NATO STANDARD

AJP-2.1

ALLIED JOINT DOCTRINE FOR INTELLIGENCE PROCEDURES

Edition B Version 1

RATIFICATION DRAFT 1

XXXX 201x

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

Published by the

NATO STANDARDIZATION OFFICE (NSO)

(INTENTIONALLY BLANK)

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

date

1. The enclosed Allied Joint Publication AJP-2.1, Edition B, Version 1, *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 1, is effective upon receipt and supersedes AJP-2.1(A) which should be destroyed in accordance with the local procedure for destroying documents.

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

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

(INTENTIONALLY BLANK)

RESERVED FOR NATIONAL LETTER OF PROMULGATION

(INTENTIONALLY BLANK)

RECORD OF RESERVATIONS

Chapter	Record of reservation by nations
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

(INTENTIONALLY BLANK)

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

(INTENTIONALLY BLANK)

References

MCM-0077-2000	*Military Committee Guidance on the Relationship between NATO Policy and Military Doctrine*
MC 0114	*Procedures for Production of NATO Agreed Intelligence*
MC 0128	*Policy Guidance for NATO Intelligence*
MC 0133	*NATO Operations Planning*
MC 0161	*NATO Strategic Intelligence Estimate*
MC 0166	*NATO Intelligence Warning System*
MC 0327	*NATO Military Policy for non-Article 5 Crisis Response Operations*
MC 0582/1	*NATO Joint Intelligence, Surveillance and Reconnaissance Concept*
MC 0600	*NATO Policy on Knowledge Development*
Bi-MNC	Reporting Directive 80-3 Volume II – *Intelligence Reports*
AJP-01	*Allied Joint Doctrine*
AJP-2	*Allied Joint Doctrine for Intelligence, Counter-intelligence and Security*
AJP-2.7	*Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*
AJMedP-3	*Allied Joint Medical Intelligence Doctrine*
AJP-3	*Allied Joint Doctrine for the Conduct of Operations*
AJP-3.9	*Allied Joint Doctrine for Joint Targeting*
AJP-5	*Allied Joint Doctrine for Operational-Level Planning*
AAP-06(2014)	*NATO Glossary of Terms and Definitions*
AAP-03	*Production, Maintenance and Management of NATOs Standardization Documents*
AAP-47	*Allied Joint Doctrine Development*
AAP-32	*Publishing Standards for Allied Publications*

Intentionally blank

Preface

Context

1. **Character of doctrine.** Doctrine is defined by the North Atlantic Treaty Organization (NATO) as: *fundamental principles by which the military forces guide their actions in support of objectives. It is authoritative but requires judgement in application.*[1] The clear understanding and acceptance of doctrine by Allied joint forces is a prerequisite for the successful conduct of operations. It evolves as its political and strategic foundation changes and in the light of new technology, lessons identified and the insights of operational analysis.

Scope

2. NATO doctrine for intelligence procedures is primarily intended for NATO forces. It could also be applied multi-nationally within the framework of an allied joint force. This can include, with adaptations agreed by participating nations where necessary, its utilization for operations under other international mandates, or as part of a coalition of NATO and non-NATO nations (when such utilization would not be against NATO's interests). Interoperability between NATO nations in these instances will be based upon NATO standardization agreements, other policy documents and publications. Allied Joint Publication (AJP)-2.1, *Allied Joint Doctrine for Intelligence Procedures*:

- focuses on the intelligence and requirement management functions;
- builds on the key themes set out in AJP-2(A) *Allied Joint Doctrine for Intelligence, Counter-intelligence and Security*; and
- provides an authoritative basis for intelligence procedures to support NATO operations.

3. **Meeting the security challenge.** The Alliance continues to adapt to the security situation it faces. The security environment contains a broad and evolving set of challenges for NATO, the territory of its Nations and their populations. Alliance security strategy remains focused on three core tasks: collective defence; crisis management; and cooperative security. Today, the Euro-Atlantic area is at peace and the threat of a conventional attack against NATO territory is low. However, the threat posed by both conventional and hybrid threats cannot be ignored. Many regions and countries around the world are witnessing the acquisition of substantial, modern military capabilities with consequences for international stability and Euro-Atlantic security that are difficult to predict. The proliferation of nuclear weapons and other weapons of mass destruction, and their means of delivery, threatens

[1] NATO Agreed – NATOTerm.

incalculable consequences for global stability and prosperity. Terrorism poses a direct threat to the security of the citizens of NATO countries, and to international stability and prosperity more broadly. Extremist groups continue to spread to, and grow in, areas of strategic importance to the Alliance. Modern technology increases the threat and potential impact of terrorist attacks, in particular if terrorists were to acquire nuclear, chemical, biological or radiological capabilities. Instability or conflict beyond NATO borders can directly threaten Alliance security, including by fostering extremism, terrorism and transnational illegal activities such as trafficking arms, narcotics and people. All countries are increasingly reliant on the vital communication, transport and transit routes on which international trade, energy security and prosperity depend. They require greater international efforts to ensure their resilience against attack or disruption. Thus, operations are likely to be conducted at some distance from the allies' home bases, and the demands of expeditionary operations will continue to be a significant cause of change. Key environmental and resource constraints, including health risks, climate change, water scarcity and increasing energy needs will further shape the future security environment in areas of concern to NATO and have the potential to significantly affect NATO planning and operations.

Purpose

4. The purpose of AJP-2.1 is to describe, primarily at the operational level, the generic procedures, interdependencies, and considerations required to conduct intelligence operations in support of peacetime and crisis operations. It specifically concentrates on the intelligence and requirement management and collection management functions of intelligence, while leaving AJP-2.7(B), *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*[2] to provide detail on joint intelligence, surveillance and reconnaissance operations. In addition, it covers intelligence support to joint tasks, specifically joint targeting.

Application

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

[2] This AJP will replace the current AJP-2.7, *Allied Joint Doctrine for Reconnaissance and Surveillance*.

Target audience

6. The framework used in AJP-2.1 provides a common understanding of generic intelligence procedures and intelligence-supported processes at all levels of NATO. It is mainly written for those charged with delivering multi-source intelligence to joint operational-level commanders.

Content

7. AJP-2.1 is divided into four chapters, with annexes to provide detail where appropriate.

   a. **Chapter 1.** Describes the background and aim of the publication.

   b. **Chapter 2.** Discusses planning considerations for intelligence operations.

   c. **Chapter 3.** Describes the procedures and processes involved within the intelligence cycle and the coherence between intelligence procedures and JISR.

   d. **Chapter 4.** Describes intelligence support to joint tasks, with a specific focus on intelligence support to targeting, both lethal and non-lethal.

Linkages

8. This publication is one of two supporting joint doctrine publications of AJP-2. AJP-2.7 sits alongside AJP-2.1 and provides detail on the planning, direction and execution of joint intelligence, surveillance and reconnaissance operations.

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

CHAPTER 1 – BACKGROUND AND AIM

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; where adversaries and other actors[3] alike compete with each other across a broad range of environments. Intelligence is crucial to develop this understanding and it must provide the insight[4] and foresight[5] commanders will need to make decisions.

1.2. Intelligence has an important part to play in contributing to NATO's three core tasks:

- collective defence;
- crisis management; and
- cooperative security.[6]

1.3. Intelligence contributes to these tasks by supporting decision-making, across the full spectrum of NATO engagement and operations.[7] The spectrum of operations can range from large-scale, high intensity, Article 5 operations, through to the seven missions anticipated for the NATO Response Force (NRF).[8]

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 task and means to ends by applying suitable ways. The ends are the objectives that it wishes to accomplish; the ways are the procedures to be employed in accomplishing such objectives; and the means are the capabilities to be employed.

---

[3] The proposed definition for the term actor is: *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 is a new term and definition and will be processed for NATO Agreed status.)

[4] Insight is knowing 'why' an event has happened or is happening.

[5] Foresight is being able to identify and anticipate what 'may' happen.

[6] *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, Lisbon 2010.

[7] See Allied Joint Publication (AJP)-01, *Allied Joint Doctrine*.

[8] The seven NATO Response Force missions are: non-combatant evacuation operations (NEO); humanitarian response; crisis response; counter terrorism; embargo operations; initial entry force and demonstrative force.

1.5. **Ends.** In the context of intelligence, the end is the requirement to support planning, decision-making and operations, with insight and foresight, via timely and accurate intelligence assessments.

1.6. **Ways.** The generic ways are described in this doctrine publication. They provide an overarching framework for the end-to-end management of intelligence requirements, information collection, and production 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.[9]

1.7. **Means.** The means, that is to say the intelligence collection capabilities, are varied in nature and can operate across the spectrum of operations. Some of these capabilities are introduced in AJP-2.7(B), *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance* and described in detail in other AJP-2-series doctrine publications and subordinate publications describing detailed tactics, techniques and procedures.

Aim

1.8. The aim of AJP-2.1 is to describe, primarily at the operational level, the generic procedures, interdependencies, and considerations required to conduct intelligence operations in support of peacetime and crisis operations. It specifically concentrates on the intelligence and requirement management functions (including the specific support to joint targeting), while leaving AJP-2.7(B) to provide detail on the planning, direction and execution of joint intelligence, surveillance and reconnaissance operations. 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 multi-source intelligence to joint operational-level commanders.

