NATO STANDARD

AJP-2.6

ALLIED JOINT DOCTRINE FOR IMAGERY INTELLIGENCE

Edition A Version 1

MARCH 2018

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)
NATO STANDARDIZATION OFFICE (NSO)
NATO LETTER OF PROMULGATION

15 March 2018

1. The enclosed Allied Joint Publication AJP-2.6, Edition A, Version 1, ALLIED JOINT DOCTRINE FOR IMAGERY INTELLIGENCE, which has been approved by the nations in the Military Committee Joint Standardization Board, is promulgated herewith. The agreement of Nations to use this publication is recorded in STANAG 6507.

2. AJP-2.6, Edition A, Version 1, is effective upon receipt.

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

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

BEL	Satellite imagery can only be shared in the event all consortium members agree
BGR	Due to the lack of capabilities, the Bulgarian Armed Forces will not implement Chapters 3, 4, 5 and 6 of AJP-2.6 EDITION A.
USA	- There is no section to guide the exploitation phase. - The doctrine is inadequate to the point of misleading in regards to who and how Precise Point Mensuration (PPM) is conducted. It's likewise inadequate in the role of IMINT in Target Dossier (NATO term for intermediate target folder production) - It references irrelevant items such as the Recognized Environmental Picture (REP) which is (1) not an agreed capability and (2) conceptually does not include intelligence. Likewise, the Common Operational Picture (COP) does not include imagery intelligence. However, both include the use of imagery from the geospatial realm. Given the scope of the document (IMINT, and not imagery as a whole), this does not fit. - There is no indication of how Nations engage with NATO and vice versa regarding IMINT issues, requirements, production, proposals, etc. - There is no indication of how incidental imagery coverage is handled. These reservations will be removed when the AJP adequately addresses these issues in appropriate level three joint doctrine (AIntP)

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

A. MCM-0077-2000, *Military Committee Guidance on the Relationship between NATO Policy and Military Doctrine*

B. MC 0114, *Procedures for Production of NATO Agreed Intelligence*

C. MC 0128/8, *Policy Guidance for NATO Intelligence*

D. MC 0133/4, *NATO Operations Planning*

E. MC 0166, *NATO Intelligence Warning System*

F. MC 0582/1, *NATO Joint Intelligence, Surveillance and Reconnaissance Concept*

G. MC 0596, *NATO Imagery Intelligence Policy*

H. AAP-03, *Production, Maintenance and Management of NATO Standardization Documents*

I. AAP-06, *NATO Glossary of Terms and Definitions*

J. AAP-47, *Allied Joint Doctrine Development*

K. AJP-01, *Allied Joint Doctrine*

L. AJP-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*

M. AJP-2 Series, *Intelligence Disciplines*

N. AJP-2.7, *Allied Joint Doctrine for Intelligence, Surveillance and Reconnaissance*

O. AJP-3, *Allied Joint Doctrine for the Conduct of Operations*

P. AJP-3.4, *Allied Joint Doctrine for Non-Article 5 Crisis Response Operations*

Q. AJP-3.9, *Allied Joint Doctrine for Joint Targeting*

R. AJP-3.15, *Allied Joint Doctrine for Countering - Improvised Explosive Devices*

S. AJP-3.17, *Allied Joint Doctrine for Geospatial Support*

T. AJP-5, *Allied Joint Doctrine for Operational-Level Planning*

U. AIntP-11, NATO *Intelligence Training*

INTENTIONALLY BLANK

Preface

Context

1. Lessons learned from recent NATO operations have demonstrated the vital importance of imagery and imagery-based intelligence in the joint intelligence preparation of the operational environment (JIPOE); support to planning and the conduct of operations.

2. This Allied joint publication (AJP) *Allied Joint Doctrine for Imagery Intelligence* AJP-2.6 considers imagery intelligence (IMINT) in the context of the digitized era where modern air, land, maritime, and space platforms may all be employed as imagery collection systems. Technological advancements (e.g. from wet film to digital sensors) have enhanced the capabilities of imagery systems, for both collection and exploitation, and changed the way that imagery can be used operationally. In the digital era, with increased communication means, still imagery, imaging radar scans, and video can now all be sources of near real-time information.

Scope

3. AJP-2.6 describes how imagery and IMINT activities are planned, conducted and assessed in NATO, with a focus on the operational level. It explains the role of IMINT as one of the Intelligence collection disciplines in the context of the joint intelligence surveillance and reconnaissance (JISR) process, and its wider application within the intelligence cycle.

Purpose

4. This doctrine is intended primarily for NATO operational level commanders and staffs' but is also applicable as a reference at any level of command. It is also intended as a reference document, on the employment of IMINT for intelligence staffs and provides an explanation of the NATO IMINT collection discipline to those external to the NATO organization. The IMINT doctrine can also to be used to support education and training activities.

Application

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

Target audience

6. AJP-2.6 is intended primarily as guidance for joint NATO commanders and staff. However, the doctrine is instructive to, and provides a useful framework for, operations conducted by a coalition of NATO members, partners and non-NATO nations. It also provides a reference for civilian personnel.

Structure

7. AJP-2.6 is divided into six chapters, and one annex that provides a list of NATO and international imagery and IMINT standards.

   a. Chapter 1 – Imagery and Imagery Intelligence Fundamentals

   b. Chapter 2 – IMINT and the Intelligence Cycle

   c. Chapter 3 – IMINT Support to NATO Operations

   d. Chapter 4 – Organizations and Responsibilities

   e. Chapter 5 – IMINT Interoperability

   f. Chapter 6 – IMINT Training

Linkages

8. AJP-2.6 is intended to be read with the NATO capstone document, AJP-01 *Allied Joint Doctrine* and the keystone intelligence document AJP-2 *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*. Other documents that are linked to AJP-2.6 are:

   a. AJP-2.1 *Allied Joint Doctrine for Intelligence Procedures*.

   b. AJP-2.7 *Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance*, as it lays out the processes whereby agencies with intelligence collection and/or processing, exploitation, and dissemination (PED) capabilities are tasked.

Table of Contents

Chapter 1 – Imagery and Imagery Intelligence Fundamentals

Section 1 – Introduction

1.1. Commanders require timely, tailored, and accurate intelligence to accomplish their missions. In order for intelligence staffs to support this requirement and to allow their commanders to better visualize the operating environment,[1] it is important for them to understand how imagery and imagery intelligence (IMINT) supplements other intelligence disciplines and how it can help commanders and staffs achieve a better understanding of the operating environment.

Section 2 – Explanation and Clarification of Terms

1.2. AJP-2.6 uses the NATO agreed terminology whenever possible. Additionally, three generic terms are used:

a. **Commander**. From the intelligence perspective, the commander is the authority, at any level, who requires the intelligence to collect, elaborate, assess and make decisions.[2]

b. **CJ2**. The combined joint intelligence staff (CJ2) is the intelligence branch in a combined joint headquarters (HQ) - the head of this branch may also be known or referred to as the CJ2. For the purpose of simplicity, the NATO staff numbering structure; 1 - personnel and administration; 2 – intelligence; 3 – operations; 4 – logistics; 5 – plans; 6 - command, control, communications, and computer systems; etc. and the C and J prefixes are used throughout this publication to imply the senior functional officer of any HQ or unit, without prejudice to size, function, service, or nation.

c. **Actor**. The term actor refers to a person or organization, including state and non-state entities, within the international system with the capability or desire to influence others in pursuit of its interest and objectives.[3]

1.3. Imagery, in and of itself, is not intelligence. IMINT is produced by imagery analysts who have conducted appropriate analysis of individual images or image sequences, using specific tools and techniques. IMINT products are the result of a deliberate effort to collect, process, and exploit select imagery, in an effort to answer intelligence requirements. IMINT can be supported by, as well as support, other intelligence collection disciplines, thereby increasing the level of confidence in the resulting product.

a. **Intelligence** - the product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of

---

[1] A composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander. (NTMS – NATO Agreed)

[2] AJP-2 *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security* (Not NATO Agreed)

[3] (This term and definition are only applicable in this publication)

actors, in order to identify threats and offer opportunities for exploitation by decision-makers.[4]

b. **Imagery** - collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media.[5]

c. **IMINT** - intelligence derived from imagery acquired by sensors which can be ground based, sea borne, or carried by air or space platforms.[6] The information conveyed by an image or full motion video may be clear and concise. It will often serve to support or confirm intelligence derived from other sources.

Section 3 – IMINT Objectives and Principles

IMINT OBJECTIVES

1.4. **Improve Common Operational Picture and the Recognized Environmental Picture**.[7] IMINT is a valuable part of all-source intelligence, providing detailed and precise information on the location and observable, physical characteristics of threats, infrastructure, and the physical environment. It is an important source of information to help, yet not limited

a. Determine and monitor the physical characteristics of key terrain features and patterns of life,

b. To develop and assess situational awareness, orders of battle, target intelligence, and battle damage assessments and munition effectiveness assessment, and

c. To develop assessments of adversary courses of action.

[4] (NTMS – NATO Agreed)
[5] (NTMS – NATO Agreed)
[6] (This term is a new term and definition and will be processed for NATO Agreed status)
[7] A complete and seamless depiction of geospatial, oceanographic and meteorological information designated for the planning and conduct of joint operations in a specific area at a specific time and which supports the unity of effort throughout the battlespace. (NTMS – NATO Agreed)

1.5. IMINT supports decision-making at all levels of command. It can provide a unique insight into hostile situation and the surrounding environment, and help to increase situational awareness.

a. **Accelerate decision-making process**. IMINT can accelerate the decision-making process by building a more complete and accurate picture of the current situation, thus helping reduce operational uncertainty.

b. **Support the intelligence process**. IMINT can be combined with results of other collection activities, such as human, signals, and open source intelligence, to build a robust analytical framework in support of the intelligence process.

IMINT PRINCIPLES

1.6. A key aspect in ensuring IMINT operational imperatives and interoperability are met, is to adhere to common principles. There are five principles of IMINT:

a. **Fully coordinated**. The management of collection for and production of IMINT must be fully coordinated, based on clear governance and a singular operational focus.

b. **Requirements focused**. IMINT products must be timely, responsive, and tailored to the objective, in order to ensure they are focused on the commander's critical information requirements.[8]

c. **Collection optimization**. The tasking of imagery capabilities and the storage and retrieval of collected imagery must be optimized so that imagery can be collected once and used many times. Optimization is dependent on clear guidance, knowledge of holdings, and accessibility of stored imagery.

d. **Collective effort**. The collection, processing, exploitation, and dissemination of imagery and IMINT must be a collective effort. Imagery and IMINT from all levels should be shared with all other levels of command, and nations should actively engage in cost and burden sharing and federated IMINT production.[9]

e. **Maximum interoperability and compliance**. Imagery and IMINT must be shared based on a balance of "need-to-know" and "responsibility to share". IMINT systems and networks must conform to the NATO-enabled tenets and principles, and apply standardized metadata[10] so that actionable imagery and IMINT can be shared in a timely manner, across NATO and with non-NATO partners.

