhaps at times contradictory to what happens in practice.

2.2.5 Recommendations

2.2.5.1 Developing NATO doctrine

- Provide clarification on the planning, tasking and co-ordination between CJ2 and CJ3 for TE tasks and missions in AIntP-10. Such clarification may also need to be elaborated in other NATO Intelligence publications.
- Provide clarification on the tasking mechanism of TE for planned missions, including the links and associations between the Operation Plan (OPLAN), Fragmentary Order (FRAGO), CTL and TE management plan in AIntP-10. Such clarification may also need to be elaborated in other NATO Intelligence publications.

2.2.5.2 Experimenting and exercising TE concepts

- Exercise the co-ordination between CJ2 and CJ3 for planning TE operations and missions.

2.3 TEF-2 PROVIDES C2 OF TE IN SUPPORT OF OPERATIONS AND INTELLIGENCE

2.3.1 MV TE Seminar Learning Objectives

Addressed during the Level 2 TEF – Capabilities, Operations & Management seminar learning objective session.

2.3.2 AIntP-10 references

Discussed in AIntP-10 in the following areas of the document:

- Section 3.4
- Section 3.5

2.3.3 Observations

The Technical Exploitation Facility Level 2, or TEF-2 for short, is a concept introduced in Edition B of AIntP-10 that was not previously present in NATO doctrine. Its inclusion in Edition B reflects lessons that nations have collected from operations and the maturation of the TE capability as an increasingly important contributor of information to the commander.

AINTP-10's description of the TEF-2 is confusing. The Combined Joint Captured Materiel Exploitation Centre Components (CJCMEC), an American capability, is provided as "an example" of a TEF-2 and then often replaces TEF-2 thereafter in the text and figures. Many who have read AIntP-10 have been confused by the term CJCMEC used in doctrine. AINTP-10 seems to imply that a TEF-2 either is a Level 2 Laboratory or that the TEF-2 can conduct TE, but elsewhere implies the opposite. One graphic displays multiple "TEFs" without distinguishing them as "TEF-2s" or Level 2 Laboratories.

Due to this confusion, the TE Seminar planning team had to perform extensive analysis and present a “best interpretation” of what the TEF-2 “should be”. This interpretation was reinforced extensively by when national panel members in the TE Seminar related their experience from operations and exercises. What follows is that “best interpretation”.

Despite the initial confusion, what is clear is that the TEF-2 is an extremely important conceptual development that most TE Seminar participants recognized as essential to the effective use of TE capabilities in coalition operations. The TEF-2 organization and management function is especially important for coalition operations in which multiple countries are contributing individual capabilities to a larger coalition force, in other words, for NATO.

Despite the use of the term “facility” in its name, the Technical Exploitation Facility Level 2 (TEF-2) is not a laboratory or unit, but is most usefully conceived of as a *function* within a theatre of operations. The TEF-2’s primary responsibility is the organization and management of TE in the theatre. The TEF-2 is under the CJTF J2 in the chain of command and translates a commanders IR’s into TE collection requirements. While theatre TE capabilities will not likely be directly under TEF-2 command, all theatre TE capabilities should have communications with the TEF-2 and the TEF-2 should have operational awareness of all TE capabilities. Conversely, TE results (reporting and CEM) produced by Level 1 and Level 2 TE capabilities across a theatre should flow through the TEF-2 for onward dissemination. This two-way flow may be simply (perhaps over-simply) illustrated thus:

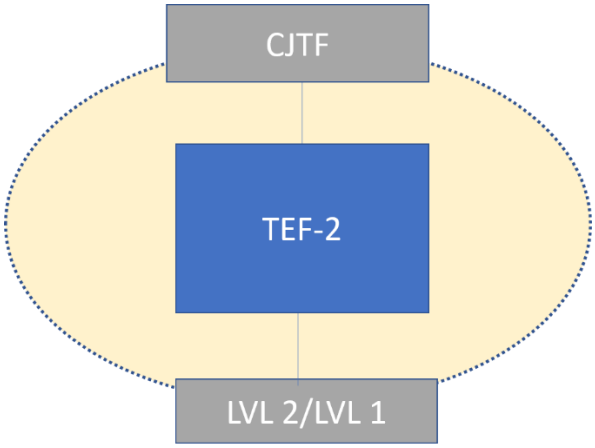

Figure 5 A simplified view of the TEF-2 flow of TE information between both upper and lower echelons

While not explicitly explained in AIntP-10, it is understood that the TEF-2 is “formed” rather than “deployed” and is a staff element rather than a TE “capability”. It may include multinational personnel, but may also be formed at a national level if the force structure is large enough. In a NATO operation,

it seems likely that the TEF-2 would be an element of the NATO operational command structure, formed as a “cell” or “task force” responsible for the organization and management of TE.

In the MV TE Seminar, a clear distinction was made between the TEF-2 and the Level 2 Laboratory. The latter is what many TE practitioners are familiar with: a container or tent based capability containing multiple TE “sub-capabilities”, “types” or “modalities” such as ELEX or CHEMEX. According to the TE Seminar’s presentation of AIntP-10, in a given theatre of operation there may be multiple Level 2 Laboratories; however it is likely optimal to have only a single TEF-2 in order to provide C2 for TE in that operation. The TE Seminar developed the following graphic to illustrate the relationship of the TEF-2 to the other elements in the TE operational framework. The graphic is illustrative, not definitive, and depicts a situation in which there is only a single Level 2 Laboratory that is not co-located with the TEF-2.