1.9. AJP-2.1 informs wider joint intelligence and joint intelligence, surveillance and reconnaissance (JISR) capabilities (including the respective commands/units/ detachments/assets and other underlying structures), who will have closely-related functions to perform. It also describes in some detail how intelligence operations are conducted within a generic formation or organization. In doing so, it offers authoritative guidance that requires judgment in application, and should be used to influence subordinate documents.

1.10. The main difference between AJP-2.1(B) and the previous version (A) is the rationalization of content. Previous background material, which introduces intelligence in general, has now been removed to AJP-2(A), *Allied Joint Doctrine for Intelligence, Counter-intelligence and Security*. Also, specific detail regarding how to

[9] The intelligence cycle comprises direction, collection, processing and dissemination. It can be conducted at strategic, operational and/or tactical levels simultaneously.

conduct intelligence analysis has been removed; this should be included in a more appropriate doctrine publication in due course. Overall, this version of AJP-2.1 is more streamlined and focuses on the generic procedures that underpin the planning and delivery of intelligence and the relationship with JISR, which is detailed in AJP-2.7.

Approach

1.11. In adopting this more focused approach, AJP-2.1 should support the development of the NATO JISR Concept and the development of the NRF.[10] The application of this doctrine will promote a fully interoperable and collaborative intelligence environment to support decision-makers at all levels, as well as among all NATO and partner nations.

1.12. The central tenet of intelligence procedures is the application of the intelligence cycle, comprising: direction; collection; processing; and dissemination. The intelligence cycle can be conducted at the strategic, operational and tactical levels simultaneously and cycles at a specific level and in a specific organization can run concurrently.

1.13. The central theme which runs through AJP-2.1 is intelligence requirements management (IRM) and collection management (CM)[11] which describes a complex management function inside a staff. IRM and CM is a set of integrated management processes and services to satisfy the intelligence requirements by making best use of collection capabilities. IRM is a complex management function that:

- develops, validates and prioritizes commanders' intelligence requirements;[12]
- coordinates the collection of associated information;
- quality controls processed outputs; and
- oversees dissemination of intelligence to customers.

1.14. It is this seamless procedure that connects requests, collection tasks, production activity and dissemination that provides the foundation of the intelligence cycle. Ultimately, IRM combined with CM, underpins the intelligence cycle. It is important to remember that IRM and CM are management functions inside a staff and not an individual. Equally, although IRM is closely related to CM, they are separate management functions.

[10] MC 0582/1, dated 31 May 2013.

[11] IRM and CM can be associated with the former term collection coordination intelligence requirement management (CCIRM).

[12] Including tasks given by higher commanders.

Terminology

1.15. 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 Allied Administrative Publication (AAP)-06, *NATO Glossary of Terms and Definitions* 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*.[13]

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.[14] 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).[15]

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

[13] NATO Agreed, AAP-06(2014).

[14] The operational environment can be initially viewed through several conceptual models. The most common in NATO are the six listed PMESII domains. But other models do exist. See AJP-2(A).

[15] AJP-2(A): Chapter 5.2.4.

coordinating with appropriate collection capabilities or agencies,[16] 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 IRM and CM, 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 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.[17]

[16] Agency is defined as: *in intelligence usage, an organization or individual engaged in collecting and/or processing information*. (NATO Agreed – NATOTerm)
[17] AJP-2(A).

Intentionally blank

CHAPTER 2 – PLANNING INTELLIGENCE OPERATIONS

Section 1 – Introduction

2.1. Supreme Allied Commander Europe's (SACEUR's) terms of reference[18] detail responsibilities for areas of responsibility (AOR) and areas of interest (AOI), including those beyond NATO's territory. Specifically, they describe the need to monitor and analyse 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 (NCRSM) and Military Committee (MC) 0166 series (NATO Intelligence Warning System (NIWS)) provide more detail on SACEUR's role in indications and warning of potential or actual crises. Allied Command Operations Directive (AD) 65-11[19] provides the complementary direction and guidance.

2.3. NATO uses the categories of strategic, operational and tactical to categorize echelons of command and operations activities.[20] These levels of warfare provide a framework within which to rationalize and categorize military intelligence activity. However, 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 will be required to contribute to, and synchronize with, planning and operations at all these levels and must act seamlessly with J3 Operations and J5 Plans activities.[21] 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 critical information requirements (CCIRs).

2.5. Intelligence procedures must adapt as the mission develops and requirements change; they should also recognize a number of guiding principles.[22]

---

[18] MC 0053-4, 12 April 2010.

[19] Allied Command Operations Directive (AD) 065-11 – *Standing Policy and Procedures for Intelligence Production Management*, March 2013.

[20] See Military Committee (MC) 0133/4, *NATO's Operations Planning*. See MC 0586 (Final), *Military Committee Policy for Allied Forces and their Use for Operations* for further detail.

[21] 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 Operational-Level Planning*.

[22] AJP-3, Chapter 1.

a. **Proactive engagement.** Proactive engagement by intelligence staffs, ideally ahead of a crisis, enables coordinated approaches to complex situations and allows more sensitive responses. Significantly, this requires an analytical approach to the collection and interpretation of crisis indicators and warnings in order to inform and direct planning and increase the available time for reaction.

b. **Shared understanding.** A shared understanding between parties, including military and civilian entities, is essential to optimize the effectiveness of their various capabilities. Each party contributes, exploiting its training, techniques and its own perception, offering additional perspectives, depth and resilience. Wherever possible, shared understanding should be engendered through cooperative working practices, synergy and integrated joint training with common principles.

c. **Outcome-based thinking.** All NATO participants involved in crisis resolution need to base their thinking on outcomes and what is required to deliver a favourable situation, when planning and conducting activities. Leadership, cohesion and coherence will be required to ensure that all NATO actors work towards agreed objectives that are outcome-based and consistent with the various national strategic aims. NATO planning and activity should be focused on a single purpose and progress judged against mutually agreed measures of effectiveness.

d. **Collaborative working.** Although NATO will likely have some organic and dedicated intelligence surveillance and reconnaissance assets, nations will still need to collaborate to deliver overall capability. Institutional familiarity, generated through personal contact and human networking, enhances collaborative working and mutual trust. Integrated information management, infrastructure and connectivity enable information sharing, confidence building and common working practices across communities of interest, including shared review and reporting. Getting NATO nations collaborating and coordinating early is essential. Intelligence sharing is a vital component of this process, and must take place between civilian and military intelligence organizations.

Section 2 – Intelligence architecture

2.6. Intelligence architecture is defined as: *the overall space, condition, surroundings, 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*.[23] The architecture should, therefore, be flexible

[23] This is a proposed definition and will be processed for NATO Agreed status.

and tailored to the demands and circumstances of the operation. In the broadest sense, the intelligence architecture will contribute to enhancing decision-making, joint effects, and effective movement 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 provided by joint intelligence, surveillance and reconnaissance (JISR).[24] 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 from all available collection capabilities to, from and 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.[25] These are not exhaustive and there may be a need for greater emphasis on some more than others, but, intelligence planning at the strategic, operational and tactical levels has to be conducted in pursuit of these principles in order to successfully support the campaign.[26]

2.8. In essence, these principles promote the idea that the intelligence effort 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. The intelligence architecture is a collaborative endeavour involving all members of the intelligence community. It aims to harmonize the intelligence process to achieve the optimal use of intelligence specialists, agencies, collection capabilities and activities to produce the best possible insight and foresight. Establishing and maintaining a dynamic intelligence architecture is critical to establish an effective framework and the conduct of intelligence operations in the contemporary and future operating environment.

2.10. The intelligence architecture is built upon personal relationships just as much as physical capabilities. It is the overall space, conditions and surroundings through which the military intelligence structure interacts and operates with other national and

[24] ACO's Annex to 3520/SH IPA/245/12-Tr 301238, dated 17 December 2012.

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

[26] In addition to the principles defined above, which apply to all operations, campaign themes such as peace support, stabilization or humanitarian assistance may also require a number of additional considerations, for example, environmental protections, further described in AJP-01, *Allied Joint Doctrine*.

international information and intelligence agencies to support decision-makers at all levels. The keys to its success are:

- educating and training NATO personnel and friendly forces: promoting a positive attitude, including reserve forces;
- making the best use of Alliance and national capabilities (including information systems);[27]
- maintaining inter-Service, cross-government and multinational links;
- bridging boundaries between the operating environments of maritime, land, air, space and cyberspace;
- removing historical distinctions between the strategic, operational and tactical levels of intelligence activity;
- driving fusion and integration at all levels; and
- networking systems to enable the effective operation of the diverse competencies within the intelligence architecture.

Section 3 – Intelligence planning

Strategic-level planning

2.11. Although AJP-2.1(B) is aimed 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.

2.12. The NATO crisis management process consists of successive phases that generally conform with the cycle of a crisis.[28] There are six phases;[29] which are described in detail in the following sub-sections:

- Phase 1 – Indications and warning;
- Phase 2 – Strategic assessment;
- Phase 3 – Military response options;
- Phase 4 – Strategic plan development;

[27] This is achieved through intelligence prioritization, coordination and management across all levels through intelligence requirement management (IRM) and collection management (CM).
[28] AJP-5.
[29] AJP-5.

- Phase 5 – Execution; and
- Phase 6 – Transition.

2.13. Progression through each phase is not automatic and will be guided by higher-level decision-making. The phases do not have precise boundaries and may overlap. Moreover, they may be repeated depending on the changing circumstances during the life-cycle of a crisis.