---

[8] Commander's critical information requirements identify information on friendly activities, enemy activities, and the environment that the commander deems critical to maintaining situational awareness, planning future activities, and assisting in timely and informed decision-making. (AJP-3 *The Conduct of Operations*, paragraph 0416.)

[9] "An agreement amongst the participants that each will specialize in producing and sharing with the other participants IMINT products based on the type of imagery, the region, the activity of interest, or some other delineating aspect." (This term and definition are only applicable in this publication)

[10] See NATO Standardization Agreement (STANAG) 3884 - *Air Imagery Interpretation Annotation*

1.7. These principles are critical to ensure a high level of operational efficiency in all NATO IMINT support. The principles address a fundamental and universal aspect of all intelligence activities, a lack of resources (time, personnel, and capability assets) to meet all demands.

1.8. To support the processing, exploitation, and exchange of both still and motion imagery across various computer systems and applications, NATO has developed and adopted a range of imagery and IMINT standards which are listed in Annex A.

Section 4 – Characteristics, Capabilities and Limitations of IMINT

1.9. **Characteristics and Capabilities**. Imagery and IMINT can enable different aspects of the multi-source intelligence picture. In comparison to other sources/intelligence collection disciplines, such as human intelligence and open source intelligence, IMINT can be:

a. considered more precise, detailed, and accurate, as it can be geo-referenced and is based on representations of physical features/objects;

b. considered low-risk, when utilizing stand-off and/or unmanned platforms to acquire imagery (imaging systems can also be operated from space, and from concealed positions);

c. considered objective, as its source information (the imagery) is more consistently factual and less subjective;

d. used to determine change over time;

e. used and analysed in near real-time;

f. used to determine pattern of life; and

g. used to survey large areas, with up to global coverage.

1.10. **Limitations**. The utility of IMINT can be limited.

a. The time required to conduct the task, collect, process, exploit, and disseminate (TCPED)[11] steps for IMINT capabilities can be lengthy, making it difficult to ensure its availability in time to impact the decision making process.

b. The conduct of IMINT activities requires a considerable number of assets, in terms of personnel, equipment, and communications connectivity.

c. Imagery collection platforms (excluding space platforms) are limited in their ability to cover vast areas, and may not be in the vicinity of the area of intelligence interest.

d. Still imagery offers only a ‘snap shot in time.’

[11] The TCPED acronym refers to the steps of the joint intelligence surveillance and reconnaissance (JISR) process, which is explained in in detail AJP-2.7 *Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance*. TCPED is used in this publication as it better illustrates the steps imagery and IMINT agencies must undertake to collect and produce their products.

e. The capabilities of a sensor may not provide sufficient resolution to allow the detection of the object or activity in question. Resolution reduces with an increase in distance from the target object or area being imaged.

f. The specific capabilities of the sensors on an available platform, such as the part of the electromagnetic spectrum which it can collect from, can be a limiting factor when specific imagery or IMINT is required.

g. The geo-referencing of some oblique imagery may be challenging and may, alone, not be sufficient for targeting purposes.

h. Imagery collection can be hampered by:

- Space weather, weather and light conditions,
- anti-satellite weapons,
- adversary actions, such as camouflage, cover and concealment and other deception activities, and
- air defence and jamming.

i. Digital imaging systems produce enormous amounts of data, requiring robust information systems to support analysis, dissemination, exchange, storage and archiving.

j. Educating and training imagery analysts to both understand the processes within the TCPED steps and to be able to generate intelligence and brief them to decision-makers can be a long term process, requiring extensive on the job training.

k. IMINT can be susceptible to adversary deception.

Section 5 – Types of Imagery

IMAGERY FUNDAMENTALS

1.11. All imagery is produced by capturing energy from the electromagnetic spectrum. With the rise of computing power in the late twentieth century, digital sensors were developed that could directly collect electromagnetic energy and produce images. As digital sensors continued to improve, “wet film”, as the chemical process has become known, slowly declined until its use, especially for military purposes, became less prominent. Different areas of the electromagnetic spectrum have different properties, such as visual light, near infrared, thermal infrared, and radio. Digital sensors, not being limited by the characteristics of light sensitive chemicals, are able to collect across the entire electromagnetic spectrum, producing images which can be seen

immediately and stored and shared electronically. For the purpose of this section we have limited the scope to only digital motion imagery and still imagery.[12]

1.12. The enormous amounts of data produced by digital sensors often can only be processed by machine logic (algorithms). Imagery analysts may have to rely on automated recognition software, without having a clear understanding of how the algorithm works. Commanders must be aware that the failure to exercise due diligence to ensure that automated recognition software is suitable for its intended purpose and functioning properly could result in unintended casualties and subject the responsible commander to personal liability.

1.13. **Digital imagery**. Digital images can be created by capturing electromagnetic energy from any part of the electromagnetic spectrum. Each image is made up of pixels, which project the attributes of the image, such as colour and brightness. Imagery from handheld devices can provide very high resolution as the lenses can often be changed. Radar images can be created in most weather conditions, but are more difficult to interpret than visible light images.

1.14. **Digital motion imagery**. Motion imagery is an important complement to still imagery. Motion imagery sensors collect a sequential or continuous stream of still images that enable observation of the dynamic behaviour of objects within the scene. The temporal rates of motion imagery, which are nominally expressed in frames per second, must be sufficient to characterize the desired dynamic phenomenon. While measurements can be made in motion imagery, it is normally easier to make them in still images. Full motion video falls within the context of these motion imagery standards and is nominally collected at, or above, 24 frames per second. Full motion video is better for detecting motion and correctly identifying activity than still imagery. This results in improved contextual and situational awareness.

1.15. Imagery can be collected using a variety of platforms. These may be military, either dedicated or multi-use, or civilian. Platforms typically used for imagery collection are:

a. satellites;

b. manned and unmanned aircraft;

c. ships, submarines, and unmanned/unattended maritime systems;

d. land vehicles and unmanned/unattended ground systems; and

e. handheld cameras.

1.16. **Sensor orientation**. The orientation of the imaging sensor, both for still and motion imagery, has significant implications for the characteristics of the resultant images, and as a result what IMINT can be produced from the image. Sensor orientation can affect the characteristics of the resulting imagery.

[12] Throughout the remainder of this publication motion imagery will always be referred to as either motion imagery or video. The term imagery will be used for all forms of imagery in the collective sense, as well as still imagery, unless for clarity the word ‘still’ needs to be included.

a. **Vertical**. Vertical imagery is taken from a point directly above and with the sensor angled directly towards the target location. Vertical imagery has the following characteristics.

(1) It generally has a constant scale which is relatively simple to calculate[13].

(2) It is similar to a map, making it is easy to compare the two and to take measurements, although the complete similarity with a map can only exist when the aerial/space imagery has been geometrically corrected.

(3) It has no 'dead ground' (where terrain relief causes areas to be obscured from a given vantage point) and targets are normally visible unless obscured by overhead cover.

(4) The vertical view is less familiar, and therefore may be more difficult to interpret.

(5) For a given sensor height, the area of ground covered in the image is less than for an oblique image.

(6) It requires that the sensor be placed directly over the target, which may put the sensor platform in danger of being lost due to adversary fires.

(7) The more oblique the image, the less detailed it will be (spatial resolution decreases as obliquity increases).

b. **Oblique**. The majority of imagery is oblique. Oblique imagery is either high oblique (when the horizon is visible in the image) or low oblique (when it is not). Oblique imagery has the following characteristics.

(1) When taken from the same altitude, oblique images provide greater ground coverage per image than vertical images.

(2) Oblique images present a more common perspective, aiding in the recognition of targets, equipment, activities and features.

(3) The collection platform is able to stand off from non-permissive areas and can collect across international borders.

(4) The scale of oblique imagery is not constant across the image, making it more difficult to measure and geo-reference accurately.

(5) Tall objects may obscure smaller ones and terrain relief can result in dead ground.

(6) Haze is more of a problem with oblique images than with vertical images taken from the same altitude since the distance to the target is greater.

(7) The more oblique the image is, the less detailed it will be (decreasing of the spatial resolution with the increasing of the obliqueness angle).

[13] Image scale will change towards the edges of the image frame.

c. **Stereo imaging**. A stereo image is created by viewing a target area from two vantage points. Stereo imagery is based on the parallax difference between two images, allowing the viewer to see a three-dimensional (3-D) representation of the area imaged. Stereo imagery requires an overlap, normally sixty percent of the image area. The sense of depth given to images using stereo is not only a useful tool to aid imagery exploitation, but can also be invaluable for inter-visibility and dead-ground studies. Stereo imagery has the following characteristics.

(1) Stereo imagery is vital in producing mensurated height coordinates and latitude and longitude coordinates in support of targeting. It is also essential for accurate production of digital elevation and 3-D models.

(2) Stereo imagery can sometimes assist in detecting activity both in wooded and in urban areas, and in revealing camouflage, concealment, and deception measures.

(3) Viewing stereo imagery requires specific hardware and software solutions, which can be costly.

(4) Collection of imagery for stereo viewing and exploitation requires specific planning.

(5) Correctly viewing stereo imagery is an acquired skill and requires analysts to have normal stereo vision acuity.

d. **Panoramic imagery**. Panoramic imagery comes from sensors with a very wide angle of view or stitching views. Panoramic imagery can be vertical and oblique (horizon to horizon), but is normally only oblique. Panoramic imagery has the following characteristics.

(1) Panoramic imagery covers a very wide area with each image.

(2) The scale in the imagery varies widely and is difficult to measure accurately.

(3) The very wide angle of view makes the imagery more difficult to analyse since it does not correspond to the human field of view.

