NATO STANDARD

AJP-2.1

ALLIED JOINT DOCTRINE FOR INTELLIGENCE PROCEDURES

Edition B Version 3

MAY 2022

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

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

Intentionally blank

NORTH ATLANTIC TREATY ORGANIZATION

(NATO) NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

4 May 2022

1. The enclosed Allied Joint Publication AJP-2.1, Edition B, Version 3, ALLIED JOINT DOCTRINE FOR INTELLIGENCE PROCEDURES, which has been approved by the nations in the Military Committee Joint Standardization Board, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 2191.

2. AJP-2.1, Edition B, Version 3, is effective upon receipt and supersedes AJP-2.1, Edition B, Version 2 which should be destroyed in accordance with the local procedure for the destruction of documents.

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

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

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

Intentionally blank

Reserved for national promulgation letter

Intentionally blank

RECORD OF NATIONAL RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Intentionally blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
GBR	Given the UK's close cooperation and integration with the US and Five-Eyes (AUS, CAN, NZL, UK, USA) intelligence communities (on specific operations and peace-time) the full-scale and enduring adoption of processes and procedures within AJP-2.1 across UK Defence may be compromised. Despite this, the UK's intention is it shall remainfully interoperable with NATO, especially when engaged on NATO multinational operations where NATO doctrine is accepted as the authorative standard.
HRV	In order to fully apply the standard, current Croatian Armed Forces limited technical and materiel resources are partially complying to requested requirements in MASINT field.
USA	(1) The AJP refers to the "comprehensive preparation of the operational environment (CPOE)". CPOE is introduced without context and without a definition. The established analytical process is Joint Intelligence Preparation of the Operational Environment (JIPOE), established AJP-2. This reservation will be lifted when reference at footnote 45, para 4.6.a, and reference in the lexicon are removed (Note: JIPOE has not been added to the NTMS by the AJP-2 custodian). (2) US doctrine and policy does not support the overall premise of NATO doctrine being used for other non-NATO operations. Of specific concern is the assumption that U.S. intelligence and information sharing procedures will translate under AJP 2-1 doctrine to non-NATO nations. US intelligence and information sharing is per US policy and US Bi-lateral intelligence sharing agreements. This reservation will be lifted when AJP-2.1 clearly articulates that intelligence and information sharing is contingent upon approved formal intelligence and information sharing agreements with the U.S.

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

Summary of changes

- The existing AJP-2.1 is updated through an editorial review to produce a second version.
- Updates and changes were required for some of the text figures and references to ensure consistency with current NATO policies, joint doctrine and other publications.
- A significant reduction in footnotes with the remaining references and sources for further information.
- It is restructured and streamlined to improve the current publication and to ensure compliance with best practices. Reproduced paragraphs from other AJPs have been deleted where possible in some areas and referenced instead.
- The new version is harmonized with AJP-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*, AJP-3.9, *Allied Joint Doctrine for Joint Targeting* and referenced with level-3 intelligence publications.

Intentionally blank

Related Documents

Policy and MC documents

MC 0114	*Procedures for Production of NATO Agreed Intelligence*
MC 0128	*Policy Guidance for NATO Intelligence*
MC 0161	*NATO Strategic Intelligence Estimate*
MC 0166	*NATO Intelligence Warning System*
MCM-0175	*Military Committee advice on NATO civilian-military Warning and Alerting Policy*
MC 0296	*NATO Geospatial Policy*
MC 0327	*NATO Military Policy for non-Article 5 Crisis Response Operation*
MC 0628	*NATO Strategic Communications*
MC 0646	*NATO Joint Intelligence, Surveillance and Reconnaissance (JISR) Policy*
MC 0677	*NATO Geospatial Intelligence Policy*

Allied publications

AJP-01	*Allied Joint Doctrine*
AJP-2	*Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*
AJP-2.2	*Allied Joint Doctrine for Counter-intelligence*
AJP-2.3	*Allied Joint Doctrine for Human Intelligence*
AJP-2.4	*Allied Joint Doctrine for Signals Intelligence (SIGINT)*
AJP-2.6	*Allied Joint Doctrine for Imagery Intelligence (IMINT)*
AJP-2.7	*Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*
AJP-2.8	*Allied Joint Doctrine for Measurement and Signature Intelligence*
AJP-2.9	*Allied Joint Doctrine for Open Source Intelligence (OSINT)*
AJP-3	*Allied Joint Doctrine for the Conduct of Operations*
AJP-3.3	*Allied Joint Doctrine for Air and Space Operations*
AJP-3.6	*Allied Joint Doctrine for Electronic Warfare*
AJP-3.8	*Allied Joint Doctrine for Chemical, Biological, Radiological and Nuclear Defence*
AJP-3.9	*Allied Joint Doctrine for Joint Targeting*
AJP-3.10	*Allied Joint Doctrine for Information Operations*
AJP-3.17	*Allied Joint Doctrine for Geospatial Support*
AJP 3.19	*Allied Joint Doctrine for Civil-military Cooperation*
AJP-3.20	*Allied Joint Doctrine for Cyberspace Operations*
AJP-5	*Allied Joint Doctrine for the Planning of Operations*
AJMedP-3	*Allied Joint Medical Intelligence Doctrine*
AAP-03	*Directive for the Production, Maintenance and Management of NATO*
NATOTerm	
APP-11	*NATO Message Catalogue*

Standardization documents

AAP-47	*Allied Joint Doctrine Development*
AIntP-5	*NATO Human Intelligence (HUMINT) Techniques, Tactics, and Procedures*
AIntP-10	*Technical Exploitation*
AIntP-11	*NATO Intelligence Training*
AIntP-13	*Human Network Analysis and support to Targeting (HNAT)*
AIntP-14	*Joint Intelligence, Surveillance and Reconnaissance Procedures in support of Operations*
AIntP-15	*Countering Threat Anonymity: Biometrics in support of NATO Operations and Intelligence*
AIntP-16	*Intelligence Requirement Management and Collection Management*
AIntP-17	*Joint Intelligence Preparation of the Operational Environment*
AIntP-18	*Processing inside the Intelligence Cycle* (when ratified)
AIntP-24	*Intelligence support to Targeting* (when ratified)

Other

Allied Command Operations *Comprehensive Operations Planning Directive* (COPD)
NATO *Lessons Learned Policy*, PO (2011) 0293-AS1, 09 September 2011
BI-SC DIRECTIVE 080-006 *Lessons Learned*, 23 February 2018

Table of contents

Lexicon

List of figures

Intentionally blank

Preface

Context

1. The subject and conduct of intelligence support to operations is complex and requires a range of publications. AJP-2.1, *Allied Joint Doctrine for Intelligence Procedures* provides a bridge between the joint keystone doctrine AJP-2, *Allied Joint Publication for Intelligence, Counter-intelligence and Security* and the level-3 intelligence publications, which provide more detailed guidance.

Scope

2. AJP-2.1, *Allied Joint Publication for Intelligence Procedures* is the level-2 NATO doctrine for Allied intelligence personnel conducting joint operations and activities. It contains supporting joint doctrine for intelligence procedures and addresses operational-level concepts relevant to the joint commander and their staff and refers, where appropriate, to level-3 intelligence publications.

Purpose

3. AJP-2.1 provides commanders and their staff with a common framework for the conduct of the intelligence procedures in support of understanding and decision-making.

Application

4. AJP-2.1 is intended to influence thinking and provide guidance to NATO joint and intelligence staffs about the application of intelligence procedures in Allied joint operations. It describes the operational context and provides guidance on how Alliance intelligence personnel and its partners operate and considers the basic principles and practices to improve intelligence coordination and interoperability.

Structure

5. AJP-2.1 is divided into five chapters to provide detail where appropriate.

- Chapter 1 describes the background and purpose of the publication.
- Chapter 2 discusses intelligence support in planning operations.
- Chapter 3 describes the process and procedures involved within the intelligence cycle. (This is also covered in detail within AJP-2.)
- Chapter 4 describes coherence with joint intelligence, surveillance and reconnaissance (JISR) procedures. (The details of JISR procedures are now covered fully in AJP-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*.)
- Chapter 5 describes intelligence support to targeting. (The detailed procedures of intelligence support to targeting is covered fully in AJP-3.9, *Allied Joint Doctrine for Joint Targeting*.)

Linkages

6. Within the hierarchy of intelligence publications, AJP-2.1 derives its authority from and complements AJP-2. AJP-2 provides overarching doctrine on Allied joint intelligence, while AJP-2.1 focuses on the unique characteristics, procedures and considerations for intelligence personnel in joint operations. It should be read in conjunction with, AJP-2.2 *Allied Joint Doctrine for Counter-intelligence and Security Procedures*, AJP-2.7 and AJP-3.9. It supports AJP-3, *Allied Joint Doctrine for the Conduct of Operations* and AJP-5, *Allied Joint Doctrine for Operational-level Planning*.

7. The detailed procedures can be found within the level-3 publications, in particular:

- Allied Intelligence Publication (AIntP)-13, *Human Network Analysis and Support to Targeting (HNAT)*;
- AIntP-14, *Joint Intelligence, Surveillance and Reconnaissance Procedures in Support of NATO Operations*;
- AIntP-16, *Intelligence Requirements Management and Collection Management*;
- AIntP-17, *Joint Intelligence Preparation of the Operational Environment*;
- AIntP-18, *Intelligence Processing;* and
- AIntP-24, *Intelligence Support to Targeting* (Harmonization Draft).

Chapter 1 – Background and purpose

Background

1.1 For the foreseeable future, the security environment is likely to contain a broad and dynamic set of challenges. Commanders should seek a deeper understanding of these challenges, adversaries and other actors that are likely to be encountered in the operating environment. Intelligence is crucial to develop this understanding and commanders' decision-making. Understanding involves the acquisition and development of knowledge to such a level that it enables insight (= knowing why something has happened or is happening) and foresight (= being able to identify and anticipate what may happen).

1.2 Intelligence is important in supporting planning, understanding and decision-making across different types of NATO engagement and operations and contributing to NATO's three core tasks and policies.

- Collective defence, crisis management and cooperative security.
- Deterrence and defence, projecting stability and fight against terrorism.

1.3 There is a spectrum of conflict in which NATO operations can be conducted to meet any of the operational themes from warfighting, security and assurance, peace support and stability, and peacetime military engagement, across the compendium of competition.[1]

1.4 Military strategy sets the manner in which military power should be developed and applied to meet the Alliance's objectives. Joint planning should be the process that seeks to match strategy to tasks, and means to ends by applying suitable ways. The ends are the objectives that it wishes to achieve; the ways are the procedures to be employed in achieving such objectives; and the means are the capabilities to be employed. In the context of intelligence, the ends, ways and means are as follows.

a. **Ends.** The end is the requirement to support planning, decision-making and operations, with insight and foresight, via timely, predictive and accurate intelligence assessments.

b. **Ways.** The generic ways are described in this doctrine publication. They provide an overarching framework for the end-to-end management of intelligence requirements, data, information collection, intelligence processing and dissemination of assessments. This framework employs a number of processes to underpin the intelligence cycle and provide a doctrinal baseline to be employed at any level of operation.

c. **Means.** The means, that is to say the capabilities facilitating the intelligence processes and procedures, are varied in nature and can operate across different types of operations. Some of these capabilities are described in detail in other Allied Joint Publication (AJP)-2-series doctrine publications and subordinate publications

[1] For more details see Allied Joint Publication (AJP)-01, *Allied Joint Doctrine*.

dealing with particular tactics, techniques and procedures (TTP).

Purpose

1.5 The purpose of AJP-2.1 is to describe, primarily focusing on the operational level, the generic procedures, interdependencies and considerations required to conduct intelligence activities in support of NATO operations. It specifically concentrates on the intelligence and overarching management functions while leaving AJP-2.7 to provide detail on the planning, direction and execution of joint intelligence, surveillance and reconnaissance (JISR) activities and AJP-3.9 on targeting activities. This framework provides a common understanding of generic intelligence procedures and intelligence-supported processes at all levels of NATO, but is mainly written for those charged with delivering all-source intelligence to joint operational-level commanders. It can also inform the respective commands/units/ detachments/assets and other underlying structures.

1.6 AJP-2.1 also describes in some detail how intelligence activities are conducted within a generic formation or organization. In doing so, it offers authoritative guidance that requires judgement in application, and should be used to influence subordinate documents.

Chapter 2 – Intelligence in support of operations planning

Section 1 – Introduction

2.1 Supreme Allied Commander Europe's (SACEUR's) terms of reference[2] detail responsibilities for areas of responsibility and areas of interest, including those beyond NATO's territory. Specifically, they describe the need to monitor and analyze regional instabilities, military capabilities and transnational issues that may directly or indirectly impact NATO's security interests.

2.2 Further, the *NATO Crisis Response System Manual,* the *NATO Civilian-Military Warning and Alerting Policy*[3] and Military Committee (MC) 0166 series (*NATO Intelligence Warning System*) provide more detail on SACEUR's role in indications and warnings of potential or actual crises.

2.3 NATO uses the categories of strategic, operational and tactical to categorize echelons of command and operations activities.[4] These levels of warfare provide a framework within which to rationalize and categorize military intelligence activity. The customers and practitioners of strategic, operational and tactical intelligence must recognize the inevitable compression and blurring between these levels and that intelligence procedures are carried out at all levels. Furthermore, specific authorities or activities can be delegated to subordinate levels by the joint force commander, particularly during operations.