2.14. Multiple phases may also be compressed into a single phase if the emerging or ongoing situation so warrants. In the case of an emerging time-sensitive collective defence situation, planning and execution process, Phases 2 and 3 (covering the political, military estimate process) may be compressed and initiation of Phase 4 and following phases accelerated. Phases 5 and 6 may also overlap.

The operations planning process

2.15. The NATO crisis management process is supported by the operations planning process (OPP). Figure 2.1 illustrates the OPP and its interface across the strategic and operational levels.

Figure 2.1 – The operations planning process

2.16. **Phase 1 – Indications and warning.** In this phase the strategic-military level will begin to develop situational awareness on the issue to support the development of strategic assessments, planning products and directives. It involves the initial consideration of information on a particular issue that is of potential interest to the Alliance. This may have come to light through horizon scanning (including indicators and warnings) or other information provided by the intelligence community. Such activity is cyclic and continuous. Planning conducted at the strategic level will support the operational level and help satisfy intelligence requirements at the operational level and inform the joint intelligence preparation of the operational environment (JIPOE) process (which is described later).

2.17. Horizon scanning is a collaborative effort drawing on all NATO political and military capabilities – especially SACEUR[30] – to assess potential risks and threats to NATO's security interests. In addition, individual nations will conduct horizon scanning and will share their assessments through and within NATO structures. It should provide timely, accurate, relevant, predictive and wide-ranging contextualized intelligence, to help prevent strategic surprise and deliver informed decision-making to NATO political-military authorities. Some commanders may be given specific responsibilities for monitoring an area of interest.

2.18. Information received from all collection capabilities should be fused together by the intelligence staff to conduct a thorough JIPOE and be articulated via the joint intelligence estimate. JIPOE represents the contribution of the intelligence staff to all phases of the OPP. Specifically, intelligence efforts should achieve the following.

a. Enable early crisis identification within a designated area by continuously monitoring the international security environment. This should include analysis of regional instabilities, military capabilities and relevant global issues.[31]

b. Establish, maintain and, as appropriate, share an initial perception of emerging crises.

c. Provide an understanding of possible threats and risks to NATO security interests.

d. Maintain a matrix of potential crisis regions/countries (and related relevant actors) not addressed in the NIWS or Potential Crisis Warning List. This matrix should be based on factors derived from NATO policy and command guidance.

e. Take maximum advantage of non-NATO expertise, including assessments, analysis and networks of experts, as authorized.

f. Identify indications and warnings. These may be identified and reported by NATO operations and intelligence centres monitoring a specific area as well as by individual nations or operational partners.[32]

2.19. **Phase 2 – Strategic assessment.** The purpose of Phase 2 is to develop and coordinate a strategic assessment of an emerging or potential crisis. A strategic

[30] See Allied Command Operations (ACO) *Comprehensive Operations Planning Directive* (COPD), Chapter 2.

[31] This may encompass activities such as terrorism/extremism, proliferation of weapons of mass destruction and their means of delivery, malicious cyberspace activities and military technological developments.

[32] They are shared and assessed using the NIWS, which is designed to share information and assessments from nations, NATO Headquarters (NATO HQ) and ACO to provide early warning of any developing threat, risk or concern.

assessment may also be conducted for an ongoing NATO operation as part of work leading to development of a revised operation plan (OPLAN).

2.20. In terms of an emerging or potential crisis, the outcome of Phase 2 is the issuing of a strategic warning order to the selected operational-level headquarters (HQ) or other subordinate headquarters to alert them to be prepared to support strategic operations planning. The intelligence contribution to shared situational awareness should contribute to:

- a fundamental understanding of the nature of the crisis, including its key PMESII aspects;
- an appreciation of the implications for NATO, including potential strategic risks and threats; and
- an appreciation of potential strategic ends, ways and means.

2.21. **Phase 3 – Military response options.** The purpose of Phase 3 is to finalize the desired NATO end-state and further develop the strategic, political and military response strategy for the crisis at hand. At the strategic-military level, Phase 3 articulates options for consideration. Intelligence staffs will continue to conduct mission analysis and develop potential courses of action in conjunction with the other staff functions.

2.22. During Phase 3 intelligence staffs will pay particular attention to:

- the refinement of the intelligence contribution to the strategic estimate;
- establishing liaison and coordination for collaborative planning;
- preparing operational liaison and reconnaissance teams (OLRT), if required;
- confirming the CCIRs;
- developing the information exchange requirements;[33] and
- providing timely and tailored analytical support to the planning process.

2.23. **Phase 4 – Strategic plan development. Comprising of Phase 4a – Strategic concept of operations development and Phase 4b – Strategic Operation plan development and force generation.** The purpose of Phase 4a is to detail the concept for the conduct of a NATO-led operation, in concert with other non-military and non-NATO efforts, to achieve the NATO strategic objectives and establish conditions required to assist in the attainment of the desired NATO end-state.

[33] These links are characterized by high volume information flows, security and timeliness in support of command, control, intelligence and support of the forces.

2.24. The purpose of Phase 4b is first to identify and activate the forces and capabilities required to implement the strategic concept of operations (CONOPS) and accomplish the mission within acceptable risks. Second, it specifies the sequence of the strategic activities and operations, including the deployment, employment, sustainment and command of NATO-led forces, as well as the possible necessary interaction required with cooperating non-NATO entities. During Phases 4a and 4b, intelligence staffs will:

- continue to refine the intelligence contribution to the strategic estimate; and
- assist with the development of the operational CONOPS, and operational design plan for an intelligence force deployment.

2.25. **Phase 5 – Execution.** The purpose of Phase 5 is to facilitate, with strategic advice, direction and guidance, the commencement and conduct of a NATO operation in order to execute North Atlantic Council (NAC) decisions and directives. During Phase 5, intelligence staffs will:

- continue to refine the intelligence contribution to the strategic estimate and operations assessment;
- coordinate actions as necessary to initiate an operation and implement the strategic OPLAN; and
- assess the relevance of current plans and directives with stakeholders, and review the OPLAN as required.

2.26. Throughout the execution phase of an operation, intelligence staffs will contribute to periodic operations assessments aimed at measuring the effectiveness of their actions in creating the desired effects, establishing desired conditions and achieving objectives. Once objectives are considered to have been achieved, consideration will be given to the re-deployment of forces. Intelligence support will be required to provide over watch in these circumstances and may also need to maintain a high operational tempo, if the continued presence of forces under military command is required to support a non-military follow-on effort.

2.27. **Phase 6 – Transition.** The purpose of Phase 6 is to coordinate the transition and termination of a NATO operation. This involves the handover of responsibility to another authority (for example, the United Nations or local national authority) in the crisis area and the re-deployment of forces under NATO military command in a controlled manner. As already described, Phases 5 and 6 are likely to overlap, as the exact moment of transition will be difficult to define.

Section 4 – Operational-level planning

2.28. **Intelligence planning.** The operational-level planning process (OLPP), carried out by a designated joint headquarters, also comprises six phases to allow close collaboration between all levels of command during the different phases of the crisis management process. The intelligence and JISR supports all these phases, but is of particular importance during the execution phase. 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. At the operational level, the six OLPP planning phases are:

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

Operational-level intelligence planning

2.29. **OPP 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 commander's decision-making. The Joint HQ 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 represents the contribution of the intelligence staff to 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 operational environment covering all PMESII[34] domains, including associated potential threats and risks, in support of planning and the conduct of a campaign or operation. It develops an integrated understanding of the main characteristics of the operational environment including its maritime, land, air, space and cyberspace dimensions, as well as the PMESII system's main adversaries, friends and neutral actors that may influence joint operations. In particular, intelligence staffs will:

- gather, collate, organize and analyse existing information, intelligence and knowledge on the emerging crisis;

[34] Political, military, economic, social, infrastructural and information.

- assist with determining CCIRs;[35]
- develop priority intelligence requirements (PIRs);
- coordinate intelligence requirements with SHAPE J2;[36]
- 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.

2.30. **OPP 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 (MROs). Phase 2 at the operational level 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 based on the developed JIPOE to JOPG at the beginning of Phase 2.

2.31. **OPP Phase 3 – Development of response options.** The purpose of Phase 3 is to understand the situation, the operational environment and the mission in detail and to develop courses of action (COAs), from which one will be selected. Depending on the situation, agencies such as the NATO Intelligence Fusion Centre (NIFC)[37] may deploy an intelligence support team to the designated Joint HQ to provide direct intelligence support and facilitate intelligence reach-back. The intelligence staff will:

- provide the updated JIPOE briefing to the Commander and their staff;
- focus on actors;
- determine key factors;
- conduct centre of gravity (COG) analysis;
- support the development of the operational design;

[35] 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 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.
[36] It is important that intelligence staffs coordinate collection requirements to avoid duplication and to make the best use of resources.
[37] Further detail in respect to the NIFC is provided in Annex A.

- support the development of COAs; and
- shape the CCIRs and finalise PIRs.

2.32. **OPP Phase 4 – Planning.** Phase 4 is divided into two parts.

a. Phase 4a -Strategic concept of operations development.

b. Phase 4b -Operation plan development and force generation.

2.33. The purpose of operational CONOPS development is to detail the joint commander's concept for the conduct of the military campaign or 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 strategic CONOPS, a number of annexes are specifically mandated; the two most pertinent to intelligence are:

- Annex D – Intelligence;[38] and
- Annex II – Joint Fires.