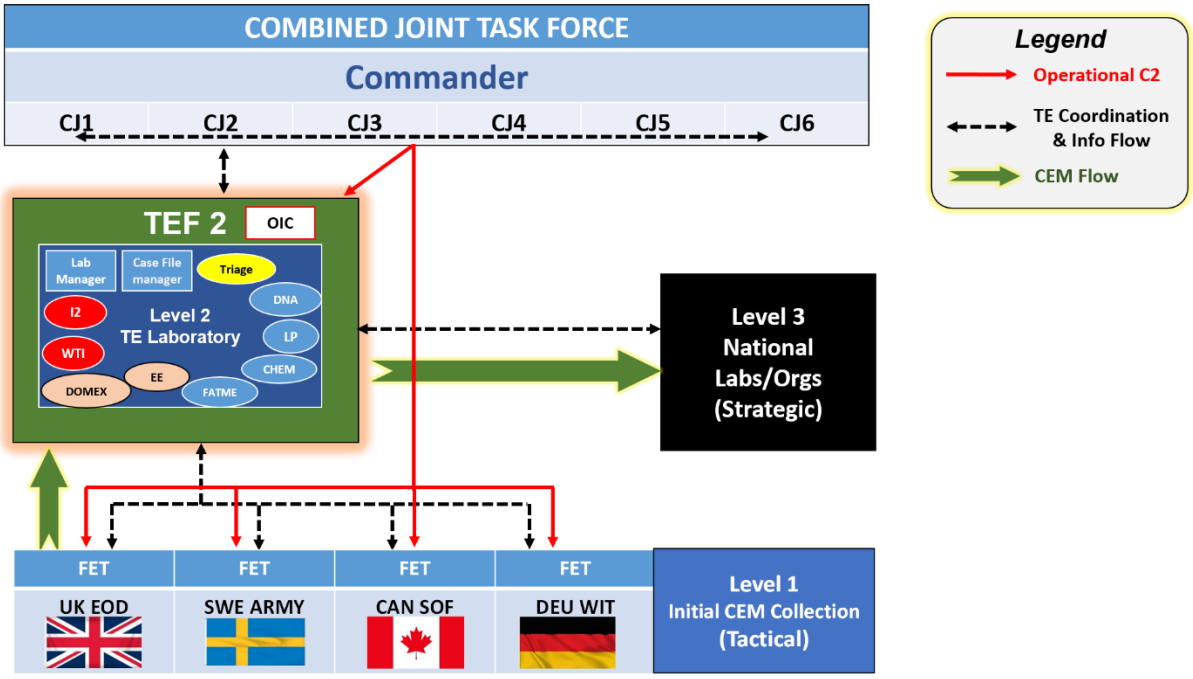

Figure 6 Visual representation of a collocated TEF-2 and Level 2 Laboratory.

While a TEF-2 might be co-located with a Level 2 Laboratory, it could just as well not be co-located. Perhaps the fundamental distinction is that the primary responsibility of the TEF-2 is the organization and management of TE while the primary responsibility of the Level 2 Laboratory is the actual processing and exploitation of CEM. Another distinction between a TEF-2 and a Level 2 Laboratory is that the TEF-2 will be composed of military staff officers and NCOs, whereas the Level 2 Laboratory will include scientific and technical staff, either military or civilian.

Three key questions raised in the TE Seminar were 1) whether the staff functions, such as Combined Joint Staff Personnel (CJ1), CJ2, CJ3, Combined Joint Planning Staff (CJ5), etc.) should be organic in the TEF-2; 2) whether the TEF-2 serves as a CEM consolidation point; and 3) whether the TEF-2 should include a kind of PED cell responsible for the fusion of TE results. Only on this last point does AIntP-10 provide and answer, including the PED in the list of TEF-2 functions. However, several nations related how they conduct PED functions either within a Level 2 Laboratory or even within Level 1 capabilities. This issue merits further investigation.

Several nations related lessons from their own operations and exercises that buttressed the TE Seminar's interpretation of the TEF-2 concept. Sweden indicated that their approach in Mali was to coordinate TE at what they called a TECC (Technical Exploitation Command and Control), which is similar concept to the TEF-2. Canada has also experimented since 2021 with a TEF-2 concept, calling it a TEG (TE Group) in its Exercise ARDENT DEFENDER. In ARDENT DEFENDER the TEG (TEF-2) exercised direct TACON of Level 1 enhanced Field Exploitation Teams (eFETs) and also established an intelligence support cell to compare intelligence results from other TE sub-capabilities, such as from WIT and Intelligence Support Teams (IST). The Netherlands described their concept for TE in which a TAC (Technical Analysis Cell) within the TE Company (COY) provides TE tasking and has an understanding of sensor capacity and capability. This role provides the C2 of TE by managing the TE process chain.

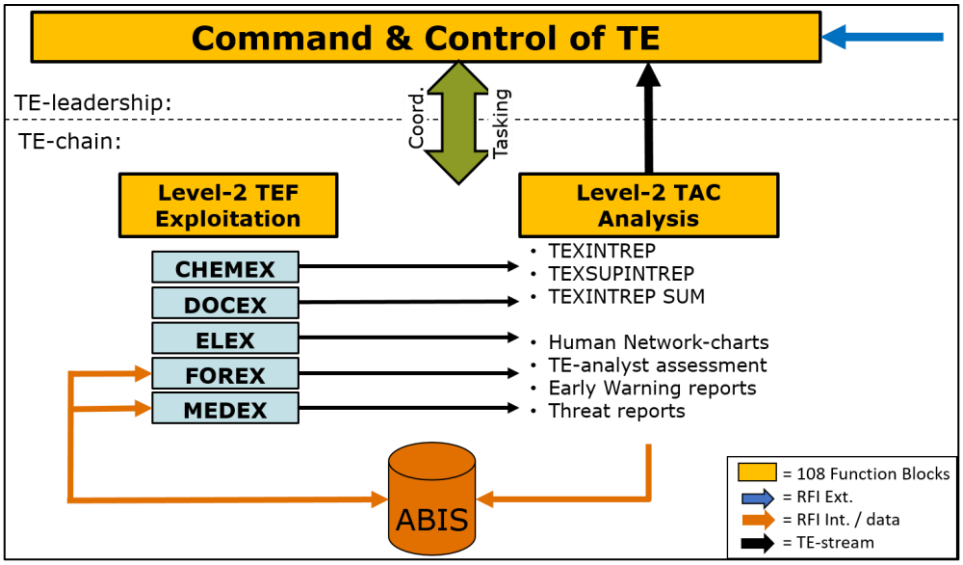

Figure 7 Illustration of TE flow of tasking, co-ordination and reporting according to Dutch doctrine.

Regardless of what it is called or its exact organization, the TE Seminar made it clear that nations have recognized the need for a TEF-2 *function* in TE. Many nations are evolving TEF-2 like structures; others have recognized the need for such a function where it was lacking in operations

or exercises. All of the nations represented view NATO as the ideal venue in which to further develop, exercise and, eventually, operate this concept.

2.3.4 Conclusions

NATO doctrine is not sufficiently detailed enough to implement such an important concept as the TEF-2. Additionally, the concept, and name, as described is easily confused with a Level 2 Laboratory, which has a completely different function. However, a number of nations have started to implement such a TEF-2 concept nationally and multi-nationally. The naming convention needs to be rationalised to avoid confusion and clearer functional responsibilities need to be established. Finally, because the TEF-2 is the link between tactical and operational TE capabilities on the one hand and non-specialized TE force elements providing collection as well as the higher level CJTF, it will be important this link be recognized in the relevant non-TE doctrine.

2.3.5 Recommendations

2.3.5.1 Developing NATO doctrine

- Develop a better term for the TEF-2 to differentiate it from the Level 2 Laboratory and to more clearly reflect the TEF-2 organization and management function.
- Elaborate more fully the TEF-2 concept to describe its role in managing and co-ordinating in-theatre TE activities.
- Ensure that the TEF-2 concept is recognized in relevant non-TE doctrines, especially intelligence doctrine.