2.4 Intelligence procedures and activities contribute to, and synchronize with, planning, operations and assessment at all these levels.[5] The manner in which the process is developed, and the interrelationships between its components, particularly where these cross national boundaries, will be crucial to meet the commander's Priority Intelligence Requirements (PIRs) and to develop the Intelligence Collection Plan (ICP). During planning, as well as operations, all commanders must recognize the responsibility to act within their mandate in order to prevent and respond to conflict-related sexual and gender based violence (CR-SGBV). Intelligence is also required to support the commander's efforts to achieve this.

2.5 Intelligence is regarded as a joint function[6] to enable decision support, to support the execution of operations and is a fundamental requirement for commanders. Intelligence procedures remain constant to enable coherence and the staff adapt as required as the mission develops and requirements change.

Section 2 – Intelligence architecture

[2] Military Committee (MC) 0053-3 (FINAL) (Revision 1), 1 October 2014.
[3] JIS(2019)0049-REV2, *NATO Civilian-Military Warning and Alerting Policy*, 4 July 2019.
[4] See MC 586/1, *Military Committee Policy for Allied Forces and their Use for Operations* for further detail.
[5] Greater details on operations and planning processes and methods can be found in Allied Joint Publication (AJP)-3, *Allied Joint Doctrine for the Conduct of Operations* and AJP-5, *Allied Joint Doctrine for the Planning of Operations*.
[6] See AJP-01 (F), *Allied Joint Doctrine*, Chapter 4 (Draft) – The Joint functional framework.

2.6 The intelligence architecture will deliver a structure covering the overall intelligence organization, its staff, systems and processes and which interacts and operates with agencies and organizations to support decision-makers at all levels. The architecture should be flexible and tailored to the demands and circumstances of the operation and be reflected in the combined joint statement of requirements. In the broadest sense, the intelligence architecture will contribute to enhancing decision-making, joint effects, and effective manoeuvre and sustainment. This will require the connection, integration and collaboration of a wide range of sensors and collection capabilities, as well as the timely and accurate exploitation of collected information. Intelligence procedures should support the planning and execution of all operations by providing timely, tailored and accurate intelligence. The intelligence process should also allow a rapid flow of intelligence derived from all available collection capabilities to, from and additionally receiving feedback and collection requirements from end users across the joint operations area.

2.7 Allied Joint Publication (AJP)-3, *Allied Joint Doctrine for the Conduct of Operations* describes in detail the principles of NATO's Allied joint operations.[7] There may be a need for greater emphasis on some more than others dependent on the operation, but intelligence planning at the strategic, operational and tactical levels must be conducted in pursuit of these principles to successfully support the operation. In addition, different operational themes such as warfighting, security and assurance, peace support and stability, and peacetime military engagement may also require a number of additional considerations, (for example, environmental protection), further described in AJP-01, *Allied Joint Doctrine*.

2.8 The intelligence architecture is a collaborative endeavor involving all members of the intelligence community. It harmonizes the intelligence process to achieve the optimal use of intelligence specialists, agencies, collection capabilities and activities to produce the best possible insight, foresight and therefore understanding. These principles promote the idea that the intelligence effort within the architecture should:

- be directed towards clearly defined and commonly understood objectives;
- fully embrace cooperation and coordination to maximize collective effort;
- have a sound leadership and administrative baseline; and
- optimize employment of all available resources.

2.9 Establishing and maintaining a dynamic intelligence architecture is critical for an effective framework and for conducting intelligence activities. The intelligence architecture is built with effective staff integration, communication and relationship building, just as much as physical capabilities. It is the overall space, conditions and surroundings through which the military intelligence structure interacts and operates with international agencies and departments that contribute to and deal in information and intelligence to support decision-makers at all levels. The keys to its success are:

- educating and training NATO personnel and allies, including reserve forces thereby promoting a positive attitude;

[7] The principles are: unity of effort; concentration of force; economy of effort, freedom of action; definition of objectives; flexibility; initiative; offensive spirit; surprise; security; simplicity; and maintenance of morale.

- making the best use of Alliance and national capabilities;[8]
- maintaining joint forces, across-government, inter-agency and multinational links;
- bridging boundaries between the operational domains of maritime, land, air, space and cyberspace;
- removing outdated distinctions between the strategic, operational and tactical levels of intelligence activity;
- driving fusion and integration at all levels; and
- networking systems by intelligence community of interest services and user applications.

Section 3 – Intelligence support to strategic planning

2.10 Although AJP-2.1 is intended for use at the operational level, it is appropriate to briefly describe the higher-level processes that take place and ultimately initiate operational activity. This is because it may be the same intelligence specialists who contribute to strategic and operational intelligence development; both planning processes have been designed along similar lines. Intelligence produced for one planning process may very well be used on other levels.

2.11 If there is an emerging or immediate crisis, NATO will utilize the NATO Crisis Management Process. From operations planning to mission execution, the process allows SACEUR to undertake preparatory planning, in a reasonable time frame, to provide strategic intelligence assessments and advice. This process consists of a sequence of planning activities to organize the work of commanders and staffs, which are:[9]

- Phase 1 – initiation;
- Phase 2 – mission analysis;
- Phase 3 – military response options course of action (COA) development;
- Phase 4 – strategic plan development and COA analysis;
- Phase 5 – execution, decisions and directives with COA validation and comparison;
- Phase 6 – transition and termination of NATO crisis management role and commander's COA decision; and
- Phase 7 – plan development.

2.12 Progression through each phase is not automatic and will be guided by higher-level decision-making with intelligence contributions made during each phase. The phases do not have precise boundaries and may overlap. Moreover, they may be repeated depending on

[8] This is achieved through intelligence prioritization, coordination and management across all levels through intelligence requirement management and collection management (IRM&CM) with the detail in Allied Intelligence Publication (AIntP)-16, *Intelligence Requirement Management and Collection Management*.
[9] AJP-01, *Allied Joint Doctrine* and AJP-5, *Allied Joint Doctrine for the Planning of Operations*.

the changing circumstances during the life cycle of a crisis. The NATO crisis response system is also supported by the operations planning process (OPP), which will be described in greater detail.

Section 4 – Intelligence support to operational-level planning

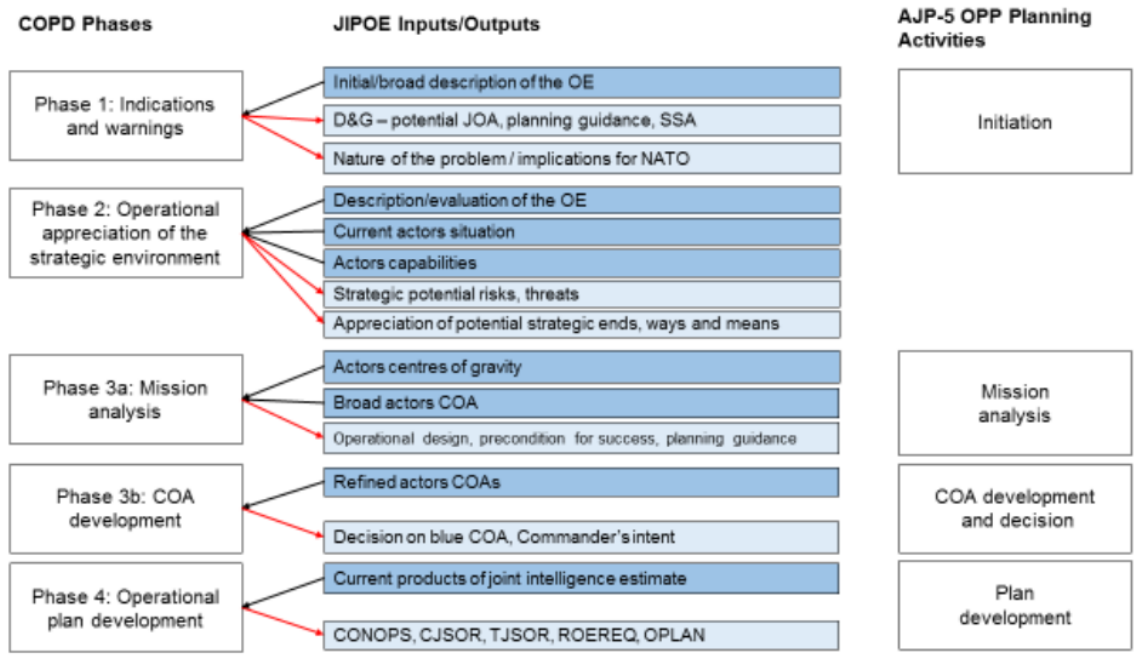
2.13 There is a linkage between strategic and operational planning and the intelligence function supports both levels and intelligence needs to be synchronized between the different levels. The activities for operations planning are described in AJP-5, *Allied Joint Doctrine for the Planning of Operations*.

2.14 Operations planning is conducted within Allied Command Operations (ACO) and carried out in accordance with the *Comprehensive Operations Planning Directive* (COPD), which is based on MC 133, *NATO's Operations Planning* and AJP-5 *Allied Joint Doctrine for the Planning of Operations*.

2.15 Additionally, synchronization between the joint intelligence preparation of the operational environment (JIPOE) process and the OPP is critical. Commanders, through their planning staff, will interpret and adapt the OPP according to their needs and it is the responsibility of the intelligence staff to adapt the JIPOE process to meet the requirements of each activity within the OPP.

2.16 Products developed in support of JIPOE will inform the OPP from the beginning of the planning process and therefore must be as mature as possible at the outset. The products to be produced during JIPOE and operations and planning staff requirements must be agreed upon as part of the mission analysis or developed into standing operating procedures (SOPs).

2.17 Figure 2.1 illustrates the types of information and intelligence products that need to be exchanged between each of the COPD phases and JIPOE and how these exchanges correlate with each of the planning activities. The JIPOE process is detailed in Section 6 and the synchronization of JIPOE with the COPD and OPP is detailed in Allied Intelligence Publication (AIntP)-17, *Joint Intelligence Preparation of the Operational Environment*.



CONOPS	concept of operations
CJSOR	combined joint statement of requirements
D&G	direction and guidance
OPLAN	operations plan
ROEREQ	rule-of-engagement request
SSA	SACEUR's strategic assessment
TCSOR	theatre capability statement of requirements

Figure 2.1 – Joint intelligence preparation of the operational environment correlation within Comprehensive Operations Planning Directive and operations planning process activities

2.18 The operational-level planning process (OLPP), carried out by a designated joint headquarters, also comprises of six phases to allow close collaboration between all levels of command during the different phases of the crisis management process. The intelligence process and joint intelligence, surveillance and reconnaissance (JISR) activities support all these phases. The close alignment of these processes means that intelligence produced at any level can be used seamlessly throughout the command chain, and ultimately contribute to operational success. There are six OLPP planning phases, which are:

- definition of indicators and warnings and situational awareness building;
- assessment of the crisis;
- development of response options;
- planning;
- execution; and
- transition.

Operational-level intelligence planning – phases

2.19 **Operational-level planning process Phase 1 – Indicators and warning and situational awareness.** The purpose of Phase 1 is to provide initial situational awareness of a potential or actual crisis to assist a commander's decision-making. The joint headquarters intelligence staff, in collaboration with Supreme Headquarters Allied Powers Europe (SHAPE) J2 staff, should initiate and lead the JIPOE process. This activity will develop an understanding and the subsequent monitoring of the crisis. The JIPOE process represents the main activity of the intelligence staff through all phases of the OLPP; however, intelligence staff must remain responsive to the commander's requirements throughout all phases of the OLPP. The JIPOE is a crisis-specific, cross-headquarters process, led by the intelligence staff to develop a comprehensive understanding of the operating environment covering all political, military, economic, social, infrastructure and information (PMESII) factors,[10] including associated potential threats and risks, in support of planning and the conduct of a campaign or operation. JIPOE develops an integrated understanding of the main characteristics of the operating environment, including its maritime, land, air, space and cyberspace domains, PMESII factors, threats, friends and neutral actors that may influence joint operations. In particular, intelligence staff will:

- gather, collate, organize and analyze existing information, and intelligence on the emerging crisis;[11]
- assist with determining the commander's critical information requirements (CCIRs) as part of the ICP;[12]
- develop PIRs;
- coordinate intelligence requirements with SHAPE J2;[13]
- lead the Joint Collection Management Board;[14]
- maintain and develop initial understanding, including the identification of key systems, sub-systems, groups, actors, key influences and relationships, and indicators and warnings; and
- monitor and report.

2.20 **Operational-level planning process Phase 2 – Assessment of the crisis.** The purpose of Phase 2 is to understand the strategic situation and to provide operational advice to SACEUR on the draft strategic military response options. Phase 2 at the operational level

[10] A more detailed description of PMSEII is in AJP-2, *Allied Joint Doctrine for Intelligence, Counter-intelligence and Security*.
[11] To further enhance the situational awareness, ensure that all human terrain factors is collected according to sex and age disaggregated data (SADD).
[12] Based on this initial analysis, the staff should advise the commander on critical information that may be required for future operational decisions. At this stage the CCIRs should focus on recognizing changes in the capabilities or behaviour of specific actors that might lead to an unacceptable situation. CCIRs will invariably change as the operation proceeds through its phases, with gathered intelligence serving to adjust the CCIRs as in AJP-3, *Allied Joint Doctrine for the Conduct of Operations*.
[13] It is important that intelligence staffs coordinate collection requirements to avoid duplication and to make the best use of resources with IRM&CM activities are coordinated and managed through an ICP or intelligence collection and processing plan (ICPP) with the process detailed in AIntP-16, *Intelligence Requirement Management and Collection Management*.
[14] The Joint Collection Management Board is described in more detail in AJP-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*.

spans Phases 2 and 3 at the strategic level. The intelligence staff will:

- continue and lead the JIPOE process;
- assist the Joint Operations Planning Group (JOPG) to understand the nature of the crisis; and
- provide a holistic briefing to the JOPG based on the developed JIPOE outputs at the beginning of Phase 2.