IMAGERY CHARACTERISTICS

1.17. **Electro-optical (EO) imagery**. EO imagery refers to the collection of electromagnetic energy from the visual, near infrared and or thermal infrared parts of the electromagnetic spectrum. EO sensors are passive, only collecting electromagnetic energy emitted by or reflected off the target itself. That said, it is common to refer to the sensors that collect from the visible light spectrum as EO sensors, and the other sensors as infrared and thermal sensors.

a. **Visual imagery**. Imagery from sensors that capture the visible parts of the electromagnetic spectrum will either be in grayscale or colour. Colour imagery adds a dimension to the analysis, and is more easily interpreted since the

images resemble what we see naturally. As with the human eye, EO imagery can be degraded or obscured by dust, smoke, haze, cloud, rain, fog, sun-reflection, light level, and angle of illumination. While colour imagery may add an additional dimension to the analysis, and may be more easily interpreted since the images resemble what we see naturally, greyscale imagery often provides high resolution.

b. **Infrared imagery**. Near infrared, infrared band II, and infrared band III[14] imagery captures reflected energy in the infrared waveband. To assist imagery analysts in identifying different types of objects when reading infrared images, algorithms are used to present capture energy in different colours than they appear in the visible light spectrum. In this way green camouflage and healthy green vegetation are presented to the analyst in different colours. Infrared sensors are excellent for collection at night and periods of very low illumination, but exploitation requires advanced technical tools, and education and training.

c. **Thermal infrared**. Thermal infrared imagery captures a target's radiant temperatures. Thermal infrared is used to measure the temperature differences between terrain features and surrounding objects on the ground, producing a near-optical quality image. Thermal imagery complements visual imagery by day, and they are commonly used together to locate and identify objects not readily noticeable in either the EO or thermal alone. Thermal imagery can observe the heat shadow left on a heat-absorbing surface before an object was moved or the thermal scar created by heat-generating object before it was moved. Based on the shape of the shadow or scar, it may be possible to determine what the object was. With training, imagery analysts can also identify objects based on their thermal signature, or the activity that is occurring in the image.

d. **Spectral imagery**. Spectral imagery is divided into multi-spectral imagery and hyper-spectral imagery, the difference being the number of spectral bands or frequencies that can be collected simultaneously. Each band is collected as a separate image, or scene, which are then used for comparative analysis. Every surface or target gives off its own distinctive pattern of radiation, made up of different electromagnetic frequencies, whether it is generated by itself or reflected. The exploitation of spectral imagery is greatly dependent on having a library of these spectral signatures. Spectral imagery usually has less resolution than visible EO imagery, but can reveal details not apparent with other sensors, and it has the capability of providing map-like products to support area familiarization and orientation.

e. **Advantages of EO imagery**.

[14] The three infrared bands are sometimes referred to as near, mid, and far infrared.

(1) Other than visible light and near infrared EO systems, all other EO systems generally operate day and night, and under most weather conditions.

(2) When used together, EO systems are generally effective at detecting concealed elements within the environment.

(3) Being passive, EO systems are very difficult to jam or disrupt.

f. **Limitations of EO imagery**.

(1) Thermal infrared is less effective for the identification of targets during day/night transition periods and when backgrounds and targets have the least difference in temperature.

(2) Camouflage and dummies can limit effectiveness of single EO systems.

(3) Other than visible light EO systems, the exploitation of all other EO systems requires advanced technical tools and/or training (education on systems limitations).

(4) Global positioning system receivers embedded in EO systems might be jammed or disrupted by spoofing.

1.18. **Radar imagery**. Radar is an active collection system that, depending on the power and frequency of the transmitter, can penetrate virtually all atmospheric conditions. Radar imagery generally is limited only by the capability of the platforms conducting the collection mission. Radar operates on the principle that all materials reflect a portion of the electromagnetic radiation directed at them and that the distance from the antenna to the target can be measured based on the time it takes for the signal to travel to the target and back. There are two types of radar imagery, synthetic aperture radar and moving target indicator imagery.

a. **Synthetic aperture radar** is a form of radar characterised by the use of relative motion between the transmitting antenna and the receiving antenna. Synthetic aperture radar therefore usually offers better standoff resolution compared with other imagery systems. Operating obliquely at high altitude, synthetic aperture radar can provide extensive area coverage and excellent stand-off ranges, permitting the platform to operate over friendly areas while imaging hostile territory. Several hundred thousand square kilometres can be covered by a synthetic aperture radar system during a single sortie, but at the expense of scale, ground resolution, and the identification of individual items of equipment. Interpretation can be almost near real-time if a data downlink is used. When it is compared with previously acquired synthetic aperture radar coverage, using techniques such as interferometry (e.g. coherent change detection), radar stereoscopy (radargrammetrics), or polarimetry more intelligence concerning target status and activity can be obtained.

b. **Moving target indicator imagery** is derived from a radar technology that employs the principle of Doppler shift to filter out stationary objects. The image

is produced by plotting a series of radar sweeps, thus showing the path of movements and allowing for the calculation of speed. The number of targets that can be tracked by a moving target indicator system is limited only by the software and computing power of the system. Moving target indicator is the best sensor for detecting on-going movement.

c. **Advantages of radar imagery**.

(1) Radar systems can penetrate fog, haze, clouds and smoke, but can be limited by severe precipitation, terrain elevation and sand storms. Additionally, space weather can interfere with radar signals, causing false returns or false targeting.

(2) Radar systems provide extensive area coverage.

(3) Radar systems can operate day and night.

(4) Radar systems provide good standoff capability and are good sensors for detecting change.

d. **Limitations of radar imagery**.

(1) Analysis of synthetic aperture radar is not intuitive and better results are possible when imagery analysts are adequately educated, well trained, familiar with the subject targets, and have access to previous visual or infrared images of the area.

(2) Synthetic aperture radar provides continuous strip imagery which makes stereo viewing of the imagery only possible under exceptional circumstances.

(3) Synthetic aperture radar is also an active system, in that it transmits energy which can be detected and locked into, which may present an operational limitation.

(4) Radar systems are susceptible to jamming and deception.

1.19. **Light detection and ranging**. Light detection and ranging (LIDAR) sensors are similar to radar, but transmit laser pulses instead of radio waves, and can be integrated into airborne platforms. LIDAR can be used to measure shorelines and beach volume changes, shallow water depths (0-50 meters), conduct flood risk analysis, identify water flow issues, and augment transportation mapping applications. LIDAR supports large-scale production of high-resolution digital elevation products displaying accurate, highly detailed, 3-D models of structures and terrain making it invaluable for operational planning and mission rehearsal. LIDAR has similar advantages and disadvantages as radar, except it is susceptible to weather conditions.

1.20. **Commercial imagery**. Commercial imagery is not a type of imagery, but rather a source. Unlike imagery available through open source collection, commercial imagery providers can provide an increased capability to supplement and complement military

imagery collection, by providing tailored imagery products. Commercial imagery providers can produce images from across the electromagnetic spectrum (such as EO, infrared, thermal infrared, and radar images). Most commercial imagery acquired by NATO comes from satellites. The commercial imagery industry continues to expand and in many fields, they have very advanced imaging capabilities. The primary benefit of utilizing commercial imagery is its unclassified nature. Commercial imagery and its resultant IMINT products can be shared with a wide range of customers and colleagues, unless classified information is overlaid, or the purchase agreement limits its use or redistribution. However, when purchasing commercial imagery confidentiality is not guaranteed, therefore, operations security must be considered before requesting commercial imagery, as the simple act of asking for imagery of a specific region may forewarn adversaries of NATO`s intentions. Furthermore, the integrity of the information contained in a commercial image is not guaranteed as the pixels and their digital values can be manipulated before delivering the image. The purchasing of commercial imagery by NATO must follow approved policies and procedures. Nations, having their own policies and procedures, may also acquire commercial imagery in support of NATO operations.

Chapter 2 - IMINT and the Intelligence Cycle

Section 1 – Introduction

2.1. The intelligence cycle is the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available for users.[15] The systematic exploitation of all sources of information is an essential part of the intelligence cycle. The activities are divided into four phases: direction, collection, processing, and dissemination, as shown in Figure 1. While the intelligence cycle outwardly appears a simple process, in reality its activities are complex and it comprises many simultaneous cycles operating at different levels and speeds. Some activities can overlap while others may coincide so that they are conducted concurrently, rather than sequentially.

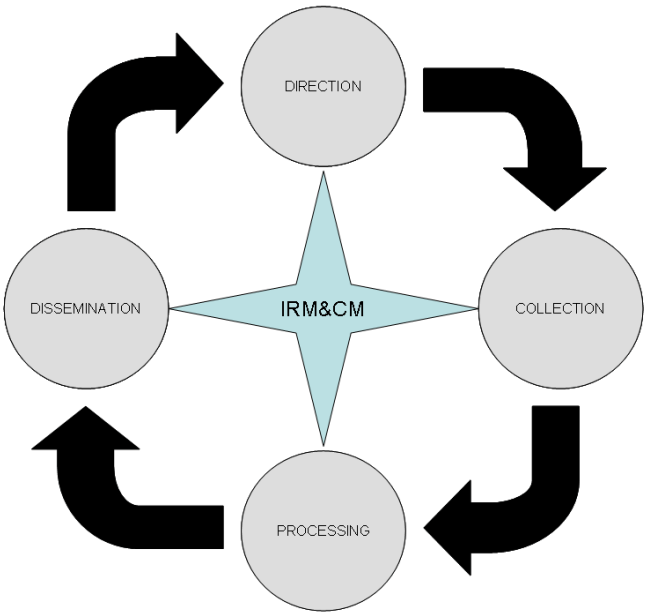

Figure 1 - The Intelligence Cycle

[15] This term and definition modifies an existing NATO Agreed term and/or definition and will be processed for NATO Agreed status.

Section 2 – Direction

2.2. IMINT is an important contribution to the multi-source intelligence that commanders require for their decision-making process. Commanders prioritize their intelligence requirements and direct their CJ2s by clearly articulating their commander's critical information requirements and identifying those priority intelligence requirements which are essential to their planning process. From the commander's direction, the CJ2 determines how the intelligence requirements are to be met and what information and intelligence is required to answer them. This information is included in the intelligence collection plan and subsequently tasked to the appropriate capabilities and agencies[16] via the joint intelligence, surveillance and reconnaissance (JISR) collection and exploitation plan. This involves actions to:

a. task agencies, units, and/or collection capabilities, where appropriate, and coordinating their activities to collect the necessary information;

b. monitor intelligence collection, processing, exploitation, and dissemination (PED) to ensure that the intelligence requirements are being satisfied;

c. ensure that intelligence activities are conducted in a timely manner, and when delays occur, ensure that collectors and PED capabilities are re-tasked and re-prioritised, as required;

d. ensure that IMINT activities are conducted legally, considering that some collections means and methods, as well as sources of imagery, and therefore IMINT, may be subject to legal restrictions in certain jurisdictions (e.g. copyrights or license restrictions, if from commercial sources, privacy legislation with respect to property and the person (biometrics) and by international/national laws);[17] and

e. ensure that NATO arrangements for the sharing and protection of IMINT, such as NATO security and release and disclosure directives are respected.