2.3.5.2 Experimenting and exercising TE concepts

- Experiment and/or exercise the TEF-2 concept during multinational experiments and exercises such as MARTIAL VISION, Exercise ARDENT DEFENDER, Exercise CLOCKWORK ORANGE and Exercise BISON COUNTER.
- Experiment and/or exercise the staff functions, such as CJ1, CJ2, CJ3, CJ5, etc. as organic to the TEF-2.
- Experiment and/or exercise inclusion of a PED cell in the TEF-2 responsible for the fusion of TE results.
- Investigate via experimentation and/or exercise whether the TEF-2 should serve as a theatre CEM consolidation point.

2.4 COLLECT ONLY VS COLLECT & EXPLOIT ROLES

2.4.1 MV TE Seminar Learning Objectives

Addressed during the TE Collection seminar learning objective session.

2.4.2 AIntP-10 references

Referenced in AIntP-10 in the following areas of the document:

- Section 1.2, paragraph 7

- Section 1.3, paragraph 3
- Section 1.3, paragraph 6
- Section 1.4, paragraph 1, item d, e & g
- Section 2.2, paragraph 1, item b

2.4.3 Observations

This section of the Seminar addressed the organization, responsibilities, and capabilities of TE Level 1 collection teams, to include incidental collection, in support of operations. After Task, Collect is the second step in the TE Process and in the minds of many this is where TE begins.

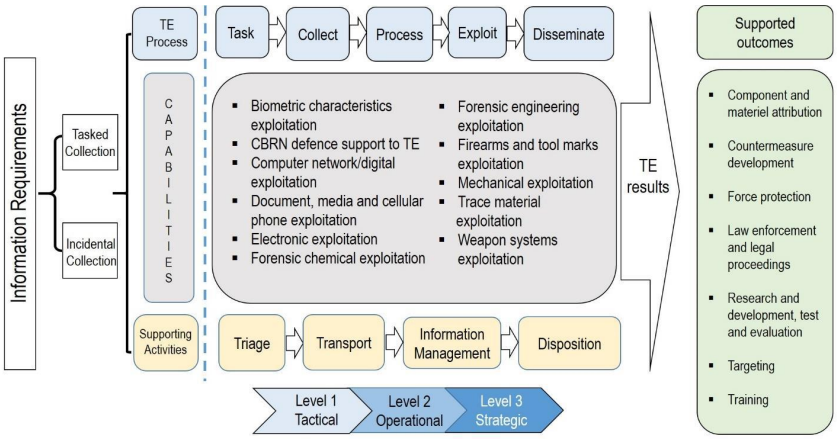

Figure 8 The TE Process "Task, Collect, Process, Exploit and Disseminate" mirrors the JISR TCPED process.

Field Exploitation Teams, or FETs, are identified in AINTP-10 as the collectors of CEM at level 1. However, the doctrine does not provide a clear definition of a FET. This necessitated the Seminar staff to propose the following as a working definition of a FET:

> *A tactical formation of undefined size capable of performing Level 1 TE collection of CEM. A FET may also be capable of limited processing, exploitation and dissemination of Level 1 TE Results. FETs are generally task-organized from non-TE-specialized force elements (ex: Military Police (MP), Explosive Ordnance Disposal (EOD), MILENG Advanced Search (AS)) but may be specialized Level 1 TE units (ex: WIT).*

FETs, therefore, may or may not have specialized TE training and could be (although they are not in AIntP-10) as non-specialized FETs and specialized FETs. FETs without specialized TE training may be limited to only performing the Collect and Process role within the TE process, and then turning over CEM to "specialized FETs", such as WIT, or delivering CEM to Level 2 for further processing and exploitation. This has important implications for reporting requirements and chain of custody. "Non-specialized" FETs are also be more likely to engage in incidental rather than tasked collection, although all FETs should be aware of intelligence requirements and be "forensically aware". This concept of Level 1 Collection is reflected as well in the NATO Defence Planning Process

(NDPP) Capability Codes and Capability Statements, which identify WIT as “Level 1 TE” (a “specialize FET) but identify that several other force elements (EOD, MIO, AS, CBRN Multirole Exploitation and Reconnaissance Team (MERT)) be capable of collecting and processing CEM (as “non-specialized FETs).

Several nations participating in the Seminar Panel supported this conceptual interpretation of the FET. The Netherlands’ TE COY, for example, includes highly trained, highly educated specialists for Level 1 TE, literally called Field Exploitation Teams, whose collection activities are supplemented by incidental collection by other force elements (Special Operations Forces (SOF), Military Engineering (MILENG), EOD). While Netherlands’ FETs exploit, some of the other force elements only collect and process. The United Kingdom (UK) and Canada flip this concept on its head, by deploying “Level 2 capability” to the site (Level 1), either as a collection capability itself (UK) or as support to Level 1 teams (Canada) – while recognizing that non-TE-specialized force elements may also collect CEM and contribute it to the TE system. Canada also is experimenting in ARDENT DEFENDER with “enhanced Field Exploitation Teams”, or “eFETs” in order to distinguish between FETs with specialized TE training and roles in the TE process and generalist “collectors”. This flexible approach to “levels” of TE is a reality and a reminder that the definition of Levels in TE doctrine is helpful as a frame of reference but should not be seen as prescriptive.

Germany indicated that this has more than just academic relevance: it is procuring equipment for these capabilities, so will need to define these two separate categories of “incidental collection” and “planned collection and exploitation”.