2.34. 6. During this phase, the joint commander should put into place the mechanisms to collect, fuse, analyse, validate and share critical information and, where appropriate, share knowledge with other commands and non-NATO actors throughout the life of the operation.[39] Within this phase, the commander approves the finalised CCIRs. The intelligence staff will:

- assist the JOPG in CONOPS development;
- assist the JOPG in OPLAN development;
- support the Commander in deriving their PIRs;
- produce Annex D – Intelligence; and
- contribute to the Combined Joint Statement of Requirements (CJSOR), the Theatre Capability Statement of Requirements (TCSOR) and the Statement of Requirements (SOR).

2.35. **Operational 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-

[38] The format to be used can be found in STANAG 2014 Ed: 9, *Formats for Orders and Designation of Timings, Locations and Boundaries*.

[39] Details are provided in appropriate OPLAN annexes such as Annex D (Intelligence); Annex W (Civil-Military Cooperation); Annex CC (Command Information Management); and Annex NN (Knowledge Development).

making, and to fuse staff effort. The intelligence staffs will need to do 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. Lead the Joint Collection Management Board (JCMB).[40]

c. Contribute to the Joint Coordination Board (JCB) decision briefing. The JCB is the commander's principal meeting. Its aim is to synchronize 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.

d. Contribute to the operations assessment process within the Assessment Board and contribute to the Joint Force Commander operational assessment briefing. The Assessment Board is the second principal meeting for the commander. The aim is to seek the commander's endorsement of the provided assessment and recommend staff actions and plan adjustments. Decisions on follow-on actions should be taken by the commander during the JCB;

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

2.36. **Operational 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 the transition of NATO military responsibilities to proper authority and the re-deployment of 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 engagement space with a particular emphasis on the presence of NATO forces in-theatre.

Intelligence staff

[40] The JCMB is described in more detail in AJP-2.7(B), *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*.

2.37. **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 a J2 Current Operations (Ops) embedded in the Joint Operations Centre (JOC). J2 Current Ops, with the JOC, will play a critical function supporting current operations prosecuted by the J3 staff and the JOC through the provision of near real-time situational understanding and will be central to intelligence requirement management (IRM) and collection management (CM) and the JISR process.

2.38. J2 Plans 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, should provide intelligence support to joint tasks, such as both lethal and non-lethal targeting, and should provide deeper all-source intelligence analysis when required to provide improved understanding and intelligence in support of decision-making. J2 Plans should also be responsible for leading the development of the JIPOE, which will provide the commander and staff with both situational awareness and deeper thematic analysis, drawn from judgments based upon a greater depth and breadth of analysis to provide the foresight and insight required to develop the plan and operation.

2.39. The intelligence staff may also include specialists to provide a detailed understanding of specific areas or themes. For example:

- representatives from national intelligence, defence or police agencies;
- intelligence representatives from the host nation;
- intelligence representatives from component commands;
- civil-military cooperation analysts;
- human environment analysts and cultural advisors;
- operational analysts; and
- representatives from other governmental and non-governmental agencies, including international and regional organizations, the media, academia or industry.

The intelligence staff is therefore central to the development of the commander's common situational awareness and understanding of the operating environment at the operational level by providing them with both foresight and insight.

Section 5 – Joint intelligence areas

2.40. To enable the commander and their intelligence staff to focus their intelligence effort, the joint operations area is divided into three areas.

a. **Area of operations.** Area of operations (AOO) id defined as: *an area defined by the joint force commander within a joint operations area for the conduct of specific military activities*.[41]

b. **Area of intelligence responsibility.** Area of intelligence responsibility (AOIR) is defined as: *an area allocated to a commander, in which he is responsible for the provision of intelligence, within the means at his disposal*.[42]

c. **Area of intelligence interest.** Area of intelligence interest (AII) is defined as: *a geographical area for which a commander requires intelligence on the factors and developments that may affect the outcome of operations*.[43]

Section 6 – Joint intelligence preparation of the operational environment

2.41. The JIPOE[44] is the responsibility of the intelligence staff and contains the analytical process used by joint intelligence organizations to produce intelligence assessments, estimates and other intelligence in support of the OLPP[45] and the commander's decision-making process. It is a continuous process, which assists commanders and their staffs in achieving information superiority by identifying adversary COGs, focusing intelligence collection at the right place at the right time, and analysing the impact of the operational environment on military operations. The JIPOE will use information, assumptions and logical deductions from the joint intelligence estimate (JIE), but focuses on intelligence efforts and delineates the prioritization of intelligence requirements and assesses potential adversary COAs.

2.42. As intelligence is produced, the JIE increases in detail, refining its input into the OPP and the JIPOE. The JIPOE is a living product and, in addition to contributing to the early stages of the operational estimate and JIE, it assists in the implementation of the plan. The JIPOE is constructed from the outset in a manner that allows timely and accurate updating.

---

[41] NATO Agreed, Allied Administrative Publication (AAP)-06(2014).

[42] NATO Agreed, AAP-06 (2014).

[43] NATO Agreed, NATOTerm.

[44] The JIPOE is a coordinated analytical process to develop an integrated understanding of the main characteristics of the operations environment, including its land, air/space, and maritime dimensions, as well as the PMESII system of adversaries, friends and neutral actors that may influence joint operations.

[45] JIPOE and the Joint Intelligence Estimate support the comprehensive preparation of the operational environment (CPOE).

JIPOE analysis

2.43. JIPOE uses an agreed methodology to describe in broad terms the operational environment, physically, culturally and electronically, and to identify specific threats and other potential barriers to mission success. The JIPOE will have a very specific focus towards an assessment of the adversary's COA. Such an agreed methodology is essential to establish shared situational awareness and understanding by the commander, within the staff and among contributing nations.[46] Ultimately, it should provide an analysis and understanding of the situation and, as far as is possible, a single intelligence narrative.

2.44. The JIPOE process is continuous and considers many factors. It should be based around the PMESII model. Additional factors can be added to PMESII if required by the specific operations (for example, health or environment matters). PMESII describes the foundation and features of an adversary and can help determine their strengths and weaknesses, as well as help estimate the effects various actions will have on actors. When conducting JIPOE the following steps and structure should be adopted as a baseline.[47]

a. **Area evaluation.** Identify the environmental factors throughout the operational environment relevant to the joint operations area. These factors include, but are not limited to:

- terrain;
- infrastructure;
- information environment;
- protected areas;
- climate and weather;
- environmental and health factors;
- borders and boundaries; and
- religion and cultural considerations.

b. **Actor evaluation.** Identify an actor's potential courses of action independent of terrain and weather constraints, for example, how the actor may operate according to doctrine or previous experience.

c. **Threat integration.** Area evaluation is combined with actor evaluation. This provides an assessment of an adversary's, neutral's, or friendly forces'

[46] Shared situational awareness also feeds the common operational picture (COP). This is a snapshot in time of friendly, neutral and adversary forces and of the battlespace.
[47] AJP-2(A), Section V.

capabilities and likely courses of action or intentions, based on all the available intelligence. It also provides a means for the operational level HQ to understand the second and third order effects of NATO forces action, and opportunities to identify intelligence planning requirements and intelligence-sharing requirements.

2.45. The results of the JIPOE process may be represented graphically or in a written format. The specific format of the intelligence estimate will depend on the operational situation and the commander's requirements.

Framework for intelligence management

2.46. The intelligence framework is a wider consideration that should be addressed in order that the intelligence architecture is established properly and is able to function as required. The following paragraphs are not exhaustive, but are intended to inspire and guide those responsible for planning intelligence operations.

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

b. **Comprehensive understanding of the 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 paramount.

c. **Mutual respect, trust and transparency.** Intelligence planning is underpinned by a culture of mutual respect and trust. Trust is built through information sharing and associated security measures to protect others' intelligence, and balance the risk against insider threats. Practical cooperation should be encouraged to allow 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.

d. **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.

e. **Efficient use of resources.** The delivery of intelligence needs to balance continuous tensions between opposing requirements, and the optimizing 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.