2.21 **Operational-level planning process Phase 3 – Development of response options.** The purpose of Phase 3 is to understand the situation, the operating environment and the mission in detail and to develop COAs, from which one may be selected. Depending on the situation, agencies such as the NATO Intelligence Fusion Centre[15] may deploy an intelligence support team to the designated joint headquarters to provide direct intelligence support and facilitate intelligence reachback. The intelligence staff will:

- provide the updated JIPOE briefing to the commander and their staff;
- focus on threats;
- determine key factors;
- conduct centre of gravity (CoG) analysis;
- support the development of the operational design;
- support the development of COAs; and
- shape the CCIRs and finalize PIRs.

2.22 **Operational-level planning process Phase 4 – Planning.** The purpose of Phase 4 is to ensure intelligence activity continues whilst operational planning is taking shape, leading to Phase 4 delivering two operational parts:

- Phase 4a – Concept of operations (CONOPS) development; and
- Phase 4b – Operation plan (OPLAN) development and force generation.

2.23 The purpose of operational CONOPS development is to detail the joint force commander's concept for the conduct of the military operation, in concert with other non-military and non-NATO efforts. It also establishes the conditions required to achieve strategic objectives and attain the end state. Within the operational CONOPS, a number of annexes are specifically mandated; the most pertinent to intelligence are:

- Annex D – Intelligence;
- Annex II – Joint targeting; and

[15] The NATO Intelligence Fusion Centre is a multinational intelligence memorandum of understanding (MoU) organization with intelligence analysts from participating member states. It falls under the operational command of SACEUR, with tasking authority delegated to SHAPE Assistant Chief of Staff (ACOS) J2, and provides timely, actionable, full-spectrum warning intelligence and intelligence in support of the planning and execution of operations, especially as a NATO Response Force.

- Annex T – Environmental support.[16]

2.24 During this phase, the joint commander should put into place the mechanisms to collect, fuse, analyze, validate and share critical information and, where appropriate, share knowledge with other commands and non-NATO actors throughout the life of the operation.[17] Within this phase, the commander approves the published CCIRs. The intelligence staff will:

- assist the JOPG in CONOPS development;
- assist the JOPG in OPLAN development;
- support the commander in deriving PIRs;
- produce Annex D – Intelligence;
- contribute to the combined joint statement of requirements (CJSOR), the theatre capability statement of requirements and the statement of requirements;
- contribute to define the Area of Intelligence Responsibility (AIR) and the Area of Intelligence Interest (AII); and
- provide Intelligence into to supporting annexes.

2.25 **Operational-level planning process Phase 5 – Execution.** The purpose of Phase 5 is to manage the execution of the approved OPLAN. This encompasses all related activity and includes operations assessment. As operations commence, the battle rhythm of briefings and meetings will be established to support the commander's decision-making, and to fuse staff effort. The intelligence staff will need to conduct the following activities.

a. Contribute to the daily situational awareness briefing (SAB). The SAB is a detailed daily update brief to the commander on the last and next 24 hours, and includes the next 48 hours in outline. It is given by the outgoing watch and the commander usually concludes the brief with any necessary direction and guidance.

b. Contribute to the Joint Coordination Board (JCB) decision briefing. The JCB is the commander's principal meeting. It synchronizes the entirety of joint activity and effects. In doing this, the commander should issue direction and guidance to all the components, and resolve potential areas of conflict.

c. Contribute to the operations assessment process within the Assessment Board and contribute to the joint force commander’s operational assessment briefing. The board seeks the commander's endorsement of the provided assessment and approves staff actions and subsequent plan adjustments. Decisions on follow-on actions should be taken by the commander during the JCB.

[16] J2 Geographical support included as Annex T Appendix 1 and Meteorological support to Annex T Appendix 2, as per AJP 3.17 and AJP 3.11 respectively.

[17] The COPD requires that details are provided in appropriate OPLAN annexes such as Annex D (Intelligence), Appendices 1-9; Annex W (Civil-military cooperation); Annex CC (Command information management); Annex NN (Knowledge development); Annex RR (Gender); Annex T-1 – Geospatial support; and Annex T-2 - Meteorological and oceanographic support. While not included in the COPD, J2 should review the Annex WW Reports and Returns to ensure all information is properly distributed across the ACO.

d. Contribute to the joint targeting cycle by supporting the Joint Targeting Coordination Board and, if established, the Joint Targeting Working Group (JTWG).

2.26 **Operational-level planning process Phase 6 – Transition.** As with the strategic-level OPP, the purpose of Phase 6 is to coordinate the transition and termination of a NATO operation. This includes transitioning NATO military responsibilities to proper authority and re-deploying forces under NATO military command and their return to national command. In this phase the intelligence staff will:

- contribute to identify and mitigate the negative risks and effects resulting from the disengagement of NATO troops; and
- contribute to a detailed systematic analysis of the operational area with a particular emphasis on the presence of NATO forces in theatre.

Section 5 – Intelligence staff

2.27 **Task organized intelligence staff.** At the operational level, the commander, through the principal intelligence staff officer, should establish a task organized intelligence staff with the role of the central management of the joint intelligence effort. The intelligence staff will provide the following.

- **J2 Current Operations.** Staff should be in close cooperation with the joint operations centre (JOC). J2 Current Operations, with the JOC, will play a critical role supporting current operations executed by the J3 staff and the JOC by using near real time situational awareness and understanding. This is central to intelligence requirements management and collection management (IRM&CM) and the JISR process. J2 Current Operations must coordinate at any time with the Senior Intelligence Duty Officer to be sure that sensors are used to enhance the real time situation awareness and understanding in accordance with the near real time assessment.

- **J2 Plans.** Staff should have a deeper time horizon and broader thematic responsibility than J2 Current Ops. J2 Plans should provide: intelligence support to the J5 planning staff; intelligence support to joint tasks; and deeper all-source intelligence analysis when required to provide improved understanding and intelligence in support of decision-making. J2 Plans leads the development of the JIPOE, to provide the commander and staff with both situational awareness and deeper analysis.

2.28 The intelligence staff is key to the development of the commander's situational awareness and understanding of the operating environment by providing both foresight and insight at the operational level. The intelligence staff may also include specialists to provide a detailed understanding of specific areas or themes. For example:

- providers of specialized intelligence products;
- Subject matter experts in specific intelligence domains such as geospatial intelligence (GEOINT) or connex domains as meteorological and oceanographic (METOC);

- representatives from national intelligence, defence or police agencies;
- intelligence representatives from the host nation;
- intelligence representatives from component commands;
- human environment analysts;
- cultural advisers and analysts;
- gender advisor (GENAD);
- operational analysts; and
- representatives from other governmental and non-governmental organizations, including international and regional organizations, the media, academia or industry.

Section 6 – Joint intelligence areas

2.29 The commander, supported by their intelligence staff, are to define the area of intelligence responsibility (AIR) and the area of intelligence interest (AII).

- **Area of intelligence responsibility.** The area for which a commander has the responsibility to provide intelligence with the means available.[18]
- **Area of intelligence interest.** An area (geographic, political, logical, boundaries) for which commanders require intelligence on the factors and developments that may affect the outcome of operations.[19]

Section 7 – Joint intelligence preparation of the operational environment

2.30 JIPOE is the process and the analytical methodology used to describe all relevant aspects of the operating environment providing commanders and staff with a comprehensive understanding of the operating environment. JIPOE identifies an actor's CoGs and vulnerabilities, and enables the development of relevant COAs

2.31 The primary focus of JIPOE is to provide predictive intelligence designed to help the commander discern an actor's probable intent and likely future COA. The conclusions drawn and the intelligence developed during most JIPOE are continually refined throughout the operation.

2.32 As an analytical process, JIPOE provides a holistic view of the operating environment to assess threats including actor capabilities and intentions. The JIPOE process not only provides a baseline understanding of the operating environment to support planning staff activities, but it also shapes how the commander and staff conceptualize the threat and more specifically what relevant actors may choose to do.

2.33 JIPOE, as a part of the overall all-source analytical effort performed by the intelligence staff, is illustrated in Figure 2.2. To manage the JIPOE effort effectively, a temporary re-structuring of the intelligence staff may be required. Identifying the amount of

[18] NATO Agreed.
[19] AJP-2.

detail required to answer PIRs avoids wasting time and resources on developing more detail than necessary on any given step of the process.[20]

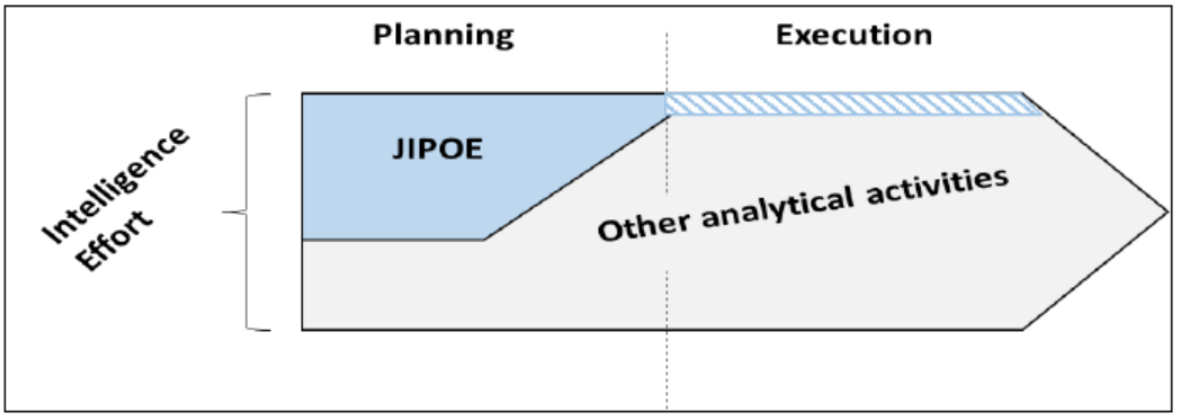


Figure 2.2 – Joint intelligence preparation of the operational environment and supporting intelligence activities

Principles and considerations for intelligence management

2.34 The intelligence framework is a wider consideration that should be addressed so that the intelligence architecture is established properly and is able to function as required. The following paragraphs are not exhaustive but are intended to guide those responsible for planning intelligence activities.

a. **Coherence.** Intelligence planning must contribute to achieving the approved overall objectives. The planning process should be coherent internally, as well as externally amongst the intelligence community.

b. **Comprehensive understanding of the operating environment.** The desired outcomes should be understood at all levels during the planning and conduct of operations. Sharing a comprehensive understanding of the environment is essential.

c. **Consultation and compatible planning.** Mutually supportive, compatible and, wherever possible, harmonized planning is fundamental for success within an all-inclusive approach. Intelligence effort and the associated information exchange and release procedures should encourage collaboration and cooperation wherever possible.

d. **Efficient use of resources.** The delivery of intelligence needs to balance continuous tensions between opposing requirements, and the optimization of effort and resources. This is true not just within the intelligence area, but also across the whole command or operation. Intelligence planners should achieve a balance between tasks and resources. Decision-makers should also be made aware of the risk of inadequately resourced intelligence capability.

e. **Flexibility and adaptability.** The intelligence planning process must allow

[20] The full JIPOE process is within AIntP-17, *Joint Intelligence Preparation of the Operational Environment*.

maximum action and interaction within the mission and agreed political and resource frameworks. The planning process should be strong, but also sufficiently flexible, adaptable and agile to allow the plan to evolve.

f. **Writing for release.** Writing for release at the lowest classification possible is a skill the analyst must be able to use and which comes with experience. The sharing of information will need to be achieved by a combination of intelligence staff pro-actively 'pulling' and 'pushing' products to and from agencies.

g. **Security classification determined by the originator.** The nation or NATO originator that provides intelligence products or collected information to the rest of the Alliance, other nations or third party, has the sole responsibility in determining the security classification along with any release restrictions. The classification and releasability cannot be changed without the consent of the originator.

h. **Criticality of dissemination.** There is little benefit in collection and processing that does not support an intelligence requirement and it should result in a disseminated product. Data, information, JISR results and fused intelligence products should be shared as early as possible after collection/production. Date and originator identity must be apparent. Methods of sharing should be supported with the appropriate compatible systems based on the customer requirements and the potential for future analysis. Information formats should also be in accordance with appropriate NATO standardization agreements (STANAGs) or generally accepted open standards. In some cases, especially with regard to available systems bandwidth, limitations exist, which have to be carefully considered during intelligence planning.

i. **Common standards for metadata.** Metadata is used for information discovery and efficient replication methods including data sharing. Robust metadata tagging must be used to enable manual and automated retrieval mechanisms to function effectively. Specifications of actual storage devices, or data servers, and their configuration should maximize interoperability between collectors, exploitation elements, intelligence processing organizations and customers.

j. **Appropriately trained, led and managed.** Importantly, personnel must be sufficiently trained in all the required skills and effectively led and managed in accordance with harmony and duty of care regulations. Equipment must be equally well managed and allocated to tasking so that momentum is maintained.

k. **Importance of intelligence information systems.** Intelligence architecture options for future missions must be addressed by all stakeholders before crises emerge. Future mission networks should include intelligence information systems, those that are funded for the NATO Command Structure, and those provided by contributing nations. Functional requirements and plans should be shared and analyzed collaboratively based on potential missions and tasks.

l. **Burden sharing.** This should help to identify capability gaps and interoperability requirements. NATO nations, commands and agencies should agree to contribute complementary applications, databases and intelligence collection and

processing capabilities, in a federated way, to burden share. Collaborative options, which consider all potential operational partners, should be developed so that CONOPS can be agreed and be ready to support rapid mission planning and force generation.[21] Additionally, the architecture should, within specific mission parameters, support reachback to those organizations that are not part of NATO.

m. **Importance of intelligence tools.** Intelligence support relies on a number of common and coherently used systems and tools to promote collaborative working and facilitate timely support.[22] These STANAG 4559 tools should be as widely available and familiar to NATO intelligence communities as possible in order to maximize their exploitation in operational contexts.

n. **Legal compliance.** All intelligence procedures and activities must be conducted in accordance with the relevant applicable law. The applicable legal framework will depend on whether the activity takes place in peacetime, including situations under the threshold of an armed conflict such as riots, internal disturbances or tensions or isolated and sporadic acts of violence or in an armed conflict (international or non-international). Accordingly, the domestic law of the respective nation(s) and international law may be applicable.[23]

o. **Mutual respect, trust and transparency.** Intelligence planning is underpinned by a culture of mutual respect and trust. Trust is built through: formal procedural information sharing; associated security measures to protect others' intelligence balancing the risk against persistent competition (as an example constantly assessing the insider threat); and collaborative procedural experience and familiarity amongst allies. Practical cooperation should be encouraged to enable collaboration and cooperation across NATO nations and operational partners, both civil and military, while also considering restricting the sharing of information due to possible counter-intelligence threats.

p. **Time versus depth.** There should be a balance between the need to provide assessments quickly and the need to conduct analysis and interpretation. Analysts rarely have as much time as they would like to consider a problem, but intelligence should be provided rapidly enough to deliver timely decision support to a commander.

q. **Quality versus quantity.** The requirement to ensure commanders receive valuable and relevant intelligence is vital. Often, the balance of effort could potentially favour collecting a volume of information, but analysts should provide high quality, predictive intelligence meeting CCIRs.

r. **Output versus ownership.** This is the tension created when the needs of a single Service or national capability provider impacts on joint force or NATO requirements. In some situations, tasking of a capability can be driven by who owns it, rather than it being focused on the wider need to contribute to a combined output.