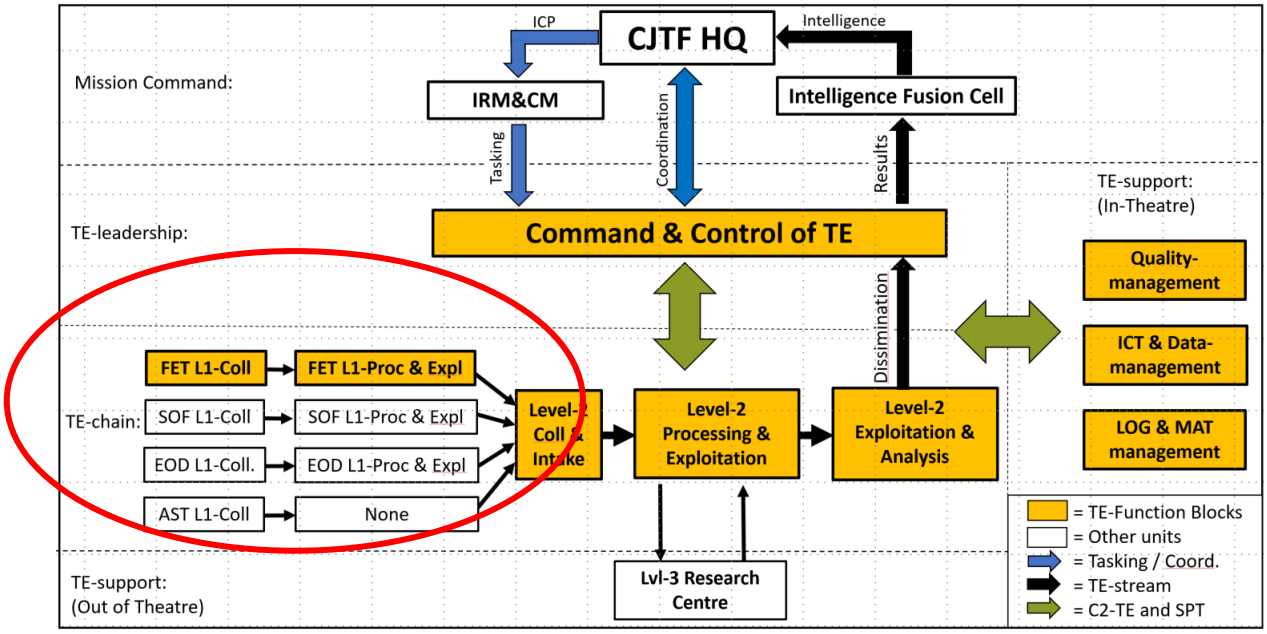

Figure 9 The Dutch conception of TE, noting the relationship among different Level 1 elements.

The Seminar highlighted a further ambiguity in AIntP-10 regarding whether the TEF-2 organization can form FETs or if a Level 1 TE capability or team was intended to be organic to a TEF-2. This is stated in AIntP-10 but could be seen as at odds with the conception of a TEF-2 as a staff element rather than an actual TE capability. This raises the further question of whether a TEF-2 has OPCON (operational control) over FETs.

Canada noted that in its Exercise ARDENT DEFENDER 2021 experimentation with a TEG (TEF-2), FETs, Level 2 Laboratories and the TEG were all co-located and the TEG had OPCON over the eFET. Such colocation strongly supported prioritization, tasking and coordination but it should be noted that such a construct may not be achievable in a larger operation. The United States review of operations in a maritime environment highlighted aspects, and constraints, that may not be adequately considered in AIntP-10 such as the role of maritime interdiction teams and divers as FETs and their relation with other elements of the TE framework like Level 2 Laboratories and TEF-2. This panel presentation highlighted the need to further consider the maritime domain when revising AIntP-10.

A final aspect of this subject to be considered is the relationship between FETs of multiple nationalities as well as a FET of one nation and Level 2 lab of another. As detailed in the next section, TE in a NATO operation will be a coalition of national Level 1 and Level 2 capabilities under NATO C2. It will be standard operating procedure for one nation's capability to disseminate CEM or TE results to another nation's capability and for TE results achieved in a coalition environment to be shared across the coalition. Better understanding the C2 and reporting relationship among all of these capabilities is further complicated by multinationality.

2.4.4 Conclusions

- AIntP-10 needs to distinguish between situations for collect only (likely via incidental collection) vs collect and exploit. This may also need to be reflected in the NDPP capability codes and capability statements as well as related NATO doctrine.
- A clearer definition of FETs and how they support TE operations will aid preparation, planning and training.

2.4.5 Recommendations

2.4.5.1 Developing NATO doctrine

- Consider "incidental collection" and "planned collection" for TE outlining the differences between the two terms within the context of "collection" vs "collection and exploitation" in AIntP-10.
- Clarify the relationship, or potential relationships, between "non-specialized" FETs, "specialized" FETs, Level 2 Laboratories and TEF-2.
- A review of the NDPP capability codes and statements for Level 1 TE capabilities should consider the role of FETs in the TE system.

2.4.5.2 Experimenting and exercising TE concepts

- Experiment concepts of incidental collection and planned collection for TE noting the impact each has on exploitation.
- Experiment with formation of FETs within/from TEF-2.

2.5 LEVELS OF TECHNICAL EXPLOITATION AND THE PED

2.5.1 MV TE Seminar Learning Objectives

Addressed during the following seminar learning objective sessions:

- TE Framework
- CJTF staff responsibility for TE
- Technical Exploitation Lab – Level 2
- TE collection

2.5.2 AintP-10 references

Referenced in AIntP-10 in the following areas of the document:

- Section 2.2, paragraph 1, item d
- Section 2.3
- Section 3.5
- Annex C

2.5.3 Observations

2.5.3.1 The Levels of TE

As currently conceived, in NATO operations Level 1, 2 and 3 TE capabilities are provide by nations while NATO provides the C2 of TE. Although not entirely clear in the doctrine, this C2 is likely provided by the TEF-2, located under the CJ2 in the CJTF and in close coordination with CJ3. These are important considerations for national capability development and NATO concept development.

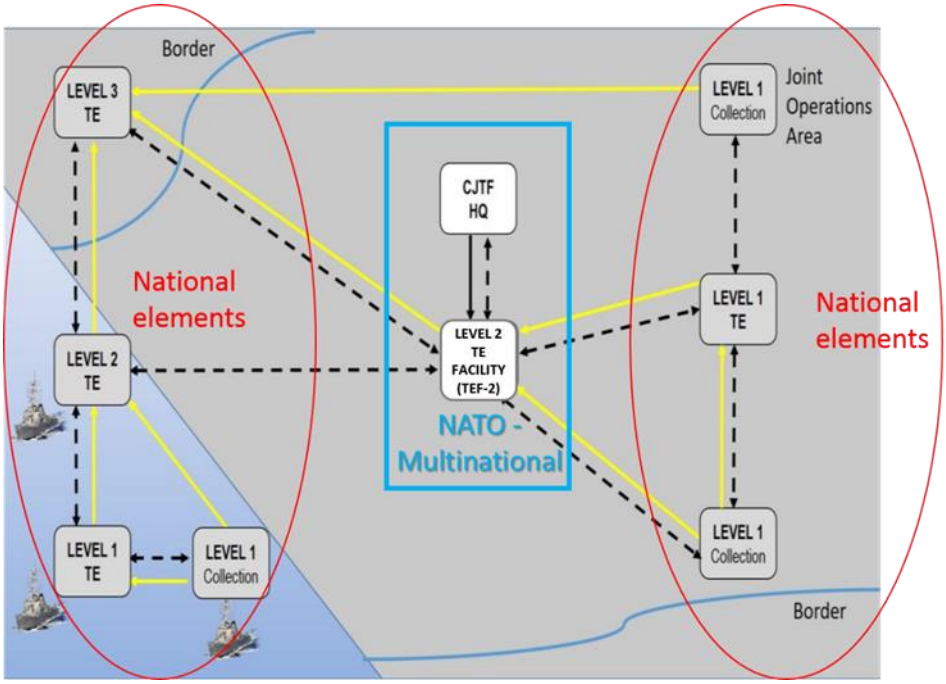

Figure 10 An operational overview of TE in a theatre of operations.