2.3. The direction[18] phase of the intelligence cycle is a continuous, iterative, and dynamic set of activities supported by the intelligence requirement management and collection management (IRM&CM) processes,[19] as depicted in Figure 1. It ensures identification and articulation of intelligence gaps and matches them with available collection and PED capabilities. It ensures identification and articulation of intelligence gaps and matches them with available and appropriate collection and PED capabilities. The

[16] NTMS – NATO Agreed.
[17] See MC 0596. *NATO Imagery Intelligence (IMINT) Policy,* 05 May 2011.
[18] "The determination of intelligence requirements, planning of collection effort, issuance of orders and requests to agencies and maintenance of a continuous check on the productivity of such agencies." This term and definition modifies an existing NATO Agreed term and/or definition and will be processed for NATO Agreed status.
[19] For more information on the IRM&CM processes, refer to AJP-2, Chapter 5 and AJP-2.7.

five steps of the JISR process (TCPED) over laid on the intelligence cycle is illustrated in Figure 2.

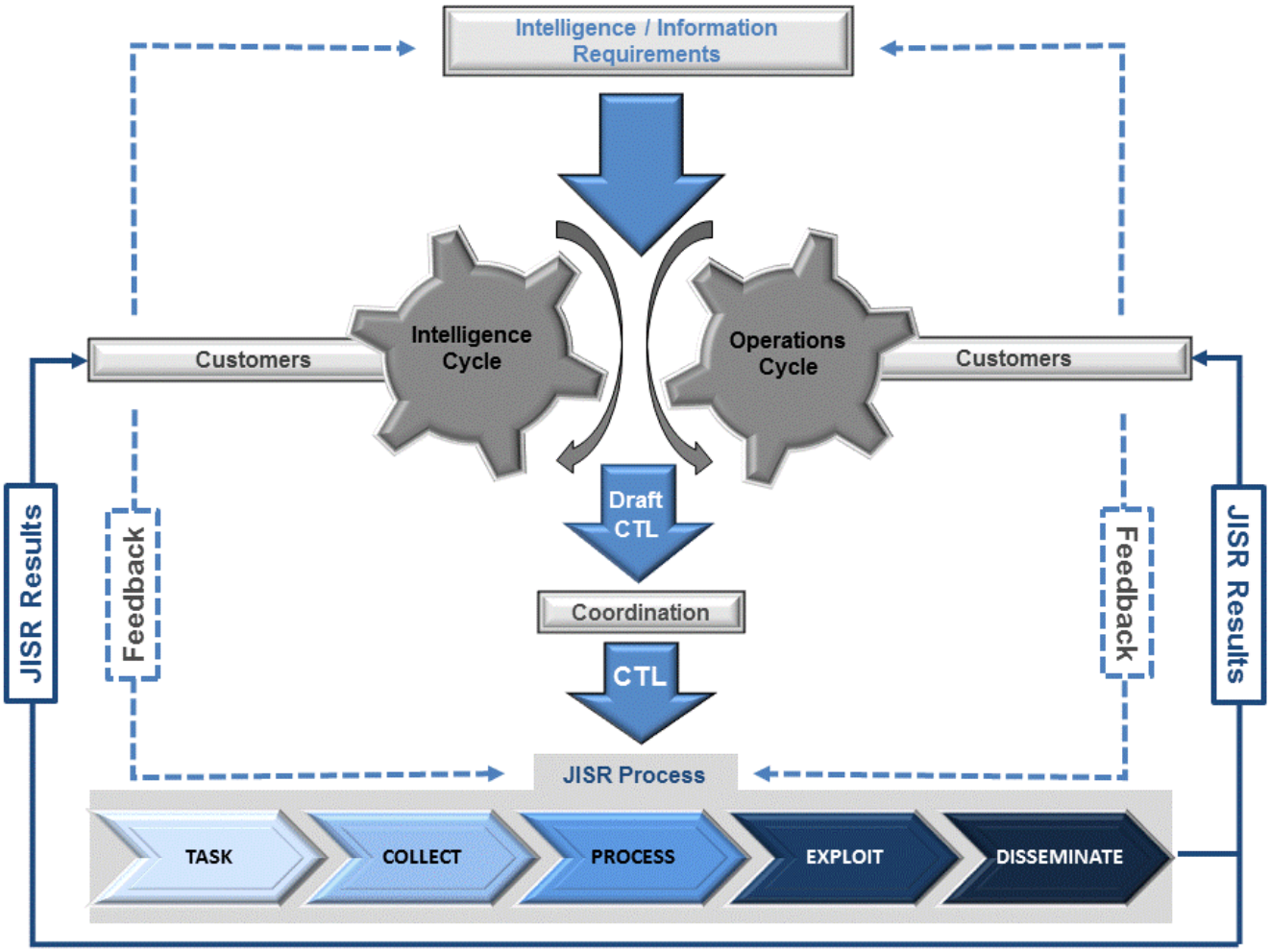

Figure 2 - The Relationship of the JISR Process to the Intelligence and Operations Cycles[20]

2.4. The IRM&CM process combines intelligence requirements from the JIPOE, planning and operational areas into a single set of prioritized requirements. The tasking of imagery collection and IMINT PED capabilities is coordinated with other disciplines in a manner that allows for mutual and de-conflicted support, and the cross-cueing at both the sensor and capability levels. When different platforms and sensors are available for collection, consideration must be given to their specific characteristics and potentially using more than one sensor or platform to increase the probability of extracting useful information (i.e. in support of technical analysis of the target, determining target activity, identification of camouflage, etc.). Collection management

[20] CTL: Candidate Target List

staffs should have an adequate understanding of imagery collection and IMINT PED capabilities, limitations, and tools to ensure they can effectively task both collection and PED agencies.

2.5. Imagery collection systems and sensors supporting the force may be airborne or ground, maritime, or space-based and may be able to operate across the area of intelligence interest, in day or night and all-weather conditions. In addition to possible organic NATO commanded capabilities, the force will usually be supplemented with additional JISR capabilities allocated from troop-contributing nations.

2.6. The IMINT specialists on the IRM&CM staffs select collection capabilities according to suitability and availability rather than the command relationship. For tasks involving complex targets, or the possibility for camouflage, concealment, and deception techniques, multiple collection capabilities may be necessary to answer a single intelligence requirement. The IRM&CM staff, having determined which capabilities best suit the tasks, works collaboratively with the CJ3 staff to ensure the JISR collection and exploitation plan supports the intelligence collection plan.

2.7. Some IRM&CM staffs will have tasking authority over declared collection capabilities and the ability to request assistance, either directly in theatre or via reach-back, from agencies such as the MoU organisation of the NATO Intelligence Fusion Centre (NIFC), the NATO Command Structure, or from national intelligence cells of supporting nations. It is essential that standard operating procedures capture and accurately describe where these responsibilities lie.

2.8. Tasking capabilities under command is relatively straight forward.[21] When the collection is achieved by national systems that are not under NATO control, special arrangements may have to be put in place based on the sharing/support arrangement with the nation. In these cases a nation can act as one or more of the following.

a. **IMINT provider**. A request can be addressed to the nation to provide IMINT products.

b. **Imagery provider**. The request will be to provide imagery for exploitation by NATO elements or declared national elements.

c. **Capability provider**. A request will seek support from a national system, resource or of a specific capability (e.g. user ground segment for a satellite system). It is usual for such support to be made available through a memorandum of agreement or similar agreement.

2.9. The amount of imagery that can be collected is rapidly increasing with the introduction of new technologies. Exploitation resources however remain limited, and when there is growth it is generally slower. A balance therefore needs to be struck between what can be collected and what is feasible to exploit. For deployed forces, the tasking of

[21] Capabilities embedded in, or organic in, subordinated units/detachments will not be tasked directly but through taskings and orders to the unit which controls them. The tasking is then the responsibility of the commander in charge of those units/detachments.

the strategic reach-back or federated capabilities to help with exploitation may be a solution. If the NIFC is tasked with non-time critical PED requirements, deployed operational and tactical level PED capabilities are able to handle more immediate tasks.

2.10. When developing tasks, either for capabilities under command (which can be tasked directly) or for external support, it is essential that the task be accurately defined. Before issuing tasks or requests, an IRM&CM staff should:

a. confirm that usable imagery and current imagery that satisfies the intelligence requirement is not already held in storage before requesting new collection take place, and if such imagery exists either provide to the requester or task an exploitation asset to complete the requested single-source intelligence products;

b. verify that collection can and will be supported by adequate PED resources;

c. ensure that any tasking complies with prioritization guidance;

d. specify all aspects of the mission that must be taken into account (e.g. timings, data-transfers, exploitation, product creation and dissemination);

e. take into account the availability of resources to ensure selection of the best available platform and sensor, in consideration of such factors as:

(1) the characteristics of available capabilities (e.g. reactivity, reliability, revisit time, security, etc.);

(2) ensuring that imagery collected is suited to support a product that can answer the original requirement; and

(3) threats to, and opportunities offered by, available platforms and sensors; and

f. ensure that the essential elements of information are sufficiently detailed to allow imagery analysts to answer the requirement. Essential elements of information should contain:

(1) only those aspects necessary to answer the specific requirement, and if appropriate, the underlying intelligence requirement can be included so that essential elements of information can be viewed in context;

(2) identification of the named area of interest to ensure both collection and exploitation are focused;

(3) any unique indicators or collateral information that may be needed to identify specific activities; and

(4) the reporting requirements, clearly laid out, in terms of time and format.

Section 3 – Collection

2.11. Collection, "the exploitation of sources by agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence,"[22] is the second phase of the intelligence cycle. During the collection phase, the tasked JISR capabilities and agencies, both collection and PED, plan, order, and execute the tasks assigned to them. The collection phase of the intelligence cycle therefore incorporates the collect, process, exploit, and disseminate steps of the JISR process.[23] The collection phase is concerned with how imagery collection and PED operations are managed and how IMINT is provided to multi-source analysts for intelligence production, or when so tasked, directly to the requester.

2.12. Execution in the collection phase is decentralized to collection agencies, which directly task and manage their capabilities, platforms or sensors, and to PED agencies. For example, tasks for unmanned aircraft collection platforms are sent to the agency "unit" that flies them, and the unit plans and conducts the collection missions. Once the imagery data has been collected, or as it is being collected, it is processed[24] into a useable format, and it is passed to the tasked exploitation agencies, which conduct the required exploitation, produce the requested IMINT product, and disseminate the result to the requester.

2.13. The processing and exploitation of imagery, which is conducted according to the collection and exploitation plan, may be conducted by the agency that collected the imagery, by a dedicated IMINT production agency, or by imagery analysts in and a multi-source agency. Imagery exploitation is driven by the specified collection requirement, the supporting essential elements of information, and by the time by which the IMINT is required.