[21] Including civilian agencies and organizations.
[22] AIntP-17, *Joint Intelligence Preparation of the Operational Environment* describes methods and tools available to an analyst.
[23] AJP-2 has further detail of intelligence legal compliance requirements.

Associated processes should enable, not delay, the transmission of information, and integrate scarce intelligence and JISR assets across the coalition whilst concurrently considering any security implications.

s. **Share versus shield.** Related to accessibility, the need to release intelligence at a classification the customer can use is another imperative of the intelligence community. The immediate customer may have a level of clearance that allows them access to the highest levels. However, as the widest possible dissemination of all-source intelligence at all levels is desirable, the analyst must be able to balance between the need to protect and the need to share (reflecting the need-to-know principle with the responsibility to share). Sharing must remain in line with NATO and national intelligence and information procedures and individual bilateral agreements. Wherever possible, tear lines of key assessments at classifications likely to be of wider utility should be released with the original report.

t. **Collect versus connect.** This is the need to balance developing an appropriate collection capability with the ability to process, exploit and disseminate the subsequent product.

u. **Stability versus change.** Procedures operate more effectively when associated with a stable requirement. Military operations, however, rarely remain constant for any significant period of time; this will be particularly true in the future operating environment. Intelligence procedures may, therefore, have to cope with increasing uncertainty and unpredictability, and will need to be agile, adaptable and flexible enough to maintain decision support.

v. **Resources versus demand.** It is unlikely that intelligence staff will ever have enough personnel or resources to satisfy every requirement or request. The intelligence head must anticipate the planning in order to build a robust organisation taking into consideration the prevailing constraints. Early expectation management and prioiritisation will be required to establish what is achievable.

Chapter 3 – Intelligence procedures

Section 1 – Intelligence cycle

3.1 The intelligence cycle is a sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users. This sequence, shown in Figure 3.1, comprises of the following four phases.

a. **Direction** – Determination of intelligence requirements, planning the collection effort, issue of orders and requests to collection agencies and maintenance of a continuous check on the productivity of such agencies.

b. **Collection** – The exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.

c. **Processing** – The conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation.

d. **Dissemination** – The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it.

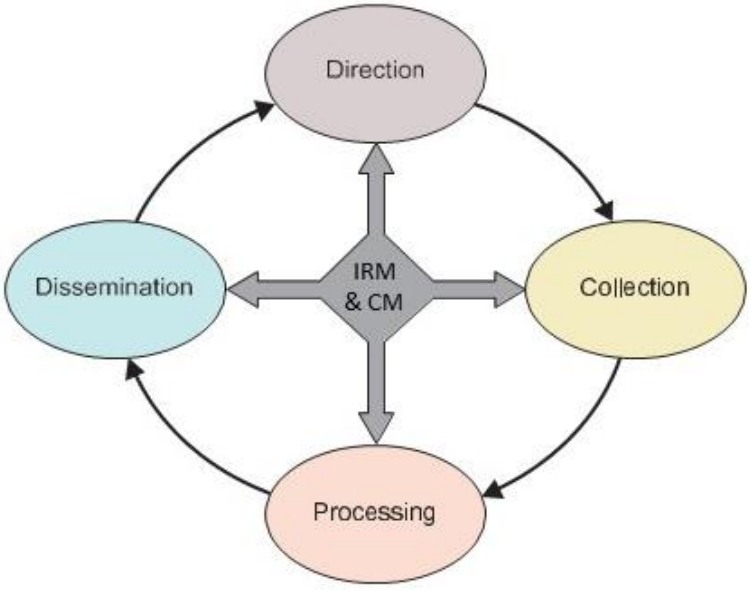


Figure 3.1 – The intelligence cycle

3.2 While the intelligence cycle outwardly appears to be a simple process, in reality it is a complex set of activities comprised of many cycles operating at different levels and speeds. Some tasks overlap and coincide so that they are often conducted concurrently rather than sequentially. In essence, direction can be applied at any stage, not just after dissemination has taken place; equally, collected data and information can, if the requirement is urgent, be

disseminated without being processed with the appropriate caveats.

3.3 Appropriate resourcing is particularly important as the vast majority of NATO intelligence capability is dependent on coordination and collaboration with different NATO member states or partners.[24] Resource availability should be considered early in the planning process to answer intelligence requirements. Ultimately, procedures should focus on optimizing the delivery of intelligence in the context of the following principles: command-led, objectivity, perspective, flexibility, timeliness, fusion, accessibility, sharing, collaboration, continuity, security, responsiveness, comprehensiveness and interoperability.

Section 2 – Intelligence requirements

3.4 The commander's critical information requirements (CCIRs) identify information on friendly activities, hostile activities and the environment that the commander deems critical to maintaining situational awareness, planning future activities, and assisting in timely and informed decision-making. As a result, intelligence requirements can be broken down further along with other information requirements which will support a decision point linked to the original CCIRs.

Priority intelligence requirements

3.5 Priority intelligence requirements (PIRs) are a vital part of the CCIR development process and are normally formulated by the intelligence staff in close cooperation with the commander and other staff elements, particularly the planning and operations staffs.

3.6 PIRs encompass those intelligence requirements for which a commander has an anticipated and stated priority in their tasking of planning and decision-making. This normally will encompass identification and monitoring of areas that represent opportunities and threats to the mission plan. They should be limited in number and in many cases provide comprehensive and coherent groupings of key issues. They may be enduring or limited to a particular phase or situation. PIRs should reference the original question and be written specifically to support the commander's decisions, focus on commander's intent and identify gaps.

3.7 PIRs and other intelligence requirements are managed locally, but also shared up, down and laterally. When assistance is required in satisfying a PIR or other subdivided intelligence requirements, it is sent as a request for information (RFI) or collection requirement (CR).

Specific intelligence requirements

3.8 A specific intelligence requirement (SIR)[25] is described as an intelligence requirement that supports and complements each PIR and provides a more detailed description of the requirement. SIRs are used by the intelligence staff to identify coordination requirements and determine which intelligence asset, collection capability or discipline can best satisfy the

[24] For example, the NATO Intelligence Fusion Centre or National Intelligence Centres.
[25] Allied Joint Publication (AJP)-2, Allied Joint Doctrine for Intelligence, Counter-intelligence and Security.

requirement. SIRs are managed in the same manner as a PIR.

Essential elements of information

3.9 SIRs are further broken down into more detailed questions known as essential elements of information (EEI). EEI add detail to SIRs and enable the production of a collection task list (CTL) based on an intelligence collection plan (ICP). EEI could be related to several SIRs and should provide enough guidance to enable analysts to give a complete and satisfactory answer to each requirement. EEI are the basis to create collection requirements and to establish relevant tasking and coordination with dedicated and non-dedicated collection capabilities or relevant agencies.

Named area of interest

3.10 A named area of interest (NAI) will also be utilized and is a geographical area where information is gathered to satisfy SIRs. It will usually be part of an ICP.

Decision points

3.11 Decision points are events in time or space on which the commander is expected to have to make a decision to ensure timely execution and synchronization of resources. Decision points can be linked to assumptions and CCIRs and they should help to prioritize the organization's collection efforts. Operational planners will develop a decision support matrix (DSM) to link decision points with: the earliest and latest time a decision is required; the intelligence (the adversary or actor) requirements; and the friendly force information requirements and is often used as the basis for intelligence requirements management (IRM) and an ICP.

Section 3 – Intelligence requirements management and collection management

3.12 Before describing the procedures that occur within the four stages of the intelligence cycle, it is important to emphasize the central roles of intelligence requirements management and collection management (IRM&CM). These procedures underpin the intelligence cycle and enable it to operate in a timely and efficient manner. Specific personnel from within the intelligence staff conduct IRM&CM. If not properly resourced, IRM&CM functions can quickly become overloaded.

3.13 IRM&CM manages the process of prioritizing and answering intelligence requirements. The answering of intelligence requirements is achieved ensuring the utilization of: all the existing data; information; joint intelligence, surveillance and reconnaissance (JISR) results; and intelligence. RFIs and the tasking of available collection and processing capabilities will also satisfy intelligence requirements and intelligence, surveillance and reconnaissance (ISR) requests supporting the needs of the operational decision cycle.

3.14 Once an intelligence requirement has been identified, validated, refined and prioritized, the intelligence staff should determine how to satisfy the requirement. In some cases, the requirement can be satisfied by information or intelligence already held by that operational headquarters or by NATO; alternatively, the intelligence requirement will need to

be matched by appropriate collection assets. If dedicated assets cannot satisfy the requirement, it can be submitted to the IRM staffs at higher, lower or adjacent headquarters or supporting forces/agencies as an RFI. In determining how to satisfy a requirement, the intelligence staff should consider each step in the intelligence cycle to ensure that the plan encompasses the entire process from collection through to utilization. The intelligence staff should identify the information needed, where and how to get it, how to package the intelligence into an appropriate product, how to deliver that product and how to request feedback from the originator of the intelligence requirement. Normally, an intelligence requirement should generate a need to:

- collect or retrieve data or information;
- process and produce intelligence in the scope and form that answers the question; and
- disseminate the product to a particular user.

Section 4 – Direction

3.15 Direction will shape intelligence requirements, allow for planning of the collection effort, the issuing of orders and requests to collection agencies, including the maintenance of a continuous check on the productivity of such agencies. Direction is key to the intelligence process and can be divided into external and internal direction. External direction comes from commanders and sets the parameters for the objectives (via CCIRs) and intelligence requirements (via PIRs). Internal direction comes from the senior intelligence officer.

3.16 The direction should be specific and, wherever feasible, should highlight those factors that are critical to the planning process and the decision cycle. Therefore a continuous dialogue should be established between commanders and their senior intelligence officer to provide clear and rigorous direction for the intelligence cycle via well-crafted intelligence requirements. These requirements can generally be divided into two groups:

- intelligence requirements that contribute to the success of the mission; and
- intelligence requirements that identify and quantify the threat to the mission.

3.17 In giving direction and initiating the process, the commander has a responsibility to the intelligence staff to:

- have a broad appreciation of intelligence doctrine, collection capabilities and their limitations including organizations, units and their assets;
- issue clear direction and guidance, defining areas and themes of interest;
- participate with drafting, approval and circulation of their PIRs;
- develop trust with intelligence staff, encouraging their integration into planning and operations, creative thinking and through analysis provide predictive assessments; and
- engage with and test these intelligence assessments without undermining their intelligence staff or seeking to impose their own interpretation.

3.18 The PIRs may have to be addressed in a variety of ways depending on the operational scenario and mission and may be satisfied by using a variety of means. These means will encompass intelligence and operational assets and may potentially involve the Alliance's, national governments' and civil capabilities. All intelligence requirements should contain details of the nature of the intelligence required, its desired priority and other governing factors.

3.19 The IRM manages these requirements is an analytical as well as an accounting function because, in addition to developing, tracking and refining intelligence requirements, it works closely with production analysts to determine what is already known and what requires new collection. This avoids unnecessary collection effort and makes the handover to the collection management staffs' function more efficient. Overall, as requirements are generated, the IRM function will:

- help to validate, prioritize and refine intelligence requirements;
- determine how intelligence requirements can best be satisfied in coordination with intelligence analysts and the collection management;
- coordinate all activities within the intelligence cycle associated with meeting the requirement in coordination with intelligence analysts and the collection management;
- coordinate collection tasking with intelligence analysts and the collection management;
- monitor activity to ensure that the right information is being collected, processed and disseminated; and
- ensure that intelligence activities are conducted in a timely manner and in coordination with the collection management staff, and that delays in collection are mitigated by re-tasking or reprioritizing collection as required.