There are 3 levels of TE defined in AIntP-10. AIntP-10 clearly emphasizes that TE levels are not defined by TE capability, but rather by where TE is conducted and the time taken to produce TE results. As a general observation, as the TE level increases the potential level of analysis of the CEM increases. This aligns with tactical, operational and strategic levels at which TE is conducted.

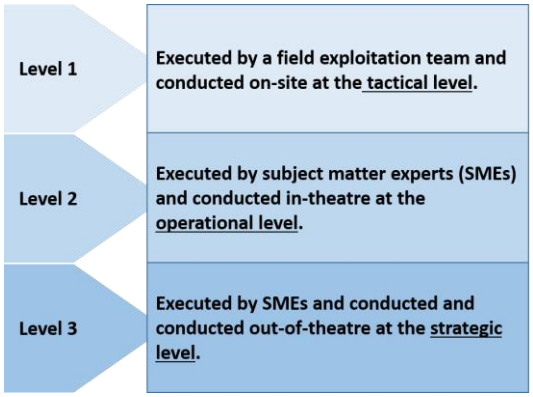

Figure 11 The levels of Technical Exploitation.

It was noted in the Seminar that improvements in technology in terms of reduction in TE processing time and miniaturisation has meant that what was considered to be a level 3 or 2 capability in the

past can often be conducted at level 1 today. This evolution has muddied conceptions of the what is meant by level 1, 2 and/or 3. Hence, the Seminar emphasized AIntP-10's definition of TE levels by their tactical/operational/strategic positioning and considering levels as useful for reference rather than as definition.

As examples of this blurring of levels, the United Kingdom no longer possesses a level 2 TE deployable laboratory capability, but does have experienced personnel and equipment that can be deployed on site (at Level 1) and require support from partner nations for Level 2 laboratory capabilities. NATO SOF noted a need for their own laboratories, or Level 2 capability, at or near the point of collection. Therefore, this "Level 2 Laboratory" capability could be considered Level 1 TE, since it is performing at the tactical site. Germany noted that in addition, Level 1 and Level 2 TE may be conducted by the same person.

Furthermore, several Seminar participants noted the possibility of re-defining levels based on "intrusive" versus "non-intrusive" exploitation and this distinction in some cases established the difference in what different units are capable of.

Despite the potential reinterpretations of levels of TE, the way they are described in AIntP-10 is a useful reference that should be maintained for now. Awareness must be maintained of the potential differing applications of the concept by different nations and force elements so that a commander can understand how to effectively organize and manage the capabilities at his/her disposal.

2.5.3.2 The PED

Within JISR doctrine, and therefore within the TE process, the PED stands for Processing, Exploitation and Dissemination. While JISR terminology does not perfectly translate to the TE Process, within the TE process PED means an analytical capability that interprets outputs from various TE sub-capabilities or types (CHEMEX, ELEX, Forensic Exploitation (FOREX), etc.) in order to provide single-source TE results to the JISR, and other, processes. Although AIntP-10 calls for TE capabilities to "include or be collocated with an intelligence and targeting analytic capability where possible" (AIntP-10 p 2-7), it remains unclear just where that capability would be or under what conditions it would be deemed "possible". Based on the comments of participants and panel members in the TE Seminar, there are currently several different approaches to providing this PED capability.

Denmark and the United Kingdom as well as NATO SOF considered the PED a requirement at Level 1. Others, including France, the Netherlands and the United States considered it more of a Level 2 capability. Considering that very few nations have experience of establishing a dedicated TEF-2 like structure, it remains to be considered by NATO whether a PED capability would reside at the TEF-2; doing so would not necessarily preclude Level 1 capabilities from also including a PED capability.

There was broad agreement in the TE Seminar that a PED capability *within the TE framework* was essential in order to prepare TE results so that they be useful to the intended "customer". This is an area obviously in need of further exploration, experimentation and definition.

As with Level 1 FETs, multinationality brings additional complexity, especially as regards classification of CEM and related TE results. Over-classification may impede returning information to the original collecting nation, as strongly attested to by one smaller nation in the TE Seminar. In principle, there is agreement that within a NATO operation TE reports, as opposed to *intelligence reports based on the TE,* from whatever level of TE should be available to the nation that originally collected the CEM. Operational planning, memorandums of agreement, TE management plans and other related planning documentation must take account of this.

2.5.4 Conclusions

While AIntP-10 clearly defines levels of TE according to where the activity takes place, and to an extent by the time involved, there are differences amongst the nations of what is considered Level 1, 2 and 3. Different nations may possess different TE capabilities and not all nations will have TE capabilities at a certain level of TE. In the latter situation, a nation may need to utilise partner nation TE capabilities.

There was wide agreement that some kind of analytical, or PED, capability be present in the TE framework in order to make TE results useful to onward customers. However, approaches differ amongst nations and force elements as to whether this capability be located at Level 1 or 2 or both. The TEF-2 concept adds an additional potential location for the PED capability that requires further experimentation.

2.5.5 Recommendations

2.5.5.1 Developing NATO doctrine

- Flexibility needs to be maintained regarding the definition of levels in TE in order to accommodate different national approaches.
- The challenges of a TE system in a coalition environment need to be accounted for in doctrine and planning - some nations may not have TE capabilities, or may have Level 1 but not Level 2 and may have to rely on other nations' TE capabilities.
- Maintenance of TE capabilities and training/certification of TE expertise (including collection) needs to be considered within the context of standardisation.
- Planning considerations must address ownership of CEM and sharing of associated TE results.

2.5.5.2 Experimenting and exercising TE concepts

- Exercise nations sharing TE capabilities at level 1, 2 and 3 within a multinational coalition.
- Experiment and exercise the TE PED function at different levels of TE, including in the TEF-2.

2.6 NON-LINEAR CEM FLOW

2.6.1 MV TE Seminar Learning Objectives

Addressed during the following seminar learning objective sessions:

- CJTF staff responsibility for TE
- CEM Flow

2.6.2 AIntP-10 references

Referenced in AIntP-10 in the following areas of the document:

- Section 3.5, paragraph 2
- Section 3.5, figure 08
- Section 4.3, paragraph 3

2.6.3 Observations

This section of the TE Seminar addressed CEM Flow – what happens to the physical stuff itself, as opposed to the information associated with or derived from CEM. TE collects Collected Exploitable Material or CEM and derives information of value from it. Very soon after entering the TE system, CEM and the information associated and derived from CEM will very likely begin to take different paths, while remaining linked via reporting and databasing.