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

g. **Time *versus* depth.** A balance should be struck 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 products should be provided rapidly enough to get inside the adversary's decision cycle. This requires a free flow of intelligence and information across a multi-level, single intelligence architecture and for the various agencies to process and fuse shared material.

h. **Quality *versus* quantity.** The requirement to ensure commanders receive valuable and relevant intelligence in context, rather than be deluged with large amounts of raw material, is vital. Often, the balance of effort can favour collecting a volume of information, rather than applying what is held to a specific context. Intelligence staffs should offer commanders solutions that sort out the detail from the torrent of information. As described above, intelligence effort should be rooted in the context of the commander's intent and include robust information management.

i. **Output *versus* ownership.** This is the tension created when the needs of single Service or national capability provider, impacts on joint force or NATO requirements. In some situations, tasking of an asset can be driven by who owns an asset rather than it being focused on the wider need to contribute to a combined output. However, intelligence staffs should focus on delivering high-quality intelligence. Associated processes should enable, not delay, the transmission of information, and integrate scarce intelligence and JISR assets across the coalition.

j. **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, but 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.

k. **Writing for release.** Writing for release at the lowest classification 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 requesting intelligence staff 'pull' and pro-active 'push' of products by agencies and collection assets.

l. **Security classification determined by the originator.** The nation or NATO originator that provides intelligence products or collected information to the rest of the Alliance, another group of countries 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.

m. **Collect *versus* connect.** This is the need to balance the development of an appropriate collection capability, with the ability to process and disseminate the subsequent product. Frequently, collection capabilities are better funded than connection programmes, yet dissemination can prove to be the weakest link of the intelligence cycle. Collection is not an end in itself but a means to gather information for analysis.

n. **Criticality of dissemination.** There is little benefit in collection that does not result in a disseminated intelligence product or support to intelligence requirements. Both raw data and finished products should be shared as early as possible after collection. Push or pull methods should be used based on the customer requirements and the potential for future analysis, and supported with appropriate bandwidth. Information formats should also be in accordance with appropriate Standardization Agreements (STANAGs) or generally accepted open standards. In some cases, especially with regard to available bandwidth, limitations exist which may have to be carefully considered during the intelligence planning process.

o. **Common standards for metadata.** Metadata tagging must be used to allow 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, analysis organizations and customers.

p. **Stability *versus* change.** All procedures operate most effectively when associated with a known and 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.

q. **Resources *versus* demand.** It is unlikely that intelligence staffs will ever have enough personnel or resources to satisfy every request. The intelligence lead must plan early and attempt to build as robust an organization as possible within the prevailing constraints. Early expectation management will be required to establish what is achievable.

r. **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.

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

t. **Burden sharing.** This should help to identify capability gaps and interoperability requirements. NATO nations, commands and agencies should agree to contribute complementary applications and databases and analysis capabilities in a federated way in order 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.[48] Additionally, the architecture should, within specific mission parameters, support reach-back to those organizations that are not part of NATO.

u. **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.

[48] Including civilian agencies and organizations.

CHAPTER 3 – INTELLIGENCE PROCEDURES

Section 1 – Intelligence cycle

3.1. The intelligence cycle is the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available for users.[49] These activities are focused through the four intelligence core stages of direction, collection, processing and dissemination. This sequence is shown in Figure 3.1.

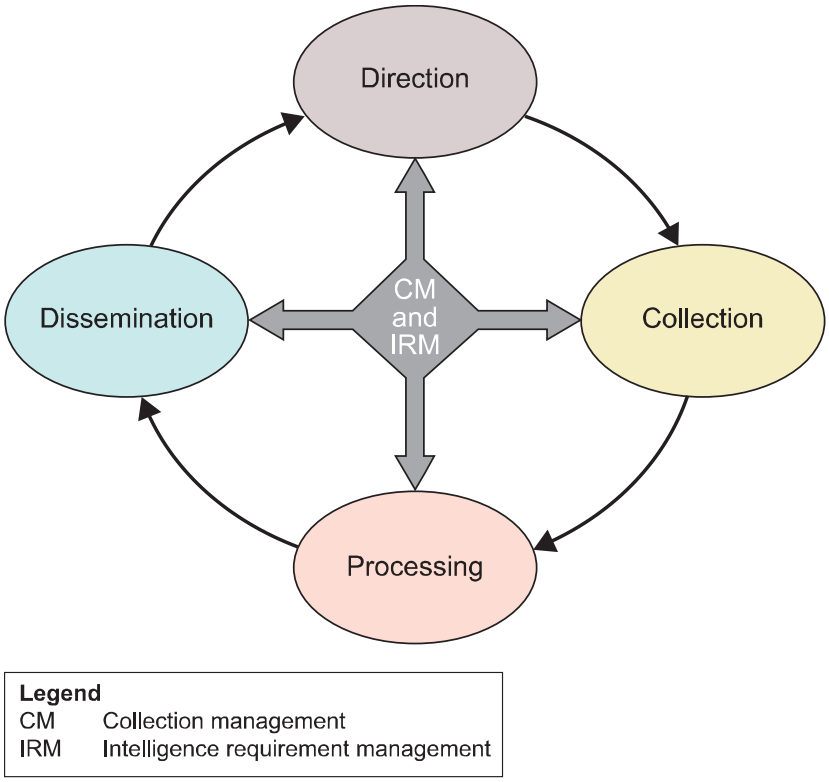

Figure 3.1 – The intelligence cycle

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 material can, if the requirement is urgent, be disseminated without being processed with the appropriate caveats.

[49] Allied Administrative Publication (AAP)-06, *NATO Glossary of Terms and Definitions* (2014).

3.3. Appropriate resourcing is particularly important, as the vast majority of NATO intelligence capability is dependent on coordination and collaboration with different member nations or partners.[50] Given that there will always be negotiation and concession in executing intelligence procedures, consideration must be given early in the planning process with regards to availability of resources to answer intelligence requirements. Ultimately, procedures should focus on optimizing the delivery of intelligence, in the context of the six foundation principles:[51]

- accessibility;
- sharing;
- responsiveness;
- flexibility;
- interoperability; and
- comprehensive.

Section 2 – Intelligence requirements

Priority intelligence requirements

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

3.5. PIRs encompass those intelligence requirements for which a commander has an anticipated and stated priority in their tasking of planning and decision-making and normally encompass identification and monitoring of areas that represent opportunities and threats to the mission plan. They should be limited in number and should provide comprehensive and coherent groupings of key issues. They may be enduring or limited to a particular phase or situation. PIRs should be written in such a way as to support a decision the commander should make, and represent an audit trail to the original question in order that all intelligence activity is focused on the commander's intent and gaps are readily identified.

[50] For example the NATO Intelligence Fusion Centre or National Intelligence Centres.

[51] Allied Joint Publication (AJP)-2(A), *Allied Joint Doctrine for Intelligence, Counter-intelligence and Security*, page 3-3.

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

Specific intelligence requirements

3.7. Specific intelligence requirements (SIRs)[52] is defined as: *specific intelligence requirements support and complement each PIR and provide a more detailed description of the requirement.*[53] SIRs are used by the intelligence staff to determine what intelligence asset, collection capability or discipline can best satisfy the requirement, and to identify the coordination required. SIRs are managed in the same manner as a PIR.

Essential elements of information

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

Section 3 – Intelligence requirements management and collection management

3.9. Before describing the four stages of the intelligence cycle, it is important to emphasize the central roles of intelligence requirements management (IRM) and collection management (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 and CM.[54] If not properly resourced; IRM and CM functions can quickly become overloaded.

3.10. IRM underpins the vast majority of the intelligence cycle, ensuring that requirements are prioritized, coordinated and actioned correctly. CM is about taking these validated requirements and assigning them to collection activities, whether joint intelligence, surveillance and reconnaissance (JISR) asset related or not, and it must be closely linked with operations staffs at all times. There will be some repetition in subsequent

[52] AJP-2.

[53] This term is a new term and definition and will be processed for NATO Agreed status.

[54] Within some staffs and nations IRM and CM are described as collection coordination and intelligence requirements management (CCIRM). Allied Command Operations (ACO) Directive (AD) Number 065-005.

paragraphs; this is intentional to emphasize how IRM and CM are an integral part of the intelligence cycle.

3.11. Collectively, the aim of the IRM and CM function is to:

- manage and maintain standardized procedures for developing, validating, prioritizing, and processing intelligence requirements and RFIs;
- manage collection requirements, ensuring the most effective use of collection assets and capabilities;
- facilitate an enhanced cycle for collecting, processing and disseminating time-sensitive intelligence products for the most urgent requirements;
- develop and manage standardized procedures to disseminate intelligence;
- provide specialist intelligence knowledge to analysts and customers, in order to assist with the drafting of valid intelligence requirements;
- measure customer satisfaction, adjust procedures as required and contribute to the lessons learned process;
- prioritize, as requirements will not always match the resources available to address them;
- optimize the collection planning by coordinating and integrating all JISR tasking with operational planning; and
- ensure the widest dissemination and availability of intelligence to customers by the need-to-know principle.

3.12. IRM and CM are complex management functions inside a staff with significant data management and interoperability challenges, involving a number of discrete activities, but based around a generally similar set of criteria. They both require seamless linkages between the various requesting, managing, tasking, production and distribution activities. Employing standardized doctrine, processes and interoperable systems to allow the automated sharing of requirements, plans, tasking requests and products best optimizes IRM and CM. Nations are responsible for complying with these standardization agreements (STANAGs) once they have been ratified.[55]

Satisfaction of requirements

3.13. Once a requirement has been identified, validated, refined, and prioritized, the intelligence staff should determine how to satisfy the requirement. In some cases the

[55] A list of relevant standardization agreements (STANAGs) is at Annex A, but as JISR processes develop, these and others will need to be developed or amended.

requirement can be satisfied by information or intelligence already held by that headquarters or by data or intelligence held by NATO; alternatively, the requirement may require the intelligence requirement being matched to available dedicated 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 utilization. The intelligence staffs should identify the information needed, where and how to get it, how to package the intelligence into an appropriate product, and how to deliver that product. 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 information to a particular user.

Section 4 – Direction

3.14. In any operation or planning situation, the commander should enable direction. Direction is defined as: *determination of intelligence requirements, planning the collection effort, the issuance of orders and requests to collection agencies and maintenance of a continuous check on the productivity of such agencies*.[56] Commanders should determine their critical information requirements in order to plan and conduct their mission.

3.15. The PIRs are a vital part of CCIRs and are normally formulated by the intelligence staffs in close cooperation with the commander.[57] The direction should be specific and, wherever feasible, should highlight those factors that are critical to the planning process. These requirements can generally be divided into two groups.

a. Intelligence requirements that contribute to the success of the mission.