2.14. The initial level of imagery exploitation involves the rapid and preliminary assessment of the collected imagery and the immediate forwarding of the results to the commander and/or requester, in as short a time frame as exploitation permits in support of current operations. This level of imagery exploitation is usually conducted by the sensor operator or an imagery analyst associated with the imagery system, but can also be undertaken by other imagery analysts having near real-time access to collected imagery. The exploited data and information are transmitted for further exploitation within the JISR process and the intelligence cycle. The initial level of imagery exploitation is short term in nature and is primarily conducted for the tactical user, consisting of short term analysis, and results in single-source intelligence answers to the given essential elements of information. The initial level of imagery exploitation generally results in what is referred to as phase 1 reporting, which

---

[22] This term and definition modifies an existing NATO Agreed term and/or definition and will be processed for NATO Agreed status.

[23] For more information on the JISR process, see AJP-2.7.

[24] Process, in this context refers to JISR Process step, the conversion of collected data and information into appropriate readable or useable formats that enable further exploitation, storage, or dissemination. For more information on the JISR process, see AJP-2.7.

requires that a response be produced within very short period of time (i.e. within 2 hours).

2.15. The second level of imagery exploitation involves a more detailed evaluation of the collected imagery, in accordance with exploitation tasking. This level of imagery exploitation can be conducted by imagery analysts associated with the imagery collection capability, but may also be conducted by imagery analysts located at dedicated IMINT facilities, either deployed or via reach-back. IMINT results from this level of exploitation may be disseminated directly to the commander/requester when so tasked, forwarded to another imagery exploitation agency for more in-depth exploitation, or to multi-source intelligence agencies for use in the production of multi-source intelligence. Imagery exploitation at this level, is still relatively time sensitive (a matter of hours or a day) and may involve the use of multiple sources of imagery to produce the answers to the given essential elements of information. The second level of imagery exploitation generally results in what is referred to as, phase 2 reporting, which requires that the response still be timely in a tactical sense (same day), but allows for fuller exploitation, and a more detailed response.

2.16. The third level of imagery exploitation involves using imagery from multiple imagery collection capabilities, and imagery collected over an extended period of time, and may include archived multi-source intelligence. This level of imagery exploitation often requires tools, processing power, and/or additional specific expertise. It can be time consuming and may be conducted within the joint operations area or via reach-back capabilities. Imagery exploitation at this level is long term in nature and is primarily conducted to support strategic level decision makers. The result of exploitation at this level is typically based on multiple sources of intelligence, to answer the essential elements of information and to create long-term detailed intelligence, such as trend analysis. IMINT products from the first and second levels of exploitation are generally incorporated into the third level IMINT products. The third level of imagery exploitation generally results in what is referred to as, phase 3 reporting, which requires that the response focuses on the completeness of the answer rather than the speed of the reporting. For example it may be a long or strategic view of a particular target, facility, or area. It can also show a long term and in depth understanding of the target informed by long periods of observation and analysis.

2.17. As the last step of the JISR process and the collection phase, processed and exploited imagery products are disseminated. Imagery and IMINT must be disseminated in time and in the format required to meet the needs of those who requested it, if its value is to be fully realized. The dissemination means and times depend upon the JISR and intelligence architectures, and the needs of those who requested the imagery and or IMINT. While some imagery and IMINT is required to be disseminated to the user in near real-time, all imagery and IMINT must be saved in databases, and made available to multi-source intelligence production agencies.

2.18. Sometimes the commander’s intelligence requirement can be satisfied simply by providing an annotated image, or by streaming motion imagery into the joint

operations centre. In these situations the JISR process shortens and shifts the exploitation step in order to move the product directly from the collection agency to the requester. Shortening or shifting the exploitation step is not without risks, and the CJ2 must be prepared to answer questions that may arise when the end user is given single-source imagery information directly from the collection agency. Operational decisions based on unevaluated or partially evaluated information should be avoided. There are also occasions when the commander's intelligence requirements can be satisfied with a textual report based on imagery analysis. A textual report can often be produced and transmitted much faster than an image and may avoid the problems associated with untrained analysis of raw imagery

Section 4 – Processing

2.19. Processing, "the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation,"[25] is the third phase of the intelligence cycle. During this phase of the intelligence cycle, IMINT is fused with other single-source intelligence and pre-existing on-the-shelf or multi-source intelligence to produce multi-source intelligence. The production of IMINT based multi-source intelligence may be conducted by the agency that initially exploited the collected imagery, a dedicated IMINT production agency, or by imagery analysts in multi-source agencies. IMINT based multi-source intelligence production, like all intelligence, is driven by the details of the taskings generated in the direction phase of the intelligence cycle, such as, that specified priority intelligence requirements and the supporting essential elements of information, and by the time by which the multi-source intelligence product is required.

Section 5 – Dissemination

2.20. Dissemination, "the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it,"[26] is the fourth, and last, phase of the intelligence cycle. While imagery and IMINT are initially disseminated[27] as the last step of the JISR process, within the collection phase of the intelligence cycle, the dissemination phase of the intelligence cycle still has a role to play in the management of imagery and IMINT products.

2.21. The CJ2 must ensure that all acquired imagery and IMINT is stored or archived such that it is lawfully able to be replicated, is easily retrievable, and follows the principle of "collect once – use many times." This not only allows and supports re-use, but also adds to the basic intelligence data base and may contribute to or help provide needed substantiation, and minimum requirements for approval, of activities like targeting.

---

[25] (This term and definition modifies an existing NATO Agreed term and/or definition and will be processed for NATO Agreed status)

[26] This term and definition modifies an existing NATO Agreed term and/or definition and will be processed for NATO Agreed status.

[27] Disseminated, in this context refers to the JISR Disseminate step, the timely provision of JISR results to those who need it, in the requested format, and through the communication means as specified by the JISR task. For more information on the JISR process, see AJP-2.7.

Archives may be off-line, but must allow search and retrieval within a reasonable timeframe.

2.22. Release and sharing of imagery and IMINT on the basis of “responsibility-to-share” is an important consideration in NATO operations. Nonetheless, commanders and CJ2s must be aware that some NATO nations may have policies and or laws which will preclude them for sharing all collected imagery and produced IMINT with some or all NATO allies, or with NATO partners.

2.23. Common sense is critical when creating local policies for imagery data storage and for NATO operations, the archival policy will be specified in the intelligence annex of the OPLAN. Some imagery missions produce large amounts of data, not all of which is useful. Imagery should be stored for as long as it is considered to have further value. If imagery needs to be deleted or archived then a review should take place to identify the imagery which is least likely to be of future use. This review should be carried out by appropriately trained staff from the agency, unit, or nation that owns or produced the data store. The review should also consider any national legal requirements or restrictions on the deletion or archiving of collected imagery. Imagery storage policies and procedures must be a part of an organization’s information management plan. Storage policies should be reviewed, and if necessary, updated on a regular basis. Nations should make available details of all relevant and releasable imagery through a catalogue which should be placed on NATO accessible systems along with a means to allow the imagery to be retrieved.

INTENTIONALLY BLANK

Chapter 3 - IMINT Support to NATO Operations

Section 1 – Introduction

3.1. NATO IMINT organizations must be prepared to operate under the same conditions and at the same levels as the deployed elements they support. Additionally, it must be realized that small unit leaders and their subordinates require intelligence as much as commanders at higher levels. Small units may require IMINT to accomplish their missions. Operational commanders may require IMINT to plan and oversee the execution of operations.

Section 2 – IMINT Support to NATO by Nations

3.2. NATO operations are intended to be conducted primarily using the resources contributed by the nations participating in the operation. Nations have the following responsibilities in regard to the conduct of IMINT activities.[28]

a. Provide the necessary IMINT support to their forces, coordinated, as appropriate, with NATO. This includes the provision of imagery support to their forces participating in an Enhanced NATO Response Force.

b. Collectively, provide the IMINT support necessary to meet NATO's intelligence requirements and NATO's imagery collection operations.[29]

c. Ensure that the capabilities they provide meet the minimum standards for interoperability and that the NATO command structure is informed of any particular capabilities or limitations.

3.3. **National Intelligence Cells**. NATO nations may retain direct national command and control (C2) of intelligence collection and production capabilities, including IMINT capabilities, operating in support of NATO so that their deployed national commanders can have direct access to national intelligence support. Operational-level national intelligence cells are under national C2 and may be attached to a permanent or deployed NATO headquarters (HQ). They provide a means for direct and timely exchange of intelligence with the NATO HQ and other troop contributing nations and should be considered part of the routine NATO HQ lay down.

Section 3 – Levels of IMINT Support

3.4. IMINT is valuable at all levels of command, particularly during the planning process, as it can provide unique intelligence and is particularly important for viewing denied areas. NATO categorizes three levels of command and operations: strategic,

[28] See MC 0596. *NATO Imagery Intelligence (IMINT) Policy,* 05, May 2011.
[29] See AIntP-11 *Intelligence Training*, which identifies standard, basic, and advance imagery specialist training requirements for NATO.

operational, and tactical. Intelligence is also categorized in these same levels. The IMINT contributes to each of these levels.

a. **Strategic intelligence**. Strategic intelligence is, intelligence required for the formation of policy, military planning and the provision of indications and warning, at the national and/or international levels.[30] Strategic-level imaging platforms generally include platforms operating at a high altitude and in space. Strategic imagery and IMINT can support:

(1) international military planning;

(2) provision of indications and warning;

(3) treaty verification;

(4) mapping;

(5) military contribution to humanitarian assistance and disaster relief; and

(6) crisis response management.

b. **Operational intelligence**. Operational intelligence is, intelligence required for the planning and conducting of campaigns at the operational level.[31] Operational IMINT helps develop the commander's understanding which assists in decision-making, and focuses on the capabilities and intentions of actors and hazards in the area of operations in support of joint targeting. Imagery collection platforms at this level operate from inside or outside the area of operations, but are in direct support of operational-level commanders. Operational-level imaging platforms generally include aircraft operating at high altitude. Aircraft with targeting pods are also valuable, although non-traditional, imagery collection capabilities.

c. **Tactical intelligence**. Tactical intelligence is, intelligence required for the planning and execution of operations at the tactical level.[32] Tactical IMINT focuses on the location, status, composition, activities and movements of adversary forces to permit tactical commanders to achieve a particular short-term mission, task or action. Imagery collection platforms at this level generally include aircraft operating at low or medium altitude as well as small unmanned aircraft system, vehicle/ship mounted surveillance systems, and handheld cameras. Among ground forces these are normally integral or organic to tactical units and formations and under command of tactical commanders.

[30] (NATO Agreed)
[31] (NATO Agreed)
[32] (NATO Agreed)

Section 4 – IMINT Support by Operational Stage

3.5. Intelligence support to operational-level commanders is critical. Campaigns and operations normally happen in a logical order, however; successive stages may overlap or occur in parallel. Operations are conducted on different levels at the same time. IMINT, as a key intelligence discipline, supports and enables a multi-source approach to building the required intelligence picture during all stages of a joint operation.