AIntP-10 outlines a very linear CEM flow from Level 1, 2 and 3 TE. This is logical and doctrinally sound and supports planning and coordination amongst the CJTF staffs to ensure that the required personnel, logistics, CIS and legal considerations are addressed.

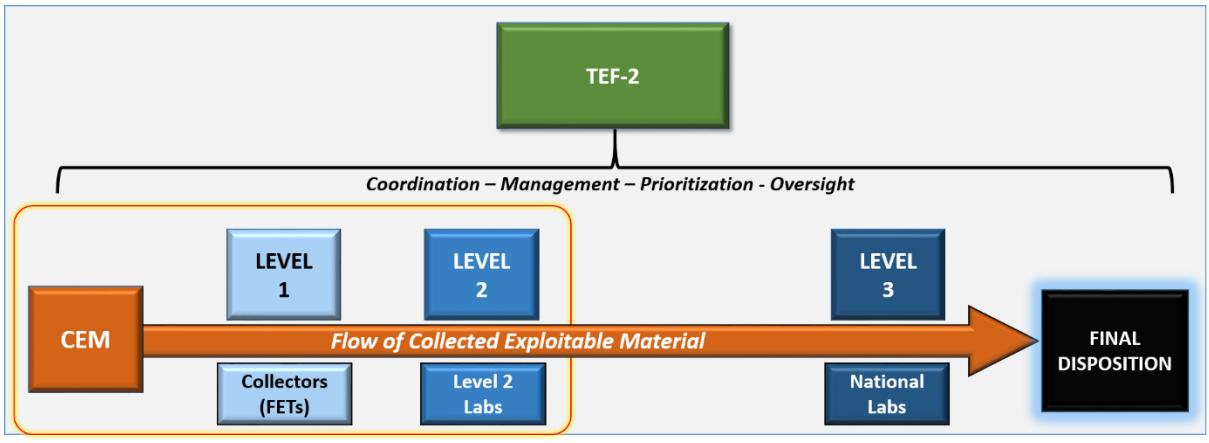

Figure 12 Idealized depiction of CEM flow.

Panel presentations and audience remarks illustrated that this linear process is highly idealized and that, in practice, CEM takes many different routes and, in fact, must do so depending on the outcome

supported or operational constraints in effect. It is sometimes necessary to move CEM from Level 1 TE to Level 3 TE, especially with time-sensitive CEM or if there are no Level 2 capabilities available. On the other hand, there may be situations where significant exploitation will be required on-site at Level 1 and the CEM itself destroyed on-site or left behind due to operational exigencies. The non-linear nature of CEM flow between the levels of TE is therefore difficult to represent in doctrine. This fact does not diminish the relevance of the linear depiction of CEM flow, which remains a valid conceptual construct. However, TE practitioners and capability developers must realize the need for flexibility in the TE framework to deal with real-world requirements and develop procedures that respond to those conditions.

Paramount among these procedures is ensuring chain of custody. Chain of custody is not only relevant in the well-known terms of “evidence preservation”, but also from the standpoint of traceability and discoverability by members of the operational coalition. Keeping CEM unclassified is a key policy step that facilitates traceability, discoverability and disposition, so important that the United States Department of Defense directed that all CEM under control of US forces should be *by default* unclassified. Considerations also have to be given to storage facilities within an operation and thereafter, including considering who owns the CEM in the long run. Disposition of CEM is a supporting activity that is not given much thought in AIntP-10, but has proven to be a very important consideration, especially if CEM is to be eventually used to support law enforcement and legal proceedings.

The United Kingdom’s experience with CEM in support to HUMINT shared in the Seminar panel illustrated the need to keep CEM available to different elements of the force in order to support different outcomes. Other Seminar participants related how clear priority for the application of TE sub-capabilities, like FOREX or ELEX, needed to be established in the TE Collection Plan to ensure that CEM exploited in support of one outcome was not compromised or destroyed before other processes could be applied. The United States related its experiences in Iraq where TE of UAS had to be conducted within the very brief 48-hour period for which Iraqi commanders agreed to loan a captured UAS to US forces. In this situation, TE priorities had to be set and sacrifices made, but clear standard operating procedures ensured that TE opportunities were maximized within the given constraints.

2.6.4 Conclusions

AIntP-10 appears contradictory at times with regard to CEM flow. In some areas of the doctrine it mentions a FET may need to forward CEM to a level 2 or level 3, but in other areas of the doctrine, such as figure 08 in AIntP-10 Ed B, indicates a linear flow of CEM from Level 1 TE, to Level 2 TE and then finally to Level 3 TE. In practice, CEM may flow in a non-linear fashion between TE levels. The linear model of CEM flow remains a valid conceptual construct but flexibility within the TE framework will help to deal with real-world conditions. Disposition of CEM is a consideration that has received relatively little attention but must be addressed in planning.

2.6.5 Recommendations

2.6.5.1 Developing NATO doctrine

- Maintain the linear CEM flow model in AIntP-10 while ensuring that TE practitioners understand the need to be flexible in the face of real-world constraints.
- Consider further development of doctrinal approaches to the TE supporting activities of transportation, CIS and disposition.

2.6.5.2 Experimenting and exercising TE concepts

- Consider experimenting and exercising CEM flow by setting up various vignettes and scenarios that will illustrate the non-linear nature of CEM flow, such as the time-limited constraints on returning CEM.

2.7 MANAGING TE RESULTS

2.7.1 MV TE Seminar Learning Objectives

Addressed during the following seminar learning objective sessions:

- TE Framework
- Managing TE results

2.7.2 AIntP-10 references

Referenced in AIntP-10 in the following areas of the document:

- Section 3.5
- Section 4.3

2.7.3 Observations

Considering that TE results, in other words, the information derived from TE, is the whole point of TE, it is surprising how little consideration is given to the management of the data derived from TE. Yet, AIntP-10 and other intelligence doctrine do not provide a lot of guidance in this area. The TE Seminar devoted a session to better understanding NATO and National data management to produce, disseminate and retain TE results.

As stated in the previous section, an important starting point is to consider CEM flow and derived data flow as separate challenges. While managing CEM flow requires physical transportation and storage capacity, managing TE results requires bandwidth, CIS and legal frameworks. In most cases TE supports multiple outcomes – not just intelligence – and thus requires reporting of TE results across the joint force. An information management plan, that may be included as part of the TE Management Plan, must be established prior to operations in order to effectively manage TE results and, as with the CEM itself, ensure traceability and discoverability by all customers across the force. This also implies that TE results need to be fit for purpose and reports tailored to individual customers so that they can easily understand the results and analysis.