---

[56] This forms part of the definition for intelligence cycle, which is defined as*: 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.* AAP-06 (2014).

[57] AJP-2(A), Chapter 5.

b. Intelligence requirements that identify and quantify the threat to the mission.

3.16. 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;[58]
- issue clear direction and guidance, defining areas and themes of interest;
- engage with drafting, approval and circulation of their PIRs; and
- develop trust with intelligence staff, encouraging their integration into planning and operations, creative thinking and predictive analysis.

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

3.18. The IRM staff function that 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.

3.19. Overall, as requirements are generated, the IRM function will:

- help to validate, prioritize and refine intelligence requirements;
- determine how they can best be satisfied in coordination with the CM;
- coordinate all activities within the intelligence cycle, associated with meeting the requirement in coordination with the CM;
- coordinate collection tasking with the CM;
- monitor activity to ensure that the right information is being collected, analysed and disseminated; and

[58] This applies to units and organizations as well as assets.

- ensure that intelligence activities are conducted in a timely manner and where delays are occurring the re-tasking or reprioritizing as required in coordination with the CM.

Request for information

3.20. The term RFI[59] is used to describe an intelligence requirement that has been passed to the IRM staffs at higher, lower or adjacent levels. A RFI is used when a commander does not have sufficient allocated collection capabilities, or the intelligence staffs are unable to answer a question through retrieval from existing data and intelligence, research or other means. They are generated when the information or intelligence that relates to the PIR/SIRs/EEIs cannot be obtained internally.

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 inform the ICP. Indicators are defined as: *in intelligence usage, an item of information which reflects the intention or capability of a potential adversary to adopt or reject a course of action*.[60]

Collection management

3.22. CM is the management function inside an intelligence staff and describes the activity of matching the validated and structured intelligence requirements and RFIs to the available collection assets. Accordingly, the CM function is positioned between the intelligence and operations staffs in order to broker requirements against tasking.

3.23. CM 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 CM areas are responsible for prioritization and coordination 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 result is an ICP.

Intelligence collection plan

[59] RFIs have to be prioritized in accordance with the intelligence requirements within the IRM.

[60] The AAP-06 (2014) definition for 'indicator' has been adjusted to reflect that AJP-5 primarily addresses the 'adversary' and not the 'enemy'.

3.24. The ICP 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 collection task list (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 or exercise. EEIs help form the basis of the ICP, which together with emerging collection requirements (for example, RFIs) 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 implementation and control of the ICP alongside the CTL that will include any additional RFIs and intelligence, surveillance and reconnaissance request. 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[61] collection requirements (CRs) are collated into a collection requirement list (CRL), which is then prioritized by the Joint Collection Management Board (JCMB) into the CTL for collection by either higher or adjacent headquarters.

PIR	SIR	EEI	Activity	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								✓	✓	✓	✓							
#3								✓							✓	✓		

Figure 3.2 – Example of a basic intelligence collection plan

3.26. Intelligence staffs involved in IRM and CM do not have the executive authority to issue orders in the operational area. Tasking is undertaken as a collaborative effort between the intelligence and operations staff. This relationship is vitally important if procedures need to be hastened in the event of time-sensitive, unexpected or urgent requirements. Together with inputs from IRM staff, liaison officers and subject matter

[61] This can be either because the appropriate collection capability is not 'owned' by that headquarters or is being used to satisfy another intelligence requirement.

experts, those involved in CM will build the ICP using the appropriate software tools in order that it can be shared and updated. The IRM and CM procedure is not conducted during ad hoc and dynamic JISR tasking.

3.27. Requests are submitted from the joint, component and tactical levels.[62] For that reason, coordination with components is critical during operations planning, and the agreed procedures for tasking, reporting and disseminating collected information and intelligence should be clearly stated in the operation plan (OPLAN), subordinate plans, subsequent plans and any support plan. Additionally, once the mission has commenced, the components should be given responsibility for determining whether they can satisfy their own and the joint commander's IRs.

Section 5 – Collection

3.28. Collection is the second phase of the intelligence cycle. It is defined as: *a phase of the intelligence cycle as: the exploitation of collection capabilities by agencies and the delivery of the data and information obtained to the appropriate processing unit for use in the production of intelligence*.[63] Intelligence agencies and collection capabilities conduct the bulk of all collection activities, but non-dedicated collection capabilities can also contribute.[64] 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.

3.29. In order to meet IRs the appropriate collection capability needs to be tasked through a coordinated and integrated procedure, which ensures accurate and timely cooperation with all interested parties. Such a capable 'system of systems', or 'enterprise', allows 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.

3.30. It is important that intelligence staff ensure the commander and staff understand the capabilities, limitations, vulnerabilities and response times of collection capabilities

[62] It should be emphasized that the processes best suited for tasking airborne imagery collection missions are not usually the best for obtaining collection from land and maritime forces.

[63] See footnote 56. AAP-06 (2014).

[64] 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 soldier a sensor’ captures this.

and agencies likely to be available to them, along with their susceptibility to deception.[65]

3.31. 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, 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

3.32. 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 defined as a phase of the intelligence cycle as: *the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation*.[66] Processing is iterative and may generate further requirements for collection before dissemination of the intelligence.

Collation

[65] 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 soldier a sensor' captures this.
[66] See footnote 56, AAP-6 (2014).

3.33. 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.

3.34. Although collation is increasingly likely to be automated, involving databases linked to graphical interfaces and automatic data transmission between headquarters, there will always be a personal element of sifting and comparison of collection results. This will provide a subjective view of responses to IRs and gauge how valuable they are in answering a commanders' 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, at the operational level, directly related to the PIRs. 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.[67]

c. **Construction.** Although electronic storage systems can manage a huge amount of data, the collation system should be intuitive and as simple as possible. The use of relational data will simplify the exploitation of data 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

3.35. Evaluation is the second step in the processing phase and consists of the appraisal of an item of information in respect to the reliability of the collection capability and the

[67] Unique codes can be allocated to people, places, vehicles, etc.

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.[68]

3.36. The evaluation rating is based partly on the subjective judgment of the evaluator, and, in the case of information produced by a sensor, on knowledge of the accuracy of the particular sensor system.[69] 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 at Table 3.1.

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

Table 3.1 – Reliability and credibility

Analysis

3.37. Analysis is defined as: *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*.[70] 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

[68] This is not always necessary, but when it is not formally employed, analysts should still mentally apply this process of evaluation.
[69] 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.
[70] AAP-06 (2014).

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.

3.38. Analysis is never exhaustive, nor absolutely certain, as the dynamics of most crises are too complex and unpredictable. However, effective analysis can help a commander to rationalize, though not necessarily reduce, complexity and ambiguity to some degree.

3.39. Analysis does more than look at the current situation, it should be predictive and therefore should address what might happen next, based upon alternative assumptions regarding the actions and reactions of different actors (including the impact of any intervention). Predictive analysis enables a commander to understand the context in which they are operating or intend to operate.

Integration

3.40. Integration is defined as: *in intelligence usage, a step in the processing phase of the intelligence cycle whereby analyzed information and/or intelligence is selected and configured into a pattern in the course of the production of further intelligence*.[71] 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 end-user information and intelligence requirements that it should satisfy, a unit will often require external products to fuse with material generated internally.

3.41. 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.

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 too many 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 of analysts to tackle specific analytical challenges, but from an alternate perspective; usually that of the adversary. Red teaming can help avoid cultural bias in analysis and can be

[71] AAP-06 (2014).

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

3.42. Interpretation is defined as: *in intelligence usage, the final step in the processing phase of the intelligence cycle and is where the significance of information or intelligence is judged in relation to the current body of knowledge*.[72] Interpretation is an objective comparison based on common sense, life experience, military knowledge and understanding, covering both the adversary and friendly forces.

3.43. 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 looked at.

a. **Identification.** This considers all the implications of the presence 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 or entity being reported on.

b. **Activity.** The significance of the activity being carried out should always be compared with information about previous activity, in order 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 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 at Tables 3.2 and 3.3.

e. **Deception.** Deception consists of those measures designed to mislead by manipulation, distortion or falsification of evidence to induce an adversary to react in a manner prejudicial to their interests. The intelligence community is a

[72] AAP-06 (2014).

primary target for hostile deception and analysts should always be cautious of the information in front of them.

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 3.2 – Confidence levels

Probability statements for assessments (numerical and verbal)	
More than 90%	Highly likely
60% - 90%	Likely
40% - 60%	Even chance
10% - 40%	Unlikely
Less than 10%	Highly unlikely

Table 3.3 – Probability levels

3.44. **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 are the gaps in knowledge; and
- what is analytical assessment.

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 engaged in the intelligence cycle to maintain discipline in their 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.

Section 7 – Dissemination

3.46. The final phase of the intelligence cycle is dissemination. It is defined as the final phase of the intelligence cycle as: *the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it*.[73] 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 and CM should determine the means of dissemination, storage and retrieval of product. That can be a single system or currently relying on a myriad of ways and means that have to be coordinated with the wide variety of entities within the IRM and CM processes.