3.6. **Operations planning and Joint Intelligence Preparation of the Operating Environment (JIPOE)**. Joint intelligence preparation of the operational environment is the methodology used by joint and component-level intelligence directorates to provide an understanding of the threat and operating environment in support of the operational planning process. IMINT analysis is a key instrument for indicators and warning as it denotes changes that occurs in a defined timeframe. Imagery and IMINT enables analysts to view key preparations on the ground in preparation to possible future operations by adversary forces. One of the main outputs of this process is identification of places where friendly or adversary forces can influence events and opinions through lethal or non-lethal means. Satellites, stand-off platforms, and exploitation personnel all contribute to providing IMINT of denied or remote areas. National imaging systems can provide classified, timely, high-resolution, IMINT to complement available commercial satellite imagery. When combined with geospatial information, the products can describe a variety of environmental aspects. To ensure this, close cooperation is needed with supporting geospatial teams.

3.7. **Preparation of the force and deployment**. As the force assembles, IMINT supports situational awareness and contributes to the continuing development of knowledge on unfolding events, thus helping the commander update plans, and inform the force of the situation they are about to face. Strategic and operational imagery collection capabilities continue their efforts to identify key adversary capabilities and environmental characteristics that may have an impact on force composition and training requirements.

3.8. **Deployment of the force**. As the deployment of the forces becomes more imminent, subordinate commanders at the operational and tactical level will have more specific requirements for detailed intelligence and information on the area of operations. These intelligence requirements are often issues such as:

a. physical aspects of air fields and installations;

b. physical aspects of ports and port facilities;

c. the condition of land entry routes, including adversary positions and obstacles;

d. the availability and location of key resources, such as gravel; and

e. enemy locations and disposition.

3.9. It is important to note that in the event of deployment within a NATO state (e.g. in response to an Article V response), tasking of NATO intelligence assets to collect and analysed imagery of ports airfields and facilities in a NATO Allied state will be highly problematic and may not be the best way to provide the required information. The J4 should simply ask their counterparts for the data instead.

3.10. **Execution of operations**. During this stage, IMINT focuses on supporting specific operational and tactical functions such as:

a. **Joint targeting**. IMINT provides visual identification and coordination of target elements from a system, critical nodes, and high-value and high-payoff targets in support of targeting. Mensuration of high resolution imagery is essential for the production of precise geo-coordinates which support the employment of precision weapons, and for the estimation of collateral and additional damage. IMINT also contributes to the combat assessment (Battle damage assessment and munition effectiveness assessment) of actions taken against the selected targets.

b. **Battlefield surveillance**. IMINT is a key aspect of all indications and warning and force protection operations. It helps provide early warning of potential hostile action. Tactical platforms are the main effort in much of the force protection effort. For example, NATO Alliance Ground Surveillance capabilities will give commanders a comprehensive picture of the situation on the ground and will be tasked to provide synthetic aperture radar/moving target indicator sensor capability to deployed elements.

c. **Monitor adversary activity**. IMINT aids in monitoring adversaries to determine their situation, force posture, and dispositions relative to friendly forces, to demonstrate physical relationship or networks, and to determine activity patterns and measure reactions to friendly combat operations.

d. **Contingency planning**. During the execution of the mission, IMINT will continue to support planning efforts for future operations. This will greatly test the IMINT concept of support and will require a coordinated, prioritized and layered approach to the employment of joint intelligence surveillance and reconnaissance (JISR) platforms.

3.11. **Operation termination and transition**. Support to this stage requires a refocus from operational and tactical IMINT support to operational and strategic support. IMINT can provide intelligence for:

a. treaty verification;

b. assessment of campaign goals and measures of effectiveness;

c. the transition to stability operations; and

d. assessments of population displacement and support to relief efforts.

3.12. **Redeployment of the force**. Similar to the “deployment of the force” stage, IMINT will shift its effort to support force protection and logistical requirements associated with redeploying forces from the area of operations to their main base of operations or home nation.

3.13. **Lessons learned**. Imagery products are an important tool to help all defence personnel visualise the physical details of their operating environment, including retrospectively. IMINT, produced during operations, supports commanders, national authorities, and other elements of the force in their review of past operations for lessons learned purposes.

INTENTIONALLY BLANK

Chapter 4 - Organizations and Responsibilities

Section 1 – Introduction

4.1. Developing the imagery capabilities and executing IMINT activities to meet NATO force requirements are challenges that require extensive cooperation and coordination among all members of the intelligence community. This chapter addresses the major roles and responsibilities of various IMINT-related organizations and key personnel within the operating forces.

Section 2 – NATO Strategic IMINT Responsibilities

4.2. Oversight of IMINT at the NATO strategic level is split between the Joint Intelligence and Security Division (JISD) at NATO headquarters and the strategic commands.

4.3. **The Joint Intelligence and Security Division (JISD) led by an Assistant Secretary General for Intelligence and Security (ASG-I&S).** The ASG-I&S is the strategic leader accountable to the Secretary General for leading the Joint Intelligence and Security Division (JISD) and responsible to the NAC and the MC on the effective provision of intelligence at NATO HQ and ensures close interaction with SHAPE and ACT on all intelligence matters.

4.4. **Supreme Allied Commander, Europe**. Supreme Allied Commander, Europe (SACEUR) coordinates imagery and IMINT support for operations, within the intelligence architecture for Allied Command Operations. To achieve this, actions are taken to:

a. plan and coordinate with the nations the imagery and IMINT requirements needed to support NATO operations, including reach-back support, data archiving, and training standards;

b. exercise tasking authority for the intelligence staff MoU organisation of the NATO Intelligence Fusion Centre (NIFC), within the scope of an overall coordination of requests for information;

c. exercise operational command over the NATO Alliance Ground Surveillance Force (NAGSF), which includes collection requirements and collection operations management functions.[33]

d. establish the release and disclosure policy (security classification guides) for NATO IMINT to ensure IMINT products are available to all troop contributing nations and communities of interest (such as geospatial and C2), within the constraints of the "need-to-know" principle; and

[33] For more information on collection requirements and collection operations management, refer to AJP-2.7.

e. support Allied Command Transformation and other NATO agencies in the development and implementation of new imagery and IMINT capabilities, by identifying operational requirements and capability deficiencies.

4.5. **Supreme Allied Commander Transformation**. Supreme Allied Commander Transformation is responsible for NATO's imagery and IMINT capability development. Capability development is supported by lessons learned analysis, the identification of deficiencies, and experimentation. Solutions are implemented through training, doctrine improvement, and standards. Supreme Allied Commander Transformation efforts seek coherence between long and short-term imagery-related capability requirements and solutions, and between all imagery user communities.

4.6. **NATO Intelligence Fusion Centre**[34]. As a MOU Organisation the NIFC provides SACEUR and subordinate commanders with timely, effective, full spectrum, network-enabled intelligence in support of the planning and execution of NATO operations and missions. The NIFC exploits all sources of imagery to produce IMINT for NATO.

4.7. **NATO Alliance Ground Surveillance Force**. The NAGSF is NATO's only operational intelligence organization capable of collecting still imagery and producing IMINT from EO, infrared, and synthetic aperture radar. The NAGSF can also produce IMINT from EO and infrared full motion video and can conduct near-real time exploitation of moving target indicator imagery for strategic and forensic analysis. NAGSF processes, exploits, and disseminates imagery derived from the NATO Alliance Ground Surveillance air vehicle as well as from STANAG-compliant imagery/data provided by external JISR sources. NAGSF supports all levels of command. Both finished and unexploited imagery and IMINT products produced by NAGSF sensors and analysts are releasable to all NATO nations.

Section 3 – Joint Task Force IMINT Responsibilities

4.8. **Commanders**. Intelligence is an essential responsibility of command and commanders are responsible for ensuring that intelligence activities are directed towards the needs of their force. Commanders focus IMINT on their requirements through the clear articulation of their intent and their commander's critical information requirements, which includes the identification of their priority intelligence requirements. These drive IMINT collection, processing, and dissemination activities. The commander must ensure their intelligence system is resourced so that it can effectively produce the intelligence they require, and that they are performing at the standard they expect. The theatre collection manager will be the one responsible for theatre-wide collection management.[35] In particular commanders must ensure sufficient imagery collection capabilities are allocated to the collection effort so that

[34] The NATO Intelligence Fusion Centre is a MOU Organisation

[35] "In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection sources or agencies, monitoring results and retasking, as required." (NTMS – NATO Agreed)

their intelligence requirements can be satisfied. Although commanders bear overall responsibility for intelligence, they normally delegates responsibility for most aspects of the process to their staff. In this instance the CJ2.

4.9. **CJ2**. The CJ2 is the commander's principal intelligence officer. As such, the CJ2 is also the commander's senior advisor on the use of IMINT. The CJ2 develops and implements intelligence plans and operations, including the integration of IMINT with other intelligence collection and production operations. The CJ2 must understand imagery and IMINT, their capabilities and limitations, and must be able to articulate all IMINT requirements to the chain of command. The CJ2's specific IMINT responsibilities are:

a. plan, direct, integrate, and supervise organic IMINT activities based on the mission, concept of operations, and commander's intent;

b. ensure IMINT tasks in intelligence collection plans and orders are appropriate for the subordinate sources, agencies and units/collection capabilities;

c. submit and coordinate IMINT collection and processing requirements, which are beyond the capability of subordinate units or formations to satisfy, to higher and flanking formations and units;

d. ensure IMINT is rapidly processed and where appropriate, fused into intelligence, and rapidly disseminated to the force and, as classification permits, to external users;

e. identify and correct deficiencies in IMINT personnel and equipment resources; and

f. facilitate understanding and use of IMINT in support of the planning and execution of operations.

4.10. **CJ3**. As the commander's battlespace manager, the CJ3 monitors, coordinates, and supervises the employment of the force within the battlespace. The CJ3 tasks and or coordinates all imagery collection capabilities operating within the commander's battlespace.[36] Close coordination between the CJ2's IRM&CM staff elements and the CJ3's joint intelligence surveillance and reconnaissance (JISR) staff elements is therefore required to ensure effective prioritization and de-confliction of collection operations. The CJ3, with primary responsibility for the planning and execution of operations, manoeuvre, and fires, is also a principal user of IMINT and closely coordinates requirements throughout the planning process to ensure timely and effective IMINT support.

4.11. **CJ5**. The CJ5 is the principal staff officer for all long-term planning. The CJ5 must define the IMINT requirements for all phases of a new operation well in advance of

[36] Imagery collection capabilities which collect on targets inside the commander's battlespace, but from outside the battlespace are not tasked or controlled by the CJ3.

commencing a planning process. The CJ5's requirements generally parallel those of the CJ3.