NATO doctrine provides only a few examples of TE reporting requirements, but exercises and operations discussed in the TE Seminar demonstrate that nations use a multiplicity of reports for different purposes. There was general consensus that NATO does not need to provide "a report form" for TE reporting, but that defining *common reporting requirements* would support interoperability and the effectiveness of TE. Similarly, there is likely not a need for a NATO information management *system*, but defining requirements for information management of TE in operations could be beneficial[6]. The United States suggested that a place to start is to establish a system for URIs (Unique Reference Identifier) for CEM and reports.

TE results and associated intelligence not only move "up the chain", but also need to be returned back down to the operational and tactical level to improve future collection and reporting. In particular, collectors at Level 1 and exploiters at Level 2 need to have a sense of validation from collection and processing of CEM. A simplified conception of how this could work is provided here:

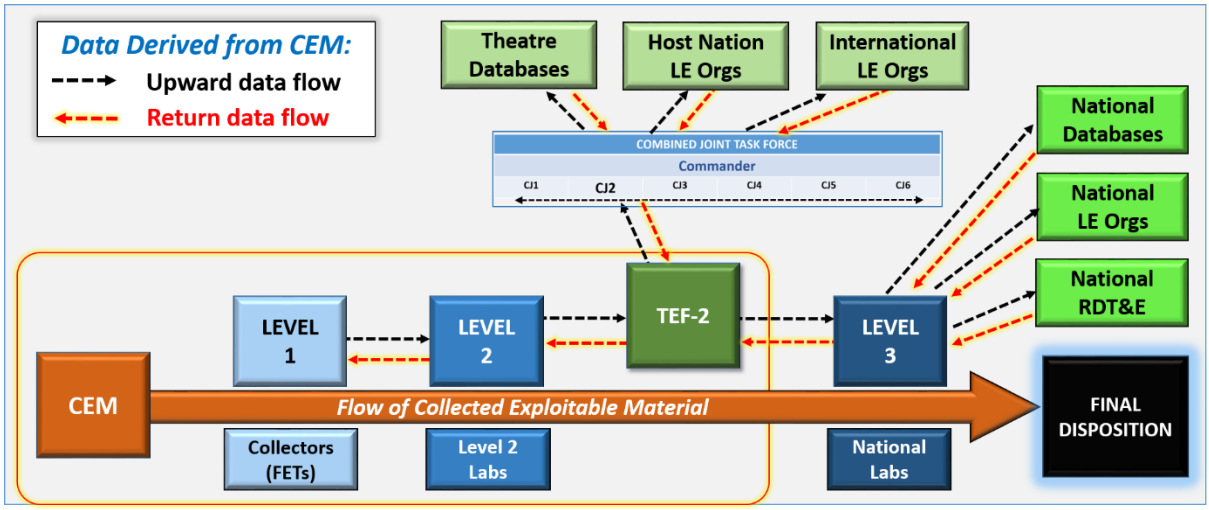

Figure 13 CEM data flow and TE results at various levels of TE, commands, and organisations.

2.7.4 Conclusions

Management of the information derived from TE is not adequately addressed in current doctrine. Especially in a multinational coalition operation, it will be important to ensure that all contributing nations have the necessary information to conduct missions in support of COM CJTFs objectives.

Depending on the size of operation, different types of reports will be generated by different nations and expected to be shared with other nations. It is therefore important to be able to register reports,

[6] See the NTEG's AC/343-WP(2021)0001 Process Data Management System to Support TE Operations working paper developed by the Netherlands as an introduction to this subject.

documents and CEM so that they can be tracked, published and made discoverable to those within the coalition.

2.7.5 Recommendations

2.7.5.1 Developing NATO doctrine

- Provide the conditions for sharing CEM and TE results and their statuses in AIntP-10.
- Consider the mechanisms for sharing TE results in AIntP-10, particularly to making reports discoverable.
- Consider "TE gaps" and means to record and share these gaps in AIntP-10.

2.7.5.2 Experimenting and exercising TE concepts

- Exercise procedures and sharing mechanism for CEM and TE results.

2.8 TECHNICAL EXPLOITATION CONDUCTED IN SUPPORT OF INTELLIGENCE-BASED VS EVIDENCE-BASED OPERATIONS

2.8.1 MV TE Seminar Learning Objectives

Addressed during the following seminar learning objective sessions:

- TE Framework
- TE Collection

2.8.2 AIntP-10 references

- There is minimal reference in AIntP-10 of evidence based-operations and no discussion of its comparison with intelligence-based operations. The mention of CEM and its technical exploitation for evidence is mentioned in AIntP-10 in the following areas of the document:
- 2.3.1, paragraph 6, item c
- footnote to 2.6, paragraph 4, 4 bullet
- Paragraph A.7
- C.1, figure 10, 4th row

2.8.3 Observations

Collected Exploitable Material (CEM) and its subsequent Technical Exploitation can support intelligence-based (including military peacetime and crisis) operations or evidence-based operations. For intelligence-based operations, the intent of TE is to support the commander's situational awareness and decision-making, normally as input to the intelligence[7] and/or operations[8] processes. In intelligence-based operations, satisfying PIRs, targeting and force protection are

[7] Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security, NSO, Edition B, Version 1, July 2020, NATO UNCLASSIFIED
[8] Allied Joint Doctrine for the Conduct of Operations, NSO, Edition C, Version 1, February 2019, NATO UNCLASSIFIED

generally the priority outcomes supported by TE. Evidence based operations on the other hand, normally support law enforcement and legal proceedings primarily.

A common source of confusion about the nature of and requirements for TE comes from a lack of understanding of the difference between these two kinds of operations. For example, CEM from evidence-based operations may be used to support intelligence, but not all, if any, results from intelligence-based operations may be used as evidence. The customers for CEM, its subsequent technical exploitation and reporting are likely to be different depending on its purpose and therefore it is important to know the customer, their requirements as well as the rules and regulations for the handling of CEM, its subsequent technical exploitation and reporting of results. Different standards for chain of custody and fidelity of information derived from CEM using TE can also have major impact on military training and materiel requirements.

It was noted during the TE Seminar that CJTF staff are supported by LEGAD who will advise on with whom to share the TE results based on bilateral, trilateral and multinational agreements in a theatre of operation.

It is the general view in most nations that TE in support of Intelligence is the primary focus in support of a NATO commander whilst support to evidence collection is secondary. The legal framework under which evidence-based operations are conducted is complex and likely can only be determined in a specific operational context and is thus clearly an essential planning consideration.

The panel member from the United States concurred that TE collection needs to ultimately support the commander's objectives, such as "Attack the Networks". Of secondary import is to support as evidence, although it was noted that US forces in Iraq collected for Intel and for evidence at the same time. The experience of the United States also shows that collecting and technically exploiting CEM within a host nation or partner nation normally will adhere to the chain of custody policy of the host nation for evidence-based operations and the TE results are pushed to the customer, but made available to others as a pull.