Request for information

3.20 In the scope of the enclosed document, the term RFI is used to describe an RFI that is passed to the intelligence requirements manager at higher or adjacent levels. Lower levels will be tasked by the ICP. Where the ICP does not foresee the collection, lower levels will be tasked through the RFI process. An RFI is used when commanders do not have sufficient allocated collection capabilities or the intelligence staff are unable to answer a question through research or other means, and thus commanders require assistance from a superior, subordinate or adjacent command[26]. The receiving organization will treat the incoming RFI as an intelligence requirement and will evaluate and decide on the prioritization, the means and the product to fulfil the respective requirement. RFIs have to be prioritized in accordance with the intelligence requirements within the IRM. A single intelligence requirement may generate a number of separate RFIs for different providers or other intelligence resources such as national JISR capabilities, agencies or adjacent headquarters.

[26] Non-intelligence personnel should also use the RFI process to access intelligence required for their mission or task.

Indicators

3.21 Before beginning the next step of the intelligence cycle, analysts should have already identified the indicators that are appropriate to the particular operation or threat. Selection of indicators appropriate to the operational situation is the responsibility of analysts, and the nature of the indicators that they select will influence the ICP. Indicators in intelligence usage, are described as an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action. To cope with the uncertainty of the future, analysts must make estimates based on observable indicators in the present that they assume will determine future actions. Therefore, to predict which alternative future the current situation is moving towards, the analyst utilizes identified indicators. These indicators, when observed, are either consistent or inconsistent with the different hypotheses, improving assessments of future developments.[27] Indicators should be regularly reviewed and refined.

Collection management

3.22 Collection management establishes collection requirements, tasking or coordinating with appropriate collection capabilities or agencies, and monitors results and re-tasks, as required, by making best use of the collection capabilities. Collection management also encompasses activities related to the execution and coordination of the JISR process. Collection management is implemented by the theatre collection manager who exercises collection management authority for a given mission and area of intelligence responsibility.

3.23 Collection management needs to include all levels of command and include mechanisms or tools that avoid duplication with other JISR-related processes, such as targeting. At the operational level, joint force or theatre collection managers are responsible for prioritization and coordination of collection across the force. They will assemble all intelligence requirements originating from their own IRM and operations area, as well as those passed up from subordinate units and turn them into synchronized and prioritized collection tasking. The ICP is a central tool for the IRM&CM function.

Intelligence collection plan

3.24 The ICP[28] identifies the intelligence requirements for a given commander and is a detailed breakdown of how each intelligence requirement is to be satisfied. The ICP is a planning tool for collection managers at each level of command. If not modified/specified by the CTL, the ICP acts also as a tasking document for subordinate headquarters. The ICP, like PIRs, will focus on a particular phase of an operation. SIRs and EEI help form the basis of the ICP, which together with emerging collection requirements are prioritized and integrated.

3.25 Normally in matrix or table form, an example of a generic ICP is shown at Figure 3.2. The ICP indicates the preferred method for satisfying intelligence requirements. It will indicate the general level of detail required and should list the organizations, agencies or assets best suited to the task. The overall collection effort is managed through the

[27] See also Allied Intelligence Publication (AIntP)-18, *Intelligence Processing*.
[28] AJP-2 refers to an ICP and AInt-P16 refers to an intelligence collection processing plan (ICPP) which supports the IRM&CM functions but in principle these are similar processes.

implementation and control of the ICP alongside additional RFIs, intelligence, surveillance and reconnaissance requests (ISRRs), the CTL and the collection and exploitation plan (CXP). The availability of collection assets is considered. If dedicated assets are available, the collection task is forwarded to the relevant unit or asset. If dedicated assets are not available[29] collection requirements are sent as ISRRs and collated into a collection requirements list, which is then prioritized by the Joint Collection Management Board into the CTL for collection by the subordinate headquarters.

PIR	SIR	EEI	Indicator	NAI	Reporting	Product	SHAPE	NIFC	MCC	LCC	ACC	Nation 1	Nation 2	OSINT	MASINT	SIGINT	Etc
PIR#1	SIR#1	EEI#1	What?	Where?	When?	Type?	✓			✓		✓		✓			
#2	#2	#2						✓	✓	✓	✓						
#3	#3	#3						✓							✓	✓	

Figure 3.2 – Example of a basic intelligence collection plan

Section 5 – Collection

3.26 Collection is the second phase of the intelligence cycle. Collection is the exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. Intelligence agencies and collection capabilities conduct the bulk of all collection activities, but non-dedicated collection capabilities can also contribute.[30] Collection activity requires close collaboration with both intelligence and command staff to optimize the use of collection assets. Those agencies with a processing capability may respond with intelligence rather than information. Given the amount of information pertinent to modern operations, a degree of analysis and processing will be required in order to effectively identify where and how collection should take place, this is encompassed by the JISR process.

3.27 To meet intelligence requirements, the appropriate collection capability needs to be tasked through a coordinated and integrated procedure, which ensures accurate and timely cooperation with all interested parties. This enables early indications of the presence of objects, phenomena or activity of interest from whatever collection capability (from specialized wide area surveillance systems to non-specialized collection means) to be acted upon in a timely manner to confirm presence and nature, and subsequently to gather the required information or intelligence. Therefore the link between collection as the second

[29] This can be either because the appropriate collection capability is not assigned or attached to that headquarters or is being used to satisfy another intelligence requirement.

[30] Non-dedicated JISR assets are capabilities that are not assigned to JISR duties but contribute to the intelligence picture through routine operations. The maxim, 'every individual, system and platform as a sensor' captures this.

phase of the intelligence cycle and the JISR process is essential.

3.28 It is important that intelligence staff ensure the commander and their staff understand the capabilities, limitations, vulnerabilities and response times of collection capabilities and agencies likely to be available to them, along with their susceptibility to deception. General factors affecting collection include the following.

a. **Security.** A particular collection capability may provide unique information, making compromise a fundamental consideration for the collection agencies. This may pose limitations on dissemination.

b. **Suitability.** The collection capability (including the respective commands/units/ detachments/assets and other underlying structures) should be selected on the basis of its availability and capacity to acquire and deliver the information or intelligence required in the required timescale and format.

c. **Risk.** In some cases, there may be a degree of physical or political risk involved. This should be weighed against the criticality of the information required.

d. **Environment.** Environmental constraints such as infrastructure, the information environment, gender, religion and culture, protected areas, borders and boundaries, threat, climate, and weather or terrain can limit the usefulness of some capabilities.

e. **Balance.** Systematic exploitation of as many collection capabilities and agencies as possible to answer a question provides corroboration and a balanced view. Coordination of this collaborative effort will also balance the burden of collection activity.

Section 6 – Processing

3.29 Processing is the third phase in the intelligence cycle and entails a structured series of activities which, although set out sequentially, may also occur concurrently. Processing is conducted at a number of points within the intelligence function and is multi-faceted. It is described as the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation. Processing is iterative and may generate further requirements for collection before dissemination of the intelligence.

Collation

3.30 Collation is the first step in the processing phase, during which related items of information or intelligence are grouped together. In practice, it is comprised of the procedures for receiving, grouping and recording all reports, and involves:

- registering the receipt of each incoming piece of information and intelligence; and
- placing each piece of information or intelligence into an appropriate category or group through logging, marking on a map or chart, filing or entry into an electronic database.

3.31 Although collation is increasingly likely to be automated, involving databases linked to graphical interfaces and automatic data transmission between headquarters, there will always be an individual element of sifting, comparison and even simple visual collation (VISCOL) of collection results. This will provide a subjective view of responses to intelligence requirements and a gauge to how valuable they are in answering a commander's requirement. Factors affecting collation include the following.

a. **Standardization.** There should be one way of collating information to a retrieval system and this should be logical and directly related to the intelligence requirements. In reality, as different intelligence disciplines perform discrete tasks, it may not be possible to standardize every database, but the aim should be to have as few as possible. Metadata tagging should be similarly standardized.

b. **Cross-referencing.** Efficient retrieval can only occur if information is stored with cross-referencing aids such as date/time reference, geospatial coordinates, metadata or another form of tagging such as unique identifier codes.[31]

c. **Construction.** Although electronic storage systems can manage a huge amount of data, the collation system should be intuitive and as simple as possible. Using relational data will simplify data exploitation by search, analysis and visualization toolsets at a later date.

d. **Network-centric architecture.** Databases of different headquarters should be networked to allow sharing of intelligence products. It is likely each database will require support from a robust database management capability.

Evaluation

3.32 Evaluation is the second step in the processing phase and consists of appraising an item of information in respect to the reliability of the collection capability and the credibility of the information. Evaluation allocates an alphanumeric rating to each piece of information or intelligence indicating the degree of assurance which may be placed upon it.[32]

3.33 The evaluation rating is based partly on the subjective judgement of the evaluator, and, in the case of information produced by a sensor, on knowledge of the accuracy of the particular sensor system.[33] Reliability and credibility should be considered independently of each other to ensure that the rating allocated to the reliability of the collection capability does not influence the rating given to the credibility of the information, or vice versa. A factor the analyst should also consider is the collection capability's access to the information provided. The values and associated statements for reliability and confidence are shown at Table 3.1.

[31] Unique codes can be allocated to objects or entities such as people, places or vehicles.
[32] AJP-2 – this is not always necessary, but when it is not formally employed, analysts should still mentally apply this process of evaluation.
[33] AJP-2 – ratings are produced by combining the values; a piece of information from a collection capability known to be usually reliable and judged probably true would be rated B2.

Table 3.1 – Reliability and credibility

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

Analysis

3.34 Analysis, in intelligence usage, is described as a step in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation. During analysis, collated and evaluated information is examined for significant facts. These are then related to other known facts, and deductions are drawn. Analysis applies the tools, processes and tradecraft to data and information to create and deliver new intelligence, insights, foresights and knowledge, with the goal of providing decision advantage to commanders and decision-makers.

3.35 Analysis is never exhaustive, nor absolutely certain, as the dynamics of most crises can be complex and unpredictable, therefore ongoing analysis will be required. However, effective analysis can help a commander to rationalize, though not necessarily reduce, complexity and ambiguity to some degree.

3.36 Analysis provides more than a picture of the current situation. It is predictive in providing the commander an analysis of what may happen based on fused data and relevant assumptions regarding the actions and reactions of different actors (including the impact of any intervention) such as assessment of enemy Most Likely and Most Dangerous Courses of Action (MLCOA/MDCOA). Predictive analysis enables a commander to understand the context in which they are operating or intend to operate. As such, predictive analysis and answering the ‘so what’ is the optimum output of analysis and should be aspired to in all intelligence products.

Integration

3.37 Integration is a step in the processing phase of the intelligence cycle whereby analyzed information and/or intelligence is selected and combined into a pattern in the course of the production of further intelligence. Integration is the drawing together of analytical deductions, and the determining of a pattern of intelligence, such as a sequence of events or the profile of an individual. To meet the full range of intelligence requirements that it should satisfy, a unit will often require external products to fuse with material generated internally.

3.38 Periodic validation, sometimes by those previously not involved in the analytical effort, can provide a fresh perspective to analysis and offset any tendency towards groupthink

and other analytical pitfalls. There are a number of standard review techniques.[34]

a. **Key assumptions check.** The analysis is broken down into the individual assumptions supporting it. These are then tested using a series of questions. If unsupported or questionable assumptions remain, the analysis may be inaccurate.

b. **Devil's advocacy.** The same information that was used to form an assessment is used to disprove rather than prove the hypothesis. This will help identify any weaknesses in the assumptions underpinning the assessment.

c. **Red teaming.** This involves creating a team with the objective of subjecting an organization's plans, programmes, ideas and assumptions to rigorous analysis and challenge. It is used for identifying and assessing, inter alia, assumptions, alternative options, vulnerabilities, limitations and risks for that organization but the tool set can also provide an alternate perspective – usually that of the adversary. Red teaming can help avoid cultural bias in analysis and can be used to generate 'wild card' scenarios to aid commanders in their decision-making.

d. **Peer review.** A review by peers or seniors can help analysts identify gaps in their assessment or identify alternate outcomes they may not have considered. Peer review should be an almost constant process.

Interpretation

3.39 Interpretation in intelligence usage is described as the final step in the processing phase of the intelligence cycle in which significance of information and/or intelligence is judged in relation to the current body of knowledge. Interpretation is an objective comparison based on common sense, life experience, military knowledge and understanding, covering both the adversary and friendly forces.

3.40 In interpreting the information presented, steps should be taken to guard against partiality or bias, especially given the natural inclination to exclude the unexpected, the inexplicable, the unpalatable or the counter-intuitive. There are a number of general considerations which should be looked at.

a. **Identification.** This considers all the implications of the presence or absence of that actor or piece of equipment at that particular point. Identification also involves considering the motivations and objectives of both the source of the intelligence and the actor being reported on.

b. **Activity.** The significance of the activity being carried out should always be compared with information about previous activity to discover whether there is any change in the pattern of activity.

c. **Significance.** The analyst must be sure that the piece of information has been fully exploited. Each deduction should be challenged, taking into account the original

[34] See also AIntP-18, *Intelligence Processing* for more details

intelligence requirements, so the final product is relevant and useable.

d. **Confidence and probability.** Throughout interpretation and all-source fusion, the analyst should attempt to find confirming information or intelligence. The degree of corroboration should enable levels of confidence to be expressed. The term 'confirmed' is rarely used in assessments given the nature of intelligence projecting forward in time. The means of expressing confidence and/or probability levels are shown in Tables 3.2 and 3.3.

e. **Deception.** Deception consists of those deliberate measures to mislead targeted decision-makers into behaving in a manner advantageous to the commander's intent. The intelligence community is a primary target for hostile deception and analysts should always be cautious of the information in front of them.