4.12. **CJ6**. The CJ6 is responsible to ensure communication and information systems (CIS), both internal to and external to the force, support the commander's requirements. This includes providing the communication paths, network access and maintenance and frequencies for IMINT organizations organic to, attached to and/or supporting the force. In addition to the multitude of different IMINT communications paths (each collection system frequently uses a unique pathway) IMINT collection and dissemination systems generally require large bandwidths.

4.13. **CJ2 IMINT support teams**. To support the CJ2, who more often than not will not be an imagery specialist, with both IMINT staffing and production, a team of IMINT specialists may be provided. The two most common types of teams are imagery support teams and the geospatial support teams.[37] Either team can be incorporated into the CJ2's Joint Intelligence Centre, or as part of a supporting multiple discipline intelligence unit, such as an All-Source Intelligence Centre. From an IMINT perspective, the primary role of either team would be to produce IMINT products, as stand-alone single source products or in support of multiple discipline intelligence production. Geospatial support teams are also able to produce a wide range of imagery based geospatial intelligence. The senior IMINT officer or imagery analyst are also able to assist the CJ2, and the IRM&CM staff, with the staffing of imagery collection requirements, and advising on imagery-related security releasability issues. They can advise on the most efficient utilization of imagery platforms and IMINT PED capabilities in order to support the mission requirements. This necessitates, particularly in the direction and collection phases, that IMINT officers and imagery analysts know the differences in capabilities and what they can and cannot do for the commander.

a. An IMINT officer is someone who works as a staff officer involved in the IRM&CM process. They do not analyse imagery, but should be quite well versed in the IMINT production process and understand IMINT's uses and limitations and what types of imagery are appropriate for a given situation.

b. An imagery analyst is an expert in imagery (EO, infrared, motion imagery, and radar) and its analysis, and is able to produce intelligence based upon the analysis.

4.14. Depending upon requirements and availability, the imagery support team or geospatial support team may also include an integrated imagery acquisition team. These teams are made up of military photographers who are trained to collect handheld imagery, of select intelligence targets, when the quality of the image is

[37] For more information on geospatial support teams see AJP-3.17 *Geospatial Support*

critical. Members of an imagery acquisition team also act as advisors on all handheld imagery matters.

4.15. **Reach-back**. In addition to ensuring there is sufficient IMINT specialist capability within the organization, the CJ2 will need to have access to other supporting capabilities, which cannot be deployed into an operational theatre, but are required to fill intelligence and/or IMINT gaps. IMINT reach-back support is the ability for deployed units or organizations to refer specific collection and production requirements to higher agencies such as the NIFC, NAGSF, or to national IMINT support agencies. The NATO intelligence community has an enormous amount of collected information, including relevant imagery, which is generally beyond the capacity of the intelligence architecture to make available to deployed formations. The reach-back capability is also critical for a deployed formation to gain access to more robust imagery sensors and platforms, such as satellite imagery that are normally only available at the national level. Although the reach-back capability within the formation is a chain of command responsibility, the CJ2 will identify the intelligence requirements that supporting agencies will service, as all technical requirements and protocols for the reach-back capabilities will need to be planned well ahead of the deployment period.

INTENTIONALLY BLANK

Chapter 5 - IMINT Interoperability

Section 1 – Introduction

5.1. The complexity of operations has increased due to a significant increase in the presence of non-military persons and organizations in the battlespace. NATO seeks to achieve its objectives through a comprehensive approach that requires effective coordination and cooperation among national governmental departments and agencies, non-governmental organizations, international organizations, and the private sector in any alliance or coalition throughout an entire operation.

5.2. Working with NATO in a combined/joint service environment is complex and requires participating nations to agree to implement certain standards and agreements related to imagery activities. Interoperability significantly enhances the capabilities of the forces involved and increases flexibility and efficiency to meet mission objectives.

Section 2 – Release and Disclosure

5.3. The exchange of imagery and IMINT between nations is strongly encouraged and in support of a comprehensive approach to resolving the complex operations of the modern battlespace, producers of IMINT should determine the classification and releasability of their product based on a “responsibility-to-share” rather than a strict “need-to-know” basis. That said, the sources and methods for producing IMINT can be sensitive, such that particularly sensitive IMINT targets, sources, and methods need to be protected by very restricted dissemination to those few who "need-to-know.” In some cases, NATO nations may, for policy and or legal reasons, not share their available imagery and IMINT with some or all other NATO nations.

5.4. Originators of IMINT, produced by or shared with NATO, have the responsibility to determine the security classification of the material in accordance with NATO’s security policy (C-M(2002)49 dated 17 June 2002). To assist originators in determining the releasability caveats, NATO command staffs must identify any considerations or sensitivities which may affect the classification and releasability of IMINT to the forces and governmental organizations of non-NATO troop contributing nations, international organizations and non-governmental organizations, and the host-nation. The NATO Security Committee’s Security of Information Directive AC/35[38] contains mandatory provisions for the handling of classified information, covering the following aspects:

a. classification and markings of information;

b. control and handling of information;

c. reproductions, translations and extracts of information;

[38] AC/35-D/2002 *Security of Information* supports NATO’s Security Policy (C-M(2002)49).

d. dissemination and transmission of information by physical means;

e. receipts and records;

f. disposal and destruction; and

g. security infractions, breaches and compromises.

5.5. **Intellectual Property and Copyright Protection**. Some source imagery, such as from commercial satellites, is acquired under contract and is therefore protected by intellectual property and copyright laws. CJ2 staffs are to be aware of the range of commercial imagery available to them and know the terms and conditions for its use and release. Care must be taken, and due diligence applied to ensure these laws are abided by. When in doubt as to how copyright laws apply, IMINT staff officers should seek legal advice.

Section 3 – IMINT Data Standards

5.6. For IMINT activities to be successful the appropriate information must be provided to the requesting user within the required timeframe. Interoperability of systems and the compatibility of data and products are essential to achieving this success. A strong synergetic effect is reached when all data can be collected, produced, disseminated, archived and retrieved using common NATO standards.[39]

5.7. This level of active and skilled management support demands the implementation of technical capabilities. To ensure the ability to retrieve and exchange imagery and IMINT in a network-enabled environment, the use of agreed information exchange requirements and metadata standards is essential. Such standards enable efficient release control, dissemination, search, optimal usage and maintenance of operational security. This active management also engenders the necessary confidence in IMINT providers in order to encourage exchange. The following information management principles apply:

a. **Security**. Imagery and IMINT must be properly classified in accordance with NATO and national security guidelines. All data must be reviewed and validated before it is disseminated or stored to ensure it is compliant. Ensuring proper classification is the responsibility of the originator, and each subsequent organisation that processes the imagery or IMINT.

b. **Discoverability**. All imagery and IMINT must be “metadata-tagged” in accordance with NATO Standardization Agreements (STANAGs) to ensure ease of discovery. NATO nations may use fields beyond the minimum defined in a STANAG, to meet national needs. These supplemental profiles should be made available to the wider NATO community.

c. **Availability**. Each unit storing and archiving imagery has the flexibility to determine where, when and for how long to store it. This also applies to

[39] For a complete list of relevant imagery and IMINT standards see Annex A.

member nations providing imagery through systems such as a coalition shared data server.[40] Nations and NATO commands making imagery available through a coalition shared data server are to ensure it remains available for as long as is possible. However, if NATO operational staffs have need for permanent archiving of imagery or IMINT products they are responsible for ensuring a copy is obtained and stored on one of their servers.

d. **Redundancy**. Imagery and IMINT stores must have redundancy or a backup capability to ensure that data is not lost in the case of system failure. This is particularly true when data is likely to be of future operational use or is required to be kept for legal reasons. Accordingly, the CJ2 must ensure that any acquired commercial imagery may be lawfully replicated.

e. **Coding.** For imagery and IMINT dissemination and storage purposes, data should be encrypted properly to reduce risks of leakages and manipulations. Commanders and their staffs may need to provide guidance to limit these risks and balancing the requirements for near real-time-data with delays resulting from encryption and decryption of large amounts of data.

Section 4 – IMINT Processing and Exploitation Systems

5.8. Generic NATO and coalition communication and information systems (CIS) do not normally have the specialized software and hardware required to exploit all types of imagery. IMINT CIS therefore impose significant hardware, software, and network challenges on to the CJ6. Access to and dissemination of motion imagery, satellite imagery, and other large files generally requires significant communications bandwidth and may exceed available means. Therefore, some imagery collection platforms may store the collected data on board during the collection mission, requiring the IMINT CIS to have capability to up-load the data from various media and from various formats. Imagery collection platforms may also store the collected data temporarily until a (more) suitable data link becomes available.

5.9. It is the responsibility of the nations and NATO to provide suitable imagery exploitation suites for the exploitation of the imaging systems they contribute. As a minimum, exploitation systems shall be capable of producing finished products, such as annotated graphics, text reports, and video clips that conform to the applicable STANAGs.

5.10. There are four common varieties of exploitation systems used in the production of IMINT:

a. **Electronic light table applications**. The NATO Alliance Ground Surveillance imagery exploitation software, along with other imagery exploitation software

[40] Coalition shared data servers are based on STANAG 4559 - *NATO Standard Intelligence, Surveillance, and Reconnaissance Library Interface*, and are the core of the architecture which enables the dissemination and storage of data from different sensors from different nations, as well as the tasking information and resultant exploitation reports.

are software packages used to exploit digital still imagery from EO, infrared, and synthetic aperture radar sources to produce and disseminate imagery and IMINT products. Depending on how the imagery is accessed by the exploitation work-station, exploitation can be done in near real-time or it may involve delays due to file transfer time. The software package could also include geospatial and normal office productivity software.

b. **Motion imagery exploitation systems** [41] can be as simple as a system capable of receiving a feed in near real-time and imagery analysts, sensor operators, and/or surveillance operators conducting near real-time exploitation and reporting using either voice or text-chat communications. Robust systems can be made up of multiple computers allowing the feed to be paused, reversed, stills extracted and annotated clips produced. The feed can be live from a sensor platform or played back from a server repository. Some of the systems also include geospatial and normal office productivity software.

c. **Moving target indicator exploitation software** is utilized for the exploitation of both streaming and archived moving target indicator imagery data. For NAGSF to exploit moving target indicator imagery data it must be STANAG-compliant.

d. **Wet film processing and light tables**. In addition to the delay of developing the film before it can be processed, the process of exploiting images using analogue light tables is slow, especially determining geo-locations. To enable the use of exploitation algorithms built into exploitation software, images can be scanned and the digital file exploited on an electronic light table.

[41] Motion imagery includes full- and slow-motion video.

Section 5 – Dissemination, Storage, Archiving, and Retrieval

5.11. To allow for interoperability with all NATO members, IMINT results should be metadata tagged in accordance with the applicable STANAGs. Reports should be produced using standard NATO reporting templates, saved in standard formats, and disseminated as read-only documents. Annotated graphics should also be exported in common non-editable formats.