Swedish experience in support of evidence-based operations within their own national territory demonstrate that the Swedish military follow the TE regulations of the Swedish Police. Sweden noted that, for them, there is no difference in their TE capabilities between domestic operations and international operations or between peacetime to crisis to conflict. The key is that TE support the end-state of these operations.

The Netherlands offered that it is challenging to train military forces to use TE to support both intelligence-based and evidence-based operations. In general, it is more effective, and sufficient, that military forces conduct "forensically aware" collection following referenced standard operating procedures. This will allow military TE that primarily serves intelligence-based operations to be used for evidence if the need arises and judicial system requirements permit. In addition, it is simply more realistic to set standards to meet military requirements based on acting together as NATO, than to

set military requirements based on the myriad different civilian judiciary and legal systems that "might" be supported.

The Dutch view was supported by NATO Special Operations Headquarters (NSHQ). NSHQ underlined the need for a better understanding of evidence-based collection planning should that be the mission priority. For intelligence-based targeting there is less need to be as stringent and it may be helpful to identify different minimum requirements for "warrant based" or "evidence-based targeting" vs "Intel-based targeting".

2.8.4 Conclusions

- TE may support intelligence-based operations as well as evidence-based operations. Each will have different customers and requirements and may follow different rules for collection of CEM and its subsequent exploitation.
- In AIntP-10, there is little reference to TE in support of evidence-based operations and its distinction from intelligence-based operations. Future editions may wish to consider this issue as it can have an important impacts on training, materiel, certification and reporting requirements.

2.8.5 Recommendations

2.8.5.1 Developing NATO doctrine

- Consideration of intelligence-based operations supporting primarily targeting and force protection and its comparison to evidence-based operations supporting primarily law enforcement and legal proceedings; the different customers for each and their implications to TE in AIntP-10.

2.8.5.2 Experimenting and exercising TE concepts

- Develop vignettes for both intelligence-based and evidence-based operations and the typical customers they support to look at their impact on TE, especially within the context of the TEF-2 concept.

2.9 CONCLUSION

2.9.1 The Martial Vision Technical Exploitation Seminar held 13-14 December 2021 welcomed approximately 80 participants from 17 NATO nations, Sweden and multiple NATO entities as well as an observer from the European Defence Agency.

2.9.2 Substantial support to the TE Seminar was provided by the San Marcial Spanish Army Division Headquarters in Burgos and by the nations and NATO bodies supporting the Martial Vision Tiger Team in planning and executing the TE Seminar.

2.9.3 This Lessons Identified Report will be distributed to the entire NATO Technical Exploitation Group (NTEG) community. As many of the lessons identified also concern other NATO communities, notably those for Intelligence, Special Operations, C-IED, EOD, CBRN Defence, Counter-Intelligence, Military Police and Stability Police, the Report will also be distributed widely among those communities. This does not imply any taskings on or concurrence of those communities with the findings in the Report.

2.9.4 At the time of publication of this Report, the Martial Vision Tiger Team is finalizing planning for the Martial Vision Technical Exploitation Experiment, which will be held 13-17 June 2022 in Burgos. The TE Experiment will further analyse and experiment with the TEF-2 concept as described in this Report. It is hoped that this Report will likewise contribute to further experimentation of other key technical exploitation concepts.

ABBREVIATIONS

ABIS	Automated Biometric Identification System
AIntP	Allied Intelligence Publication
AJP	Allied Joint Publication
AS	Advanced Search
C2	Command and Control
C-IED	Countering Improvised Explosive Devices
C-UAS	Counter Unmanned Aircraft System
CBRN	Chemical, Biological, Radiological and Nuclear
CELEX	Cellular (cell phone data) Exploitation
CEM	Collected Exploitable Material
CEMA	Cyber and Electromagnetic Activities
CHEMEX	Chemical Exploitation
CI	Counter Intelligence
CIS	Communications and Information Systems
CJ1	Combined Joint Staff Personnel
CJ2	Combined Joint Intelligence Staff
CJ3	Combined Joint Operations Staff
CJ4	Combined Joint Logistics Staff
CJ5	Combined Joint Planning Staff
CJ6	Combined Joint Communications and Information Systems Staff
CJCMEC	Combined Joint Captured Materiel Exploitation Centre Components
CJTF	Combined Joint Task Force
CTL	Collection Task List
COE	Centre of Excellence
CONOPS	Concept of Operations
COY	Company
DNA	Deoxyribonucleic Acid
DOMEX	Document and Media Exploitation
eFET	Enhanced Field Exploitation Team
ELEX	Electronic Exploitation
EOD	Explosive Ordnance Disposal
FET	Field Exploitation Team
FOREX	Forensic Exploitation
FRAGO	Fragmentary Order
HNA	Human Network Analysis
HNAT	Human Network Analysis and support to Targeting

HUMINT	Human Intelligence
HQ	Headquarters
I2	Identity Intelligence
ICP	Intelligence Collection Plan
IMINT	Imagery Intelligence
IRM and CM	Intelligence Requirements Management and Collection Management
IST	Intelligence Support Team
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
JIPOE	Joint Intelligence Preparation of the Operational Environment
JISR	Joint Intelligence, Surveillance and Reconnaissance
LEGAD	Legal Advisor
MASINT	Measurement and Signature Intelligence
MEDEX	Media Exploitation
MERT	Multirole Exploitation and Reconnaissance Team
MILENG	Military Engineering
MIO	Maritime Interdiction Operations
MOU	Memorandum Of Understanding
MP	Military Police
MV	MARTIAL VISION
NDPP	NATO Defence Planning Process
NSHQ	NATO SOF HQ
NTEG	NATO Technical Exploitation Group
OPCON	Operational Control
OPLAN	Operation Plan
OSINT	Open Source Intelligence
PED	Processing, Exploitation, and Dissemination
QM	Quality Manager
R&D	Research and Development
RDT&E	Research, Development, Test & Evaluation
RECCE	Reconnaissance
SIGINT	Signal Intelligence
SOF	Special Operations Forces
SOP	Standard Operating Procedures

TAC	Technical Analysis Cell
TACON	Tactical Control
TE	Technical Exploitation
TECC	Technical Exploitation Command and Control
TEF-2	Technical Exploitation Facility – level 2
TEG	Technical Exploitation Group
TEXINT	Technical Exploitation Intelligence
TEXINTREP	Technical Exploitation Intelligence Report
TEXTSUPINTREP	Technical Exploitation Supplementary Intelligence Report
TEXTINTREPSUM	Technical Exploitation Intelligence Summary Report
TTP	Tactics, Techniques and Procedures
UK	United Kingdom
URI	Unique Reference Identifier
WIT	Weapons Intelligence Team