Table 3.2 – Confidence levels

Confidence levels	
High	Good quality of information, evidence from multiple collection capabilities, possible to make a clear judgment.
Moderate	Evidence is open to a number of interpretations or is credible and plausible but lacks correlation.
Low	Fragmentary information or from collection capabilities of dubious reliability.

Table 3.3 – Probability levels

Probability statements for assessments (numerical and verbal)	
Almost certain	More than 90%
Highly likely	75%-85%
Likely	55-70%
Possible	45% - 50%
Plausible	25% - 40%
Unlikely	15% - 20%
Highly unlikely	Less than 10%

3.41 **Intelligence assessments.** The end product or assessment is critically important to inform decision-making and to enable the commander to exploit opportunities and measure mission progress. The intelligence staff should assist the commander to establish joint and

interagency assessments. This will include assessments against progress in the political, diplomatic, economic, rule of law and security spheres of activity, with specific measurements for campaign objectives and decisive conditions. The method and criteria behind the assessments must be coherent across the joint task force and highlight:

- what is known as fact;
- where there are gaps in knowledge; and
- what is analytical assessment.

Section 7 – Dissemination

3.42 The final phase of the intelligence cycle is dissemination, which is the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. It also requires security, conformity to the requester's requirement and a mechanism for feedback. Dissemination planning enables the right information to be distributed to the right people in the right format and within the right timescale. Staff elements responsible for IRM&CM should determine the means of dissemination, storage and retrieval of product. That can be a single system or multiple systems that rely on numerous ways and means for dissemination, storage and retrieval. In all cases, however, dissemination must be coordinated with the wide variety of IRM&CM processes.

3.43 Dissemination of intelligence should be in a timely manner without overloading the user but still minimizing the load on available bandwidth. Web-based technologies and standards are now commonly used to organize and present intelligence products.

3.44 It is important for the intelligence staff to continuously manage the dissemination process. Without effective management, communications paths can become saturated by information. For example, single-source reporting may be re-transmitted by many intermediate entities, resulting in circular reporting. Advances in technology will also affect dissemination and communications; importantly, these areas should be complemented by appropriate human communication skill sets, including linguistic ability.

3.45 **Circular reporting.** Units and single-source or single intelligence discipline collectors provide specialist capabilities and intelligence in support of commanders and their staff, and subordinate, higher and flanking organizations. It is important for all intelligence staff to maintain discipline in reporting so as to avoid circular reporting: the use of intelligence from other disciplines or units as collateral, prior to the processing all-source intelligence within an all-source context. This will also provide an audit trail for intelligence analysts seeking to clarify reporting with collectors or to provide feedback.

Principles for dissemination

3.46 Computers and modern communication systems have reduced the information-to-production timeline for delivering intelligence products. Likewise, some collection assets are capable of disseminating collected information to requesters on a near-real time basis, vastly increasing their responsiveness. Even with use of technical systems, disseminated products should adhere to the following basic principles.

a. **Clarity.** Products should use plain language and avoid the use of acronyms, unless they are well understood. Where possible, it should follow a standard format and use maps, drawings and diagrams to enhance the information being presented.

b. **Relevance.** Products should only be disseminated to the audience for whom the topic is relevant. This avoids unnecessary overloading of systems or distracting individuals from other tasks.

c. **Brevity.** To be succinct is the key to the successful dissemination of intelligence. Background material may be relevant, but products should only answer the question being asked, and only be as long as necessary.

Intelligence formats

3.47 The format selected for dissemination should be appropriate to the requirement and the recipient using standardized templates where appropriate. They can be disseminated in the following formats.

a. **Verbal.** Verbal briefing is best for establishing trust and credibility and provides the opportunity to emphasize significant issues. It can also give immediate feedback and guidance.

b. **Written.** Written dissemination includes formal intelligence reports and intelligence summaries or ad hoc summaries. Some are disseminated at regular intervals, while urgent material can be disseminated when required. Presentation is important in written products, which makes them slower to prepare than other forms of dissemination. All originators should use plain language and write for release.

c. **Multimedia.** Multimedia dissemination, encompassing pictorial, audio and video formats, may increase understanding, but requires careful editorial control and appropriately trained intelligence staff.

d. **Data.** Data is commonly presented as discrete facts or simple products of observation. A single piece of data often has little meaning in isolation, but may sometimes not be subject to further exploitation.

Section 8 – Monitoring and evaluation

3.48 Monitoring is the continual gathering and interpreting of information to maintain situational awareness and develop insight. It helps identify the extent to which objectives have been achieved. Evaluation draws upon monitoring activities and is the observation and interpretation of progress towards desired conditions against defined criteria. Monitoring and evaluation occurs as an assessment of the intelligence process. Intelligence personnel should assess the execution of the tasks they perform. To perform these assessments, intelligence personnel develop metrics to assess measures of performance (MOPs) and measures of effectiveness (MOEs). These measures are informed by a variety of indicators related to the conduct of intelligence tasks or their impact. The evaluation process promotes intelligence personnel understanding of the ways, means and ends required for decision-making.

Section 9 – Assessment

3.49 The primary focus at the operational and component levels of command is the execution of the operation, the creation of effects, and the achievement of the operational objectives defined in the operation plan (OPLAN). The operation is planned by the Joint Operations Planning Group (JOPG) and assessed by the Assessment Working Group (AWG). To ensure coherence, the commander and their staff design and agree to operational measurements and assessments at the JOPG, and the AWG provides the material for the Assessment Board briefing to the commander.

3.50 The operations assessments process is all activity that enables the measurement of progress and results of operations in a military context, and the subsequent development of conclusions and recommendations in support of decision-making.[35] It is essential to recognize that operations assessments are not isolated but considered across all levels of warfare to understand the strategic to tactical perspective. The operations assessment process involves four major steps:

- designing the operations assessment and support to planning;
- developing the data collection plan;
- data collection and treatment; and
- analysis, interpretation and recommendations.

3.51 Intelligence staff must be involved throughout the operations assessment process, providing an effective review, analysis and feedback service. It can involve both subjective and objective assessments to inform decision-making, through measuring different criteria such as: adversary or enemy capabilities and movements; mood and disposition of the population; rule of law; and economic indicators.

3.52 At the operational level, the process is based on the overall analysis of metrics from using a pre-agreed MOP linked to the extent of task accomplishment. From an intelligence perspective, this typically relates to the efficiency of collection activities and intelligence production. It may also relate to the retrospective evaluation of assessment validity in order to identify analytical blind-spots or bias. Secondly, using an MOE as they relate to the attainment of the desired end state. Are we doing the right things? In general, intelligence staff will need to support two aspects.

a. The first is broad in nature and seeks to answer the question: 'Are we accomplishing the mission?' This involves continuous monitoring and evaluation of all our effects and objectives, as well as the evaluation of desired and undesired effects across all the political, military, economic, social, infrastructure and information (PMESII) factors.

b. The second is more focused and supports the ongoing synchronization and execution of the campaign or operation. It is a short- to mid-term review of effects along particular lines of operation, and the evaluation of any special events or

[35] This is described in detail in Allied Command Operations, *Comprehensive Operations Planning Directive* (Interim) v3.0, (December 2020, Final Draft), Chapter 5.

situations that may arise.

Section 10 – Lessons Learned

3.53 A mature and fully functional Lessons Learned (LL) capability is crucial to the success of ongoing and future NATO operations and exercises and to the transformation of all NATO Bodies.

3.54 In an uncertain and continuously changing security environment, learning is an essential part of being credible, capable and adaptive in Intelligence Procedures development. Some lessons are spontaneously discovered without preparations while others are collected based on a guided plan made in advance.

3.55 In accordance with MC 0133/5 NATO'S OPERATIONS PLANNING, 11 September 2019, NATO has developed ways to improve the planning and conduct of ongoing and future operations, including through a better use of Lessons Learned, training, education and exercises.

3.56 The BI-SC Command Directive 080-006 Lessons Learned, describes the Lessons Learned structure, process and tools to be used within NATO, providing directions for implementing the NATO Lessons Learned Policy. The ACO Directive 080-001 Lessons Learned make available for leading the LL capability in Allied Command Operations (ACO), providing direction and guidance for SHAPE and subordinate commands concerning LL.

3.57 The NATO Lessons Learned process does not replace but supports the normal staffing of lessons through the chain of command.

3.58 NATO Lessons Learned Portal (NLLP). The NLLP is the single NATO tool for collection, managing, tracking, monitoring and sharing of lessons. The NLLP is established and managed by the JALLC (Joint Analysis Lessons Learned Centre), providing the needed regulations. NLLP runs on the NS WAN and is the only place in NATO where uploaded lessons can be tracked throughout the NATO LL Process providing transparency, accountability and as well, be visible for all others.

3.59 If considered relevant to be staffed and shared in accordance with the LL Process to become a Lesson Learned or Best Practice, all Observations related with Intelligence Procedures should be inserted in this portal, using the link:

http://nllp.jallc.nato.int/lessonlearned/Pages/SubmitObservation.aspx

Chapter 4 – Joint intelligence, surveillance and reconnaissance

Section 1 – Joint intelligence, surveillance and reconnaissance planning

4.1 Joint intelligence, surveillance and reconnaissance (JISR) planning is an integral part of the operations planning process (OPP) and must be included at the onset of all planning activities. This, along with the ability of the intelligence staff to provide and maintain continuous situational awareness and promote a shared understanding of the threat and the operating environment, also requires the continuous integration of newly acquired information. Through the joint intelligence preparation of the operational environment (JIPOE) process, intelligence analysts have the ability to evaluate, interpret and correlate newly acquired information to other items of information and finished intelligence held in databases to provide holistic knowledge to the commander and staff elements.

4.2 NATO missions demand a wide range of JISR capabilities to obtain optimal JISR results to support operations and missions. This necessitates having the capabilities, assets, skills, connectivity, tools and interoperability to meet information and operational requirements, ensuring a federation of networked-enabled capabilities and collaborative processes. Having the right capabilities and number of assets coupled with a comprehensive JISR architecture will provide the commander with the agility to respond to a constantly evolving environment. The key aspects of JISR have been included in Allied Joint Publication (AJP)-2.1, *Allied Joint Doctrine for Intelligence Procedures* where applicable but the detail is within AJP-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*.

Section 2 – Joint intelligence, surveillance and reconnaissance architecture

4.3 NATO's JISR architecture consists of the organizations, processes and systems connecting taskers, controllers, collectors, exploiters, analysts, databases, applications, producers and consumers of data, information and intelligence and operational data in a joint environment. The JISR architecture facilitates the management of JISR results, enables JISR functions and supports intelligence and operations functions at all levels. The JISR architecture consists of intelligence-related networks, applications, databases and metadata, including their structure, processes and the required connectivity. Consequently, the intelligence cycle and the JISR process must be seamlessly synchronized.

Section 3 – Joint intelligence, surveillance and reconnaissance synchronization

4.4 The ability of intelligence staff to continuously acquire new information relies on information collection activities and collection capabilities. JISR is a set of intelligence and operations capabilities to synchronize and integrate the planning and operation of all collection capabilities with the processing, exploitation and dissemination (PED) of the resulting information in direct support of the planning, preparation and execution of operations. JISR synchronizes intelligence activities, plans and other enabling staff functions by exploiting joint, multi-source and multidiscipline collection in coordination with established operational and intelligence processes and procedures to satisfy political and military

intelligence requirements. The intelligence requirements management and collection management (IRM&CM) process is critical to the effectiveness of the JISR process as it provides the 'gearing' to enable synchronization with the intelligence cycle.[36]

Section 4 – Joint intelligence, surveillance and reconnaissance approach

4.5 JISR is a multi-disciplined and methodical approach which synchronizes and integrates the planning and operations of all collection capabilities with PED of the resulting information in direct support of the planning, preparation and execution of operations. This approach comprises four distinct elements: joint; intelligence; surveillance; and reconnaissance, which are defined as follows.

a. **Joint.** The term 'joint' refers to activities, operations and organizations in which elements of at least two Services participate. Components and Services operate in a joint environment for greater effectiveness and efficiencies by integrating available intelligence, surveillance and reconnaissance (ISR) capabilities. JISR integration is not only the technical connection of various ISR data sources but also the operational integration, command and control and tactical employment of ISR capabilities.

b. **Intelligence.** The term 'intelligence' refers to the intelligence collection disciplines or collection capabilities/assets and the results these disciplines/ capabilities/assets can deliver to the commander and/or staff elements. Intelligence disciplines include acoustic intelligence (ACINT), human intelligence (HUMINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), open source intelligence (OSINT) and signals intelligence (SIGINT).

c. **Surveillance.** Surveillance is the systematic observation of aerospace, surface or subsurface areas, places, persons or things, by visual, aural, electronic, photographic or other means. Surveillance is designed to provide indications and warning of adversary initiative and threats and to detect changes in adversary activities. It can provide early warning of activity over a wide area or can focus upon a particular location, facility, activity or actor within the operating environment.

d. **Reconnaissance.** The term 'reconnaissance' refers to information-gathering methods that are conducted to answer a specific question about specific locations, facilities or people. It collects results through visual observation or other detection methods to provide specific information to the requester.

4.6 Both surveillance and reconnaissance can include visual observation (for example, soldiers on the ground covertly watching a target, unmanned aircraft systems (UASs) with cameras), as well as electronic observation. The difference between surveillance and reconnaissance has to do with time and specificity; surveillance is a more prolonged and deliberate activity, while reconnaissance missions are generally rapid and targeted to retrieve specific information.

[36] AJP-2.7(B), *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance* and Allied Intelligence Publication (AIntP)-14, *Joint Intelligence, Surveillance and Reconnaissance Procedures in Support of NATO Operations* provide more detail.