5.12. Imagery and IMINT products should be electronically disseminated onto the common mission network in accordance with the appropriate security regulations. This will ensure that all mission partners, who can benefit from IMINT, have easy access to it.

5.13. Imagery for use by all mission-employed imagery analysts should be in shared repositories, preferably a coalition shared data server, in a format conforming to the NATO JISR interoperability architecture standards.

5.14. Storage requirements for coalition shared data servers will increase as imagery quality and quantity expand. This will require all coalition shared data servers to increase, as the metadata must be mirrored for national imagery analysts to access the data that other nations hold.

5.15. Deletion of imagery and IMINT results is managed as NATO classified information, including those aspects related to the disposal and destruction of the information. At the end of the life cycle, information shall be reviewed for retention, archival storage, downgrading, declassification, destruction, or release to the public. Any such actions need to meet not only security requirements, but also NATO information management and archival requirements.[42]

[42] AC/35-D/2002 *Security of Information*

INTENTIONALLY BLANK

Chapter 6 - IMINT Training

Section 1 – Introduction

6.1. Nations are responsible for ensuring that their forces declared to NATO meet the stated essential operational capability, NATO readiness and sustainability criteria, and other operational requirements. NATO is responsible, in cooperation with nations, for establishing the operational standards against which exercises and evaluations are executed. In addition, nations are responsible for the individual education and training of all personnel and units prior to deployment. NATO is responsible for providing mission-specific training.[43]

6.2. This chapter provides IMINT-related training goals and objectives and recommends major topics for inclusion in IMINT and imagery-related training. It does not provide a baseline unit training plan nor does it attempt to describe specific IMINT-related, individual, or unit training standards, operational procedures, or systems training requirements.

Section 2 – Objectives and Requirements

6.3. Training should be performance-oriented. Extensive practical application, in support of real intelligence objectives and requirements (e.g. in support of actual contingency planning) will be key to well-trained IMINT personnel and units. Training must cover the full range of IMINT activities employing a blend of traditional classroom techniques, communication and information systems (CIS) training, and practical application.

Section 3 – Training for IMINT Specialists

6.4. **Analytical focus**. IMINT training for imagery analysts[44] employed in NATO positions should include/provide specialised training for still and motion imagery analysis, and if required by the specific position specialised moving target indicator exploitation training. Effective analysis is the ultimate focus of IMINT activities as it is the principal determinant of the quality of the intelligence that will be produced. IMINT specialists use various processing and exploitation techniques and procedures to gain maximum value from imagery and imagery-sourced data. They perform these processes as part of an overall production cycle. The result is the development of relevant and timely IMINT products. Therefore, training for imagery analysts and teams must be focused on developing the quality and speed of their analytical and production skills and be designed to practice and improve their capability to develop quality products under operational conditions.

---

[43] See STANAG 2555 *NATO Intelligence Training*

[44] Imagery analyst training requirements can also apply to NAGSF Sensor Operators and Surveillance Operators, as both these positions also act as imagery analysts.

6.5. **Multiple discipline application**. NATO training opportunities should serve to educate IMINT specialists in how to support multiple discipline intelligence missions. Participation by IMINT specialists in exercises, involving multiple intelligence elements, will help to teach IMINT staff operational intelligence requirements, and maximize the interaction of commanders and staff with IMINT specialists. Interaction with the CJ2, CJ3, CJ5 and CJ6 during exercises can refine coordination requirements and improve intelligence flow during actual operations.

6.6. **Competency requirements**. As a minimum, key IMINT training objectives should include:

a. planning, integrating, and directing IMINT activities within the conduct of multi-discipline intelligence missions;

b. understanding of typical IMINT information requirements in a joint task force HQ, to include:

(1) type of imagery and IMINT products required;

(2) specific users within each staff branch and their typical scales, annotations, and time requirements;

(3) the organization's internal imagery reproduction capabilities;

(4) the capabilities, limitations, and unique requirements needed to integrate and support attached or supporting IMINT elements; and

(5) the capabilities and scope of organic imagery available in product libraries.

c. understanding the capabilities and limitations of IMINT collection operations, to include:

(1) the various types of imagery and their advantages/limitations;

(2) the planning, integration, coordination, and execution of IMINT collection with multi-discipline joint intelligence surveillance and reconnaissance (JISR) collection operations

(3) coordination requirements for the acquisition of commercial imagery from external sources; and

(4) coordination requirements for the planning and tasking of aerial imagery operations within the air tasking order process.

d. understanding the capabilities and limitations of IMINT production operations, to include:

(1) the various IMINT unique analytical techniques and working aids;

(2) the purpose, development and use of various IMINT products, to include both text and imagery products;

(3) the use of IMINT and imagery within multiple source and discipline intelligence;

(4) the planning, integration, coordination, and execution of IMINT production with multiple discipline intelligence production operations; and

(5) the use of various intelligence information systems and databases.

e. understanding of the capabilities and limitations of IMINT dissemination activities, to include:

(1) the planning, integration, coordination, and execution of routine and time-sensitive IMINT dissemination operations; and

(2) the requirements, establishment, and integration of unique IMINT and multi-use CIS architectures.

Section 4 – Training for the CJ2 staff

6.7. The ultimate objective of IMINT training for intelligence personnel is to ensure the effective contribution and integration of IMINT into NATO intelligence missions. For effective IMINT support to occur, realistic IMINT training must be developed and integrated with other intelligence training programs. The two main training objectives for non-IMINT specialist working in the intelligence function are to:

a. understand imagery and IMINT capabilities and limitations; and

b. understand IMINT unique requirements to support effective planning and direction of IMINT activities and the subsequent collection, processing and exploitation, production, dissemination and use of imagery and IMINT products.

Section 5 – Training for the CJ3 and CJ5 staffs

6.8. The objective of IMINT training for the CJ3 and CJ5 staffs is to support the efficient and effective identification of their IMINT requirements. Key IMINT training objectives for operations, planning, and joint fires personnel are to:

a. understand the advantages and disadvantages of the various types of imagery and IMINT products;

b. understand typical IMINT planning, collection, and processing response times in support of manoeuvre and joint fires; and

c. understand how to request or task a capability rather than an asset, including how to describe requirements accurately, ensuring that the requirements are understood and can be collected and processed correctly and efficiently.

INTENTIONALLY BLANK

Annex A
NATO Imagery and IMINT Standardization Agreements

1. The following NATO Standardization Agreements (STANAGs) and International Organization for Standardisation (ISO) standards contain provisions, which through references in this text constitute provisions of this STANAG. All recommendations and standards are subject to revision, and parties to agreements based on this STANAG are encouraged to investigate the possibility of applying the most recent editions of the STANAG, recommendations and standards listed below. The NATO Standardization Office maintains registers of currently valid STANAGs.

   a. STANAG 1059 - *Letters Codes for Geographical Entities*
   b. STANAG 3377 - *Air Reconnaissance Intelligence Report Forms*
   c. STANAG 3596 - *Air Reconnaissance Requesting and Target Reporting Guide*
   d. STANAG 3764 - *Exchange of Imagery*
   e. STANAG 3884 - *Air Imagery Interpretation Annotation*
   f. STANAG 4545 - *NATO Secondary Imagery Format*
   g. STANAG 4559 - *NATO Standard ISR Library Interface*
   h. STANAG 4607 - *NATO Ground Moving Target Indicator Format*
   i. STANAG 4609 - *NATO Digital Motion Imagery Standard*
   j. STANAG 4676 - *NATO Intelligence, Surveillance and Reconnaissance Tracking Standard*
   k. STANAG 5500 - *Concept of NATO Message Text Formatting System*
   l. STANAG 5524 - *NATO Interoperability Standards and Profiles*
   m. STANAG 5525 - *Joint Command, Control, and Communications Information Exchange Data Model*
   n. STANAG 7023 - *Air Reconnaissance Primary Imagery Data Standard*
   O. STANAG 7074 - *Digital Geographic Information Exchange Standard*
   p. STANAG 7194 - *NATO Imagery Interpretability Rating Scale*
   q. ISO 639-2 - *Codes for the representation of names of languages - Part 2: Alpha-3 code*
   r. ISO/IEC 7498-1 - *Information technology - Open systems interconnection - Basic reference model: The basic model*

s. ISO/IEC 11179-3 - *Information technology - Metadata registries - Part 3: Registry metamodel and basic attributes*

t. ISO/IEC 12087-5 - *Information technology - Computer graphics and image processing - Image Processing and Interchange - Functional specification: Basic Image Interchange Format*

u. ISO/IEC 14750 - *Information technology - Open distributed processing - Interface definition language*

Lexicon

Part I - Acronyms and Abbreviations

3-D	three-dimensional
AAP	Allied administrative publication
AJP	Allied joint publication
C2	command and control
CIS	communication and information systems
CJ2	combined joint intelligence staff
CJ3	combined joint operations staff
CJ5	combined joint planning staff
CJ6	combined joint command, control, communications, and computer systems staff
EO	electro-optical
HQ	headquarters
IMINT	imagery intelligence
IRM&CM	intelligence requirement management and collection management
JISR	joint intelligence, surveillance and reconnaissance
LIDAR	light detection and ranging
NAGSF	NATO Alliance Ground Surveillance Force
NATO	North Atlantic Treaty Organization
NIFC	NATO Intelligence Fusion Centre
NTMS	NATO Terminology Management System
PED	processing, exploitation and dissemination
SACEUR	Supreme Allied Commander Europe
SACT	Supreme Allied Commander Transformation
STANAG	NATO standardization agreement
TCPED	task, collect, process, exploit, disseminate

Part II - Terms and Definitions

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

collection
The exploitation of sources by agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. (NATO Agreed)

collection management
In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection sources or agencies, monitoring results and re-tasking, as required. (NATO Agreed)

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

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

imagery
Collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. (NATO Agreed)

intelligence
The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers. (NATO Agreed)

intelligence cycle
The sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users. (NATO Agreed)

named area of interest
A geographical area where information is gathered to satisfy specific intelligence requirements. (NATO Agreed)

operational intelligence
Intelligence required for the planning and conducting of campaigns at the operational level. (NATO Agreed)

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

recognized environmental picture
A complete and seamless depiction of geospatial, oceanographic and meteorological information designated for the planning and conduct of joint operations in a specific area at a specific time and which supports the unity of effort throughout the battlespace. (NTMS – NATO Agreed)

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

strategic intelligence
Intelligence required for the formation of policy, military planning and the provision of indications and warning, at the national and/or international levels. (NATO Agreed)

tactical intelligence
Intelligence required for the planning and execution of operations at the tactical level. (NATO Agreed)

AJP-2.6(A)(1)