3.47. This should be in a timely manner without overloading the user and minimizing the load on available bandwidth. Dissemination consists of both 'push' and 'pull' control principles. The 'push' concept allows the higher formations to push information to satisfy intelligence requirements at lower levels of command. The 'pull' concept involves direct electronic access to databases, intelligence files or other repositories by intelligence organizations at all levels of command. Web-based technologies and standards are now commonly used to organize and present intelligence products.

3.48. 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

[73] AAP-06 (2014).

be complemented by appropriate human communication skill sets, including linguistic ability.

3.49. 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.

Principles

3.50. All 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 is necessary.

Intelligence formats

3.51. Intelligence can be disseminated in five formats. The format selected should be appropriate to the requirement and the recipient, and use standardized templates where appropriate.

a. **Verbal.** This method is quick and can be delivered to a wide audience. 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 (INTREP) and intelligence summaries (INTSUM), 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 make 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 staffs.

d. **Data.** Data is information resulting from measurement, observation or facts (for example, geospatial references), which may not be subject to further analysis. The use of raw data will invariably be when the material is time critical.

Section 8 – Monitoring and evaluation

3.52. 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 occur 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 measurements of performance (MOP) and measures of effectiveness (MOE). These measures are informed by a variety of indicators related to the conduct of intelligence tasks or their impact. This promotes the understanding required to support decision-making.

Section 9 – Assessment

3.53. 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 plan. 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 staff design and agree operational measurements and assessments at the JOPG, and the AWG provides the material for the Assessment Board briefing to the commander.

3.54. 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.[74] It is essential to recognize that operations assessments are not isolated, but considered across all levels of warfare, in order to understand the strategic to tactical perspective. The operations assessment process involves four major steps:[75]

- designing the operations assessment and support to planning;
- developing the data collection plan;

[74] This is described in detail in Allied Command Operations *Comprehensive Operations Planning Directive* (Interim) v 2.0, (October 2013), Chapter 5.

[75] These are described in detail in the *NATO Operations Assessment Handbook*.

- data collection and treatment; and
- analysis, interpretation and recommendations.

3.55. Intelligence staff must be involved throughout the operations assessment process, providing an effective review, analysis, and feedback service.[76] It can involve both subjective and objective assessments to inform decision-making, through measuring different criteria.

3.56. At the operational level, the process is based on the overall analysis of metrics measuring progress of planned actions (MOP)[77] and the achievement of planned objectives (MOE).[78] In general, intelligence staffs will need to support two aspects.

3.57. The first is broad in nature and seeks to answer the question: 'Are we accomplishing the operational 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 PMESII areas.

3.58. 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 situations that may arise.

Section 10 – Lessons learned

3.59. Establishing a lessons learned process at the start of a new operation is essential to enable continuous improvement across both NATO as an alliance and individual nations. Commanders should include intelligence representation when collating lessons for subsequent analysis and critical review; as such lessons are relevant to many stages of planning and execution.

3.60. The strategic planning directive will provide guidance for capturing lessons and best practices, to promote operational effectiveness and strategic success. Ultimately, the purpose of a lessons learned procedure is to learn from experience and to provide validated justification for amending existing methods, in order to improve

[76] Example measurement and assessment criteria may include: adversary capabilities and movements; mood and disposition of the population; rule of law; and economic indicators, etc. Collaboration or close cooperation with non-military actors to gain a better understanding of the engagement space should be considered.

[77] This is the assessment of the realization of specified effects and involves metrics that measure a current system state. It examines whether or not the operation or campaign is achieving its purpose. It can also test the logic of a plan to see if it is plausible and complete.

[78] This evaluates task performance and uses metrics to determine the accomplishment of actions or tasks (for example, how the maritime force performed against its given mission within the OPLAN Annex F). The focus for the intelligence staff will be the impact of joint operations on an adversary and normally consists of an informed assessment.

performance. As all other disciplines, intelligence can derive great benefit from this process.

3.61. Lessons learned from previous operations are available through the use of the NATO Lessons Learned Portal (NLLP) and NATO Lessons Learned Database (NLLDB), which are managed by the Joint Analysis and Lessons Learned Centre (JALLC), Lisbon. The Supreme Headquarters Allied Powers Europe (SHAPE) historical office and JALLC can also be consulted and asked to assist with historical analysis.

Section 11 – Joint intelligence, surveillance and reconnaissance

3.62. Joint intelligence, surveillance and reconnaissance (JISR) is defined as: *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 of the resulting information in direct support of the planning, preparation and execution of operations*.[79] JISR synchronizes intelligence operations, 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 information and intelligence requirements. The IRM and CM process is critical to the effectiveness of the JISR process as it provides the 'gearing' to enable synchronization with the intelligence cycle. Allied Joint Publication (AJP)-2.7(B), J*oint Intelligence, Surveillance and Reconnaissance (JISR)* provides more detail.

JISR approach

3.63. JISR is a multidisciplinary approach comprised of four distinct elements:

- joint;
- intelligence;
- surveillance; and
- reconnaissance.

3.64. The 'J' in the term 'JISR' covers the 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 capabilities.

[79] Allied Joint Publication (AJP)-2(A). This term and definitions modifies an existing NATO Agreed term and/or definition and will be processed for NATO Agreed status.

3.65. The 'I' 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. These disciplines include:

- **acoustic intelligence** (ACINT) results include the collection and exploitation of acoustic signals or emissions;
- **human intelligence** (HUMINT) results are based on information, which is collected and provided by human sources;
- **imagery intelligence** (IMINT) results are based on the collection, processing and exploitation of image sequences;
- **measurement and signature intelligence** (MASINT) results are based on the collection of scientific and technical information in order to obtain distinctive and differentiating features;
- **open source intelligence** (OSINT) results are based on openly available or restricted access information; and
- **signals intelligence** (SIGINT) delivers results by collecting and exploiting electromagnetic signals or emanations - the main subcategories of SIGINT are communications intelligence and electronic intelligence.

3.66. Surveillance is defined as: *the systematic observation of aerospace, surface or subsurface areas, places, persons or things, by visual, aural, electronic, photographic or other means*.[80] 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 operational environment. Over extended periods of time, surveillance enables pattern of life analysis, which can lead to an in-depth understanding of threats, activities or behaviour.[81]

3.67. Reconnaissance is defined as: *a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area*.[82] It is a focused method of collecting information about specific locations, facilities or people. Reconnaissance tasks are not confined by specific reconnaissance units, but may be undertaken by other force elements in the course of their duties. Reconnaissance enables the collection of specific information within the joint operations area, against

[80] AAP-06 (2014).
[81] See AJP 2.7.
[82] AAP-06 (2014).

known and potential adversaries and non-aligned actors in support of current and future operations. It must be focused in time and space to answer specific requirements. It collects results through visual observation or other detection methods, to provide specific information to the requester.[83]

JISR key principles

3.68. The harmonization of intelligence and operations functions is essential to maximize the efficiency and effectiveness of the employment of JISR capabilities. JISR operates in accordance with six key principles that are appropriate at all levels across the full range of NATO operations to ensure effectiveness, these are:

- centralized direction, decentralized execution;
- responsive – timely and flexible to satisfy the needs of the requester;
- shared – planning and results should be available and accessible to those who require it on a responsibility-to-share basis;
- sustainable – capabilities need to be sustainable to meet mission requirements;
- reliable – to give commanders and their staffs confidence in JISR results; and
- accurate – results must answer the information requirements in the most accurate way possible.

JISR process

3.69. The JISR process is a framework through which a single collection requirement is satisfied by a JISR asset and consists of five sequential steps: task, collect, process, exploit and disseminate (TCPED). 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 both multi-source and all-source intelligence.

3.70. In order 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

[83] See AJP-2.7.

of the operations staff. A simplified diagram showing the relationship of the JISR process to the intelligence and operations cycles is shown below in Figure 3.3.

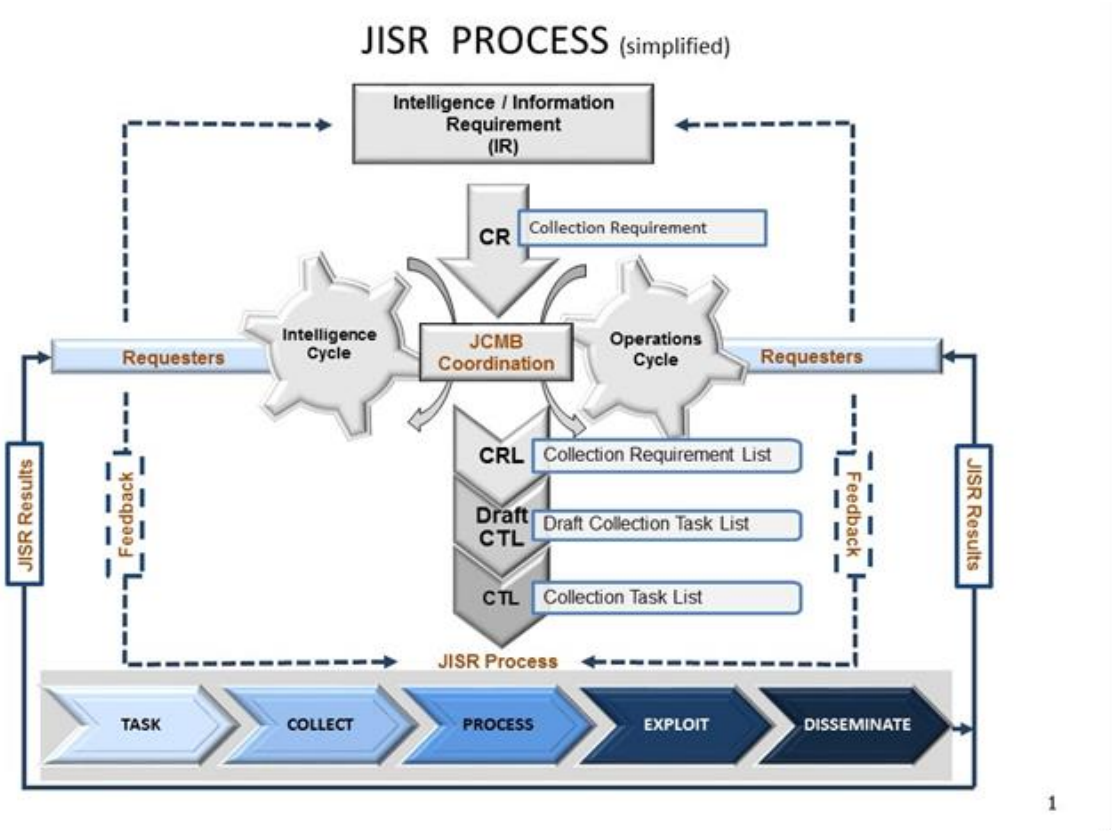

Figure 3.3 – Relationship of the JISR process to the intelligence and operations cycles