Section 5 – Joint intelligence, surveillance and reconnaissance process

4.7 The JISR process is a coordination process through which intelligence collection disciplines, collection capabilities and exploitation activities provide data, information and single source intelligence to address an intelligence requirement in a deliberate, ad hoc or dynamic time frame in support of operations planning and execution. The JISR process consists of five steps: task, collect, process, exploit and disseminate (TCPED). The outcome of the TCPED process is a JISR result.

4.8 These steps apply at all levels of command, across components, for any type of mission and in all operational environments. The JISR process provides commanders with specific data, information and intelligence to address an operational or intelligence collection requirement. The JISR process supports both current operational needs and, ultimately, the production of all-source intelligence.

4.9 To provide timely, relevant and accurate results to all levels of command, JISR operations require coordination, de-confliction and prioritization through JISR synchronization and integration activities to ensure the most effective and efficient use of capabilities. Within the JISR process, JISR synchronization activities are the responsibility of the intelligence staff while integration activities are the responsibility of the operations staff. The JISR TCPED process is synchronized with the direction, collection and processing steps of the intelligence cycle and is integrated with plan and direct phases of the decision cycle. The relationship of the JISR process to the intelligence cycle and operations is shown in Figure 4.1.

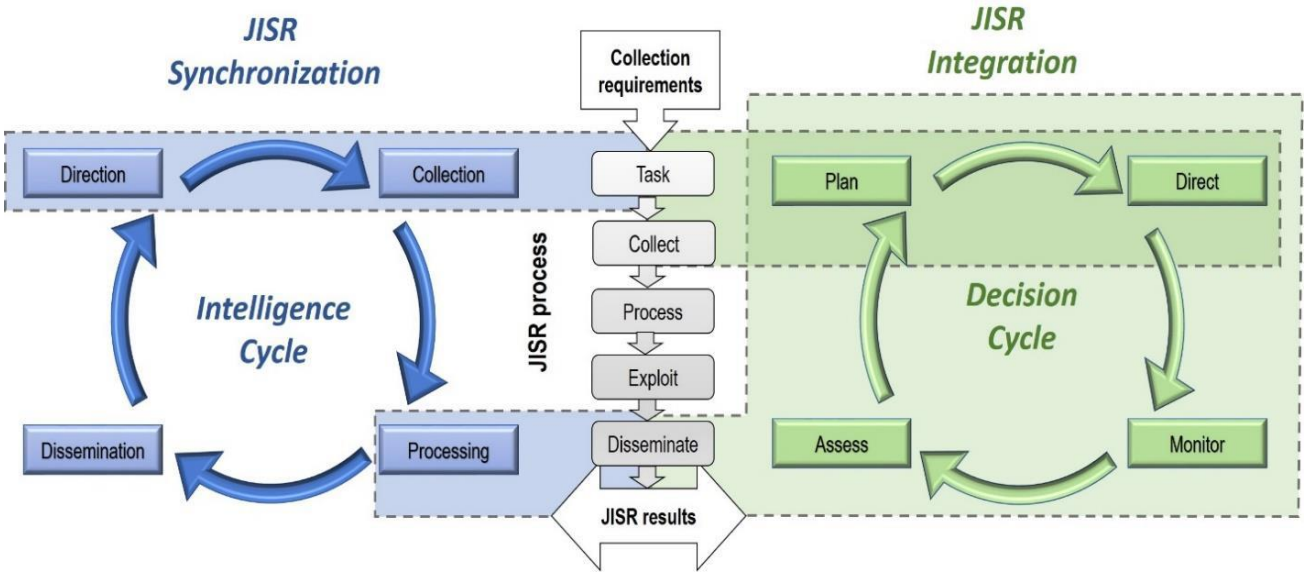


Figure 4.1 – Relationship between intelligence and decision cycles and joint intelligence, surveillance and reconnaissance process

Section 6 – Joint intelligence, surveillance and reconnaissance

collection management

4.10 The proliferation of collection capabilities coupled with the increasing importance and demands for timely, relevant, and actionable intelligence have resulted in an expanded set of tasks beyond the traditional collection management functions performed by the intelligence staff.

4.11 Collection management is a management staff function that converts intelligence requirements into collection requirements. This includes prioritizing, tasking, requesting or coordinating with appropriate collection capabilities, assets or commands and monitoring results and re-tasking as required.

4.12 Within the JISR framework, PED support should be based on the PED capacity of NATO, component and coalition partner capabilities and coordinated early on to ensure an intelligence architecture is in place to route data to predetermined PED nodes. A federated PED capability is the means for collected JISR data to be processed and exploited through different PED capabilities that are owned by other entities. Collection management is described in detail within in AJP-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance* and Allied Intelligence Publication (AIntP)-16, *Intelligence Requirement Management and Collection Management*. PED capacity can be owned by the entity in charge of collection (for example, multi-ISR aerial platforms with intelligence personnel as members of the aircrew) or can be based on a federated PED capability.

4.13 JISR collection management will be most effective if basic data held by member nations is accessible from the onset of a mission. Therefore respective repositories need to be synchronized wherever the same type of data is held. Wherever possible data fields are to be arranged in accordance with AIntP-3.

Chapter 5 – Intelligence support to targeting

Section 1 – Introduction

5.1 Intelligence supports joint tasks such as locating, identifying and analyzing adversaries, systems and potential targets to identify their value and vulnerability to an appropriate method of lethal or non-lethal action. Intelligence can then be used to allocate relative importance to adversaries, systems and potential targets, be they for lethal or non-lethal action in support of operational decisions. Targeting-intelligence staff support joint targeting by leading on target analysis, contributing on target system analysis and targeting strategy, and by providing a detailed picture of the threat's capabilities, structure, organization, intentions, objectives and vulnerabilities. The detail of the targeting process and intelligence support to the associated phases is described in detail in Allied Joint Publication (AJP)-3.9, *Allied Joint Doctrine for Joint Targeting*.

5.2 Joint intelligence preparation of the operational environment (JIPOE) is again utilized in this process and combined with target system analysis (TSA) to identify high-value targets (HVTs), high pay-off targets (HPTs), time sensitive targets (TSTs), and target sets (to include sex and age disaggregated data (SADD), where appropriate). Ideally before but also during operations, intelligence staff, in collaboration with other targeting staff, will further refine potential target sets, and target audiences as part of a TSA. This intelligence is used to allocate relative importance to targets, in support of operational decisions and the target prioritization process. These products also assist the joint coordination and synchronization staff element to identify targeting strategies during planning. Having identified adversaries, systems and potential targets to be a focus for a variety of potential effects, intelligence must support creating the desired effect.

5.3 During operations, intelligence staff are responsible to the commander for the timely and efficient development of targets in support of the commander's objectives. The intelligence staff, posted in the targeting cell, conduct two main functions:

- target development coordination via the target development working group (TDWG); and
- target list management (TLM) up to the point that targets are validated to the joint target list (JTL) or the restricted target list (RTL).

5.4 Advances in global communication technology has enabled federated target development, and intelligence staff may be called on to manage a global, federated, target development organization. The TDWG provides the forum for the intelligence staff, other targeting staff and subject matter experts to assign areas of target development, confirm or update target development priorities and tasks, relay future target development requirements and coordinate overall target material production. The TDWG also allows target development cells to identify their development progress, specialist analytic requirements and share intelligence gained on targets outside their area of operations. During the TDWG, it is important to evaluate the potential gain or loss of intelligence in case of engaging the considered target.

Section 2 – Intelligence targeting activities

Target intelligence production

5.5 Target intelligence production relies on a searchable and accessible integrated database as well as access to intelligence collection capabilities. The database should contain all identified entities within the area of responsibility, some of which could be considered to be potential targets or no-strike list (NSL) entities within a NATO area of intelligence interest. The NATO integrated database (IDB), maintained by Supreme Headquarters Allied Powers Europe (SHAPE), is created with contributions from NATO members, and other support organizations as required, to support NATO operations. The IDB contains all entities within the NATO area of intelligence interest, some of which could be considered to be potential targets or NSL entities. SHAPE will request nations to provide their information to the IDB. This provides the basis for Phase 2, Target development, of the joint targeting cycle (JTC). The IDB is kept under constant review to ensure currency and accuracy.

5.6 This provides the basis for TSA and entity-level target development during Phase 2 of the JTC. Target intelligence documents, including target material, are produced in a logical sequence that aligns with the three stages of target development: basic, intermediate, and advanced. As part of the target material production (TMP) process nations may, using their own resources, provide various specialized intelligence products (for example, geomatics products) in support of the targeting process. All target intelligence is stored in electronic target folders (ETF) on a database accessible by the NATO Joint Targeting System (N-JTS) targeting management software.

5.7 NATO relies on member states and NIFC to provide intelligence input and target material to enable an effective targeting process. Coordination of intelligence support from nations is made via SHAPE Centralised Targeting Capacity (CTC), who are authorized to engage directly with national intelligence and targeting organizations. Providing such support early in the operations planning process enhances NATO's ability to adopt a comprehensive approach.

Basic target development

5.8 Basic target development (BTD) begins the process of uniquely identifying, locating, describing, functionally characterizing, and subsequently databasing entity-level target details. The BTD standards are: identification, location and function.[37] Entity-level target development can occur very quickly for obvious military objectives, such as, a threat to a logistics node. The greater the complexity of a target, its elements or proximity to civilian structures and critical infrastructure, the greater the requirement for time and intelligence collection resources. The intelligence collection used in support of target development is tracked in the target package.

[37] Significance and Description are Part of ITD In CJCSI 3370.01. Only Facility Description is Part of BTD, Significance is Part of ITD.

Target analysis

5.9 To meet the commander joint task force's (JTF's) operational objectives, target behaviour must be changed/influenced in a manner that supports those objectives. Targets are categorized based on their type: facility, individual, virtual, equipment, or organization (FIVE-O) and the function they perform. The start point for target analysis is JIPOE. The JIPOE provides intelligence staff with a baseline for developing an understanding of target systems and/or intended audiences, as well as their relationship to existing entities and networks. Therefore, a full understanding of the information environment and cultural customs or conventions, the outcome of a gender analysis concerning gender norms, gender roles and gender relations needs to be taken into consideration will enable decision-makers' understanding of operational impacts during this process.

Target systems analysis cell

5.10 In coordination with the SHAPE CTC, the JTF should consider establishing a TSA cell under CTC responsibility, to deliver fused, all-source, intelligence analysis. Such a cell normally consists of a core all-source analytic team augmented by specialist advisors who coordinate and produce updated TSAs. The intelligence staff should, at a minimum, coordinate TSA production on behalf of the JTF by leveraging NATO and national reachback capabilities not necessarily collocated with the JTF. A reachback planning group can then establish a TSA community of interest to engage subject matter expertise from across the Alliance, both military and civilian, best suited to addressing the mechanism of any given target system.

Quality control

5.11 Quality control is an intelligence-led activity. It is a part of target development that assesses the accuracy of the supporting target intelligence. Quality control is a risk management process that informs the JTF or their designate during target validation. It provides a wider intelligence community consensus on the function associated with a target and its elements and also draws upon specialists who may be able to provide additional target intelligence. The Intelligence staff will coordinate quality control of target intelligence at least one command level above the JTF. NATO nations may also conduct their own quality control process prior to nominating targets to the commander JTF.

Intermediate target development

5.12 Intermediate target development (ITD) is the second stage of target development. Analysts fully characterize the entity, assessing possible threat system impact once the entity is affected and steps an adversary might take to mitigate loss of the target during hostilities. When ITD and quality control standards are met, as specified in the operation plan (OPLAN) Annex II – Targeting, the entity is placed on a candidate target list for validation.

Target validation

5.13 Target validation ensures nominated entities support the commander JTF's objectives, guidance, intent and desired effects, compliance with relevant international law and rules of engagement, and the accuracy and credibility of sources used to develop a

target. This process is a part of target development and involves validating entities from the candidate target list. Once validated, these entities can be included on the JTL or the RTL and be considered for inclusion on the Target Nomination List (TNL). The intelligence staff's role during target validation is to support the Target Validation Authority's (TVA) commander JTF's decision-making by providing an overview of target intelligence, including the accuracy and credibility of intelligence sources used to develop a target. Target validation authorities are delegated in relevant OPLANs/operation orders (OPORDs).

Advanced target development

5.14 Advanced target development (ATD) is a critical task supporting the JTF and the components. The provision of specialized ATD products, such as target coordinate mensuration (TCM) in support of weaponeering and collateral damage estimation (CDE), is one area where NATO members can provide a critical enabling capability to a JTF, coordinated as necessary by CTC. It is noted that NATO lacks some of the target automation tools and systems necessary during the ATD process, and therefore, relies on national capabilities for CDE, TCM and weaponeering.

Target nomination

5.15 Once potential targets are validated, they are nominated for approval via the Joint Targeting Coordination Board (JTCB). Nominated targets are prioritized based on the JFC's objectives, guidance and intent to maximize effective use of joint force capabilities while minimizing the likelihood of unintended and potentially undesired effects. Validated targets are placed on either the JTL or the RTL and once prioritized, approved to the Joint Prioritized Target List (JPTL). Intelligence staff use the JPTL to coordinate target intelligence collection requirements in support of combat assessment.

5.16 SHAPE CTC will maintain a dedicated target intelligence database that will include all relevant target intelligence gathered during peacetime target development activities, and submissions from subordinate headquarters. This database will provide an intelligence foundation to inform JTF planning and establish target development and engagement priorities. NATO member states are encouraged to contribute intelligence to the target intelligence database. Requests for other target intelligence are made through appropriate command channels using the intelligence requirements management and collection management (IRM&CM) process.

Security and accountability

5.17 Regardless of storage or dissemination methods, all target intelligence and target material products are to be correctly classified and caveated from the outset. Distribution to NATO users through targeting software and databases is provided on a strict need-to-know basis and is only to be handled by those personnel with the appropriate clearances.

Intelligence support activities by phase of the joint targeting cycle

5.18 Intelligence support to the JTC is provided not only by intelligence staff, but by other elements of the intelligence community. Contributions by all-source intelligence analysts, imagery analysts, human or signals intelligence specialists, among others, contribute to the

provision of intelligence support to targeting. The JTC is inextricably linked to the joint intelligence, surveillance and reconnaissance (JISR) process and feeds the planning process. Throughout the joint targeting process, intelligence staff will identify and coordinate collection and exploitation requirements, manage the targeting database and manage target lists. The key intelligence activities by JTC phase are depicted in Figure 5.1.

Joint Targeting Cycle Phase	Intelligence Support Activities
Phase 1: Commander's intent, objectives and targeting guidance	Identify vulnerabilities, provide indicators and warnings, initiate joint intelligence preparation of the operational environment (JIPOE) analysis, develop Measures of Performance (MoP) and Measures of Effectiveness (MoE).
Phase 2: Target development	Conduct target analysis to identify, describe and characterize entities that when engaged by specific means will create the Commander's desired effects. Update all target development products on a continuous basis.
Phase 3: Capabilities	Determine the functional characterization of the target, identify risk factors and likely effects and damage to protected objects and functions.
Phase 4: Commander's decision, force planning and assignment	Continue to support the planning and decision-making process. Support the prioritization of joint prioritized target list (JPTL) targets for joint intelligence, surveillance and reconnaissance (JISR) collection and completing the target validation process.
Phase 5: Mission planning and force	Review target intelligence for currency and accuracy and support post-engagement assessment.
Phase 6: Assessment	Conduct and coordinate BDA activities and support operational and campaign assessments. Assess effects on the system and help update Target system analysis.

Figure 5.1 – Key intelligence activities within the joint targeting cycle

Other intelligence outputs – battle damage assessment

5.19 Battle damage assessment (BDA) consists of physical and functional damage assessment and target systems assessment. It is defined as: 'the assessment of effects resulting from the application of military action, either lethal or non-lethal, against a military objective.'

5.20 Such assessment is primarily an intelligence staff responsibility, but it is also closely linked with the wider targeting process. The need for BDA will create a series of post-attack intelligence requirements and intelligence staff should establish effective procedures to support BDA.

Intentionally blank

Lexicon

Part 1 – Acronyms and abbreviations

AAP	Allied administrative publication
ACINT	acoustic intelligence
ACO	Allied Command Operations
ACOS	assistant chief of staff
AII	area of intelligence interest
AIntP	Allied intelligence publication
AIR	area of intelligence responsibility
AJP	Allied joint publication
ATD	advanced target development
AWG	Assessment Working Group
BDA	battle damage assessment
BTD	basic target development
CATL	candidate target list
CCIR	commander's critical information requirement
CDE	collateral damage estimation
CJSOR	combined joint statement of requirements
COA	course of action
CoG	centre of gravity
CONOPS	concept of operations
COPD	Comprehensive Operations Planning Directive
CR	collection requirement
CR-SGBV	conflict-related sexual and gender based violence
CTC	Centralised Targeting Capacity
CTL	collection task list
CXP	collection and exploitation plan
DSM	decision support matrix
EEI	essential elements of information
ETF	electronic target folders
FIVE-O	facility, individual, virtual, equipment, or organization
GENAD	gender advisor
GEOINT	geospatial intelligence
HNAT	human network analysis and support to targeting
HUMINT	human intelligence
HVT	high-value target
ICP	intelligence collection plan
ICPP	intelligence collection and processing planIDB integrated database

IMINT	imagery intelligence
IRM	intelligence requirement management
IRM&CM	intelligence requirements management and collection management
ISR	intelligence, surveillance and reconnaissance
ISSR	intelligence, surveillance and reconnaissance request
ITD	intermediate target development
JALLC	Joint Analysis and Lessons Learned Centre
JCB	Joint Coordination Board
JIPOE	joint intelligence preparation of the operational environment
JISR	joint intelligence, surveillance and reconnaissance
JOC	joint operations centre
JOPG	Joint Operations Planning Group
JPTL	joint prioritized target list
JTC	joint targeting cycle
JTCB	Joint Targeting Coordination Board
JTF	joint task force
JTL	joint target list
JTWG	Joint Targeting Working Group
MASINT	measurement and signature intelligence
MC	Military Committee (NATO)
METOC	meteorological and oceanographic
MOE	measure of effectiveness
MOP	measure of performance
MoU	memorandum of understanding
NAC	North Atlantic Council
NAI	named area of interest
NATO	North Atlantic Treaty Organization
N-JTS	NATO Joint Targeting System
NLLP	NATO Lessons Learned Portal
NSL	no-strike list
OLPP	operational-level planning process
OPLAN	operation plan
OPORD	operation order
OPP	operations planning process
OSINT	open source intelligence
PED	processing, exploitation and dissemination
PIR	priority intelligence requirement
PMESII	political, military, economic, social, infrastructure and information
RFI	request for information
RTL	restricted target list
SAB	situational awareness brief
SACEUR	Supreme Allied Commander Europe

SADD	sex and age disaggregated data
SHAPE	Supreme Headquarters Allied Powers Europe
SIGINT	signals intelligence
SIR	specific intelligence requirement
SOP	standing operating procedure
STANAG	NATO standardization agreement
TCM	target coordinate mensuration
TCPED	task, collect, process, exploit and disseminate
TDWG	target development working group
TLM	target list management
TMP	target material production
TSA	target system analysis
TST	time sensitive target
TTP	tactics, techniques and procedures
TVA	Target Validation Authority
UAS	unmanned aircraft system
VISCOL	visual collation

Part 2 – Terms and definitions

actor
A person or organization, including state and non-state entities, within the international system with the capability or desire to influence others in pursuit of its interest and objectives. (This term may have changed – since written as it was a new term and definition and will be processed for NATO Agreed status.)

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

analysis
In intelligence usage, a step in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation.
Notes: The analysis identifies and extracts the pieces of information relevant to the intelligence requirement. (NATO Agreed)

area of intelligence responsibility
The area for which a commander has the responsibility to provide intelligence with the means available. (NATO Agreed)

area of operations
An area within a joint operations area defined by the joint force commander for conducting tactical level operations. (NATO Agreed)

basic intelligence
Intelligence, derived from any source, that may be used as reference material for planning and as a basis for processing subsequent information or intelligence.
Notes: Basic intelligence is fused from all available data, information, joint intelligence, surveillance and reconnaissance results, single-source intelligence and all-source intelligence and it is fundamental to current intelligence. (NATO Agreed)

battle damage assessment
The assessment of effects resulting from the application of military action, either lethal or non-lethal, against a military objective. (NATO Agreed)

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

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

current intelligence
Intelligence which reflects the current situation at either strategic or tactical level. (NATO Agreed)

deception
Deliberate measures to mislead targeted decision-makers into behaving in a manner advantageous to the commander's intent. (NATO Agreed)

evaluation
In intelligence usage, an activity in the processing phase of the intelligence cycle consisting in an appraisal of the quality of the reported information, which is key to determining the reliability of the originator or source and the credibility of the information. (NATO Agreed)

geospatial
Of or related to any entity whose position is referenced to the Earth. (NATO Agreed)

human network analysis and support to targeting
An intelligence process intended to provide understanding of the organizational dynamics of human networks and recommends individuals or nodes within those networks for interdiction, action, or pressure. (NATO Agreed)

indicator
In intelligence usage, an item of information, which reflects the intention, or capability of a potential enemy to adopt or reject a course of action. (NATO Agreed)

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

integration
An activity in the processing phase of the intelligence cycle whereby analysed information and/or intelligence is selected and combined into a pattern in the course of the production of further intelligence. (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 architecture
A structure that consists of the overall organization and hierarchy, processes and systems within which the NATO military intelligence structure interacts and operates with other national and international agencies and organizations to support decision-makers at all levels. (NATO Agreed)

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

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

intelligence requirement
A statement that provides the rationale and priority for an intelligence activity, as well as the detail to allow the intelligence staff to satisfy the requirement in the most effective manner.
Notes:
1. Intelligence requirements should cover the broad scope of information on the political, military, economic, social, infrastructure and information spectrum.
2. The military spectrum will be covered by the commander's critical information requirement.
3. Military types of intelligence requirements are: priority information requirements, specific intelligence requirement and essential elements of information. (NATO Agreed)

intelligence requirements management
The management function that develops, validates and prioritizes intelligence requirements, forwards validated intelligence requirements to the collection management function, and oversees dissemination of the intelligence products. (NATO Agreed)

intelligence, surveillance and reconnaissance request
A formal request for joint intelligence, surveillance and reconnaissance assets from adjacent or subordinate commands to support their prioritized intelligence requirements for a specific mission, operation or time period. (NATO Agreed)

interpretation
In intelligence usage, an activity in the processing phase of the intelligence cycle during which the significance of information or intelligence is judged in relation to the current body of knowledge. (NATO Agreed)

joint intelligence, surveillance and reconnaissance
An integrated intelligence and operations set of capabilities, which synchronises and integrates the planning and operations of all collection capabilities with the processing, exploitation, and dissemination of the resulting information in direct support of the planning, preparation, and execution of operations. (NATO Agreed)

joint prioritized target list
A prioritized list of targets approved and maintained by the joint force commander. (This term is a new term and definition in AJP-3.9 and will be processed for NATO Agreed status)

joint target list
A consolidated list of selected but unapproved targets considered to have military significance in the joint operations area. (Not NATO Agreed)

medical intelligence
Intelligence derived from medical, bio-scientific, epidemiological, environmental and other information related to human or animal health.
Notes: The intelligence being of a specific technical nature, requires medical expertise throughout its direction and processing within the intelligence cycle. (NATO Agreed)

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

reconnaissance
A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an adversary or potential adversary; or to secure data concerning the meteorological, hydrographical or geographic characteristics of a particular area. (NATO Agreed)

sensor
An equipment which detects, and may indicate, and/or record objects and activities by means of energy or particles emitted, reflected or modified by objects. (NATO Agreed)

specific intelligence requirement
An intelligence requirement that supports and complements each priority intelligence requirement and provides a more detailed description of the requirement. (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)

surveillance
The systematic observation across all domains, places, persons or objects by visual, electronic, photographic or other means. (NATO Agreed)

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

target
An area, structure, object, person or group of people against which lethal or non-lethal

capability can be employed to create specific psychological or physical effects.
Note: The term ‘person’ also covers their mindset, thought processes, attitudes and behaviours. (NATO Agreed)

targeting
The process of selecting and prioritizing targets and matching the appropriate response to them taking into account operational requirements and capabilities. (NATO Agreed)

target intelligence
Intelligence, derived from any source, that is used for targeting purposes.
(NATO Agreed)

time sensitive target
Those targets requiring an immediate response because they pose (or will soon pose) a danger to friendly forces or are highly lucrative, fleeting targets of opportunity whose destruction is of high priority to achieve campaign objectives. The time available does not allow for the standard targeting timeline to be followed. (Not NATO Agreed)

visual collation
A traditional means of overlaying activity onto a map in order to discern patterns, trends and clusters to aid in analysis. This can be done on a GIS, PowerPoint or paper mapping using talc overlays. VISCOL provides a simple but effective 'common intelligence picture'; a more advanced picture, and analysis can be provided by GEOINT and geospatial support to intelligence.
(New NATO term to be agreed)

Terminology

Although complex, AJP-2.1 aims to describe intelligence procedures as simply as possible. Consequently, while there may be different abbreviations and terms in use, this document uses one set throughout, acknowledging differences as required and aligning with NATOTerm wherever possible. Specifically, the following terms are used.

a. **Commander.** The commander is the authority, at any level, who requires intelligence to support decision-making.

b. **Intelligence staff.** Intelligence specialists who are involved in the direction, collection, production and dissemination of intelligence.

c. **Intelligence.** Intelligence is defined as: 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.[38]

d. **Intelligence requirements.** Intelligence requirements provide the rationale and priority for any intelligence activity as well as providing the detail to allow the intelligence staff to answer the requirement in the most effective manner. Intelligence requirements should cover the broad scope of information on the political, military, economic, social, infrastructure and information (PMESII) model. PMESII will be covered by the commander's critical information requirements (CCIRs). Types of intelligence requirements are: priority intelligence requirements (PIR); specific intelligence requirement (SIR); and essential elements of information (EEI).[39]

e. **Intelligence requirements management.** A set of integrated management processes and services which: validate, summarize and prioritize incoming intelligence requirements; initiates the collection of associated information; quality controls processed outputs; and oversees dissemination of intelligence products. This management process is led by the intelligence staff or agency.

f. **Collection management.** In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection capabilities or agencies, monitoring results and re-tasking, as required by making best use of the collection capabilities.

g. **Intelligence requirements management and collection management.** The combination of intelligence requirements management and collection management, which provides a set of integrated management processes and services to satisfy the intelligence requirements, by making best use of the available collection capabilities.

h. **Joint intelligence, surveillance and reconnaissance.** An integrated intelligence

[38] NATO Agreed.
[39] AJP-2.

and operations set of capabilities, which synchronizes and integrates the planning and operations of all collection capabilities with processing, exploitation and dissemination of the resulting information in direct support of planning, preparation, and execution of operations.

Intentionally blank

AJP-2.1(B)(3)