JISR planning

3.71. JISR planning is an integral part of the operations planning process (OPP) and must be included at the onset of all planning activities. 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.

JISR architecture

3.72. 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. An essential and integral part of the JISR architecture is the intelligence system support architecture (ISSA)[84] consisting of intelligence related networks, applications, databases and metadata, including their structure, processes and the required connectivity. The components of JISR are invariably combined in a single theme, but each is distinct and fulfils a specific purpose.[85] Consequently, the intelligence cycle and the JISR process must be seamlessly synchronized.

JISR tasking

3.73. Relative to the available planning times, tasking of JISR assets can either be deliberate, *ad hoc* or dynamic. A tasking timeline is depicted in Figure 3.4.

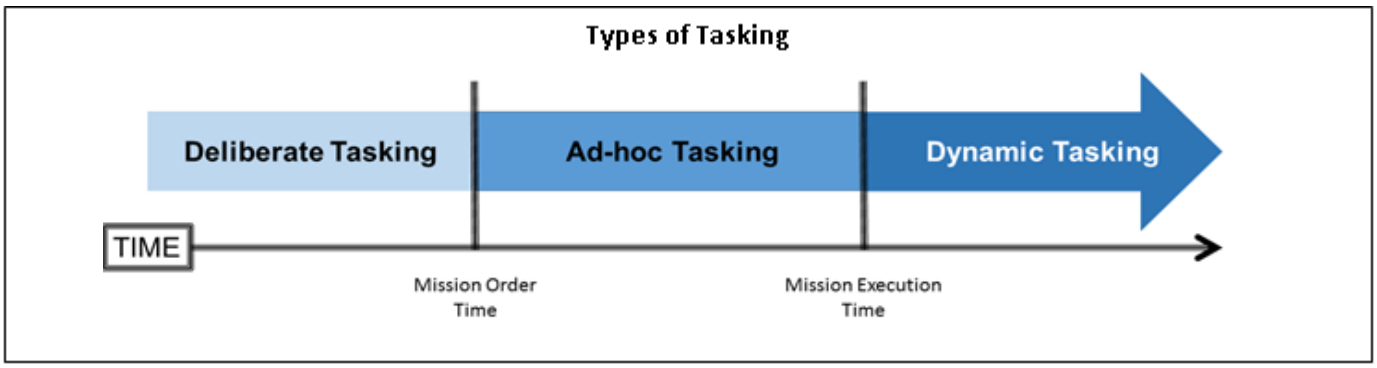

Figure 3.4 – Types of JISR tasking

Intentionally blank

[84] MC 0582/1 (2013), Section 1.

[85] The concept for JISR is expressed in detail in MC 0582/1. This chapter should also be read in relation to AJP 2.7(B), *Joint Intelligence, Surveillance and Reconnaissance (JISR)* and Allied Intelligence Publication (AIntP)-14, *JISR TTPs*.

CHAPTER 4 – INTELLIGENCE SUPPORT TO JOINT TASKS

Section 1 – Introduction

4.1. Intelligence supports joint tasks such as locating, identifying and analysing actors, systems and potential targets in order to identify their value and vulnerability to an appropriate means of influence, be that lethal targeting or their willingness to be positively influenced to provide support or at a minimum to secure their acquiescence. Intelligence can then be used to allocate relative importance to actors, systems and potential targets, be they for lethal or non-lethal action in support of operational decisions. Intelligence ensures that the commander selects appropriate and beneficial actors systems and potential targets contributing to the achievement of operational objectives. Intelligence activity must ensure the timely passage of indicators and warnings to promote early full spectrum target development.

4.2. Having identified actors, systems and potential targets to be a focus for a variety of potential influence effects, intelligence must support the creation of the desired effect. The process of human network analysis to support targeting (HNAT) is used by the intelligence staff where targets are individuals or members of threat networks. HNAT is an intelligence function that is a component of NATO's approach to attack the networks[86] (AtN) operations. HNAT consists of human network analysis, support to operations, targeting and effects that attack, neutralize or influence human networks. HNAT provides understanding of the dynamic organization of threat networks and recommends individuals, locations or activities within these networks to be subject to influence and action.

4.3. Intelligence staffs also support targeting by leading on target analysis (TA)[87] which provides, within context, a detailed picture of actors' capabilities, structures, organization, intentions, objectives and vulnerabilities in context. TA is the holistic and dynamic intelligence assessment of all aspects of potential target sets, physical and psychological, to identify vulnerabilities which, if targeted by the appropriate action (lethal or non-lethal) would create the desired effects. This intelligence is then used to allocate relative importance to targets and actors in support of operational decisions and the target prioritization process. Within the mission planning and execution phase, intelligence supports the engagement of targets with intelligence throughout the tactical engagement process, across the full spectrum of lethal and non-lethal options.

---

[86] Attack the networks is defined as: *in countering improvised explosive devices, to isolate the component parts of networks through the coordinated and selective use of cognitive and physical activities to defeat an improvised explosive device system*. NATO Agreed – NATOTerm.

[87] Target analysis includes target system analysis (TSA) and target audience analysis (TAA).

4.4. The tactical engagement process determines whether a target that can be engaged by lethal action in terms of both required military effect and is lawful under the rules of engagement. Once potential targets are identified and validated, they are then nominated and prioritized. It is essential that the Joint Prioritized Target List (JPTL), provided via the Joint Targeting Coordination Board (JTCB), enable a coherent JISR plan to be developed. Meanwhile, the commander's Joint Coordination Board (JCB) assigns execution responsibilities, prioritizes, de-conflicts and synchronizes all aspects of component activities. It ensures that both lethal and non-lethal targeting efforts are coordinated and focused on the commander's objectives. The JCB allocates available joint intelligence, surveillance and reconnaissance (JISR) assets, as recommended by the Joint Collection Management Board (JCMB) to the appropriate component commander for tasking.

Section 2 – Joint targeting cycle

4.5. The joint targeting cycle consists of six phases and is equally applicable to both deliberate and dynamic target prosecution. The phases are built on the principles of effective and efficient joint targeting. The cycle focuses targeting options on the commander's objectives for operations, while diminishing the likelihood of undesirable consequences. The joint targeting cycle is shown below at Figure 4.1 along with a brief explanation of each phase.[88]

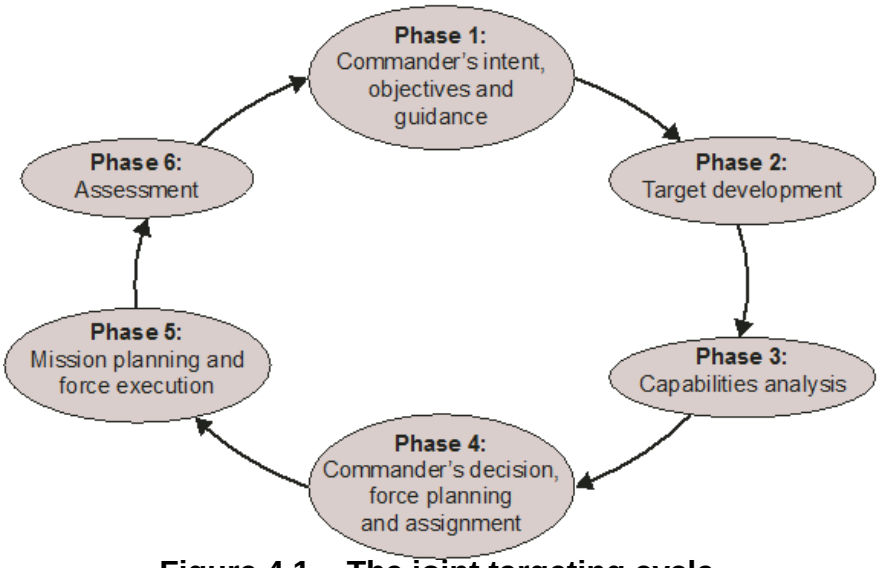

Figure 4.1 – The joint targeting cycle.

a. **Phase 1 – Commander's objective, guidance and intent.** Identifies what the

[88] The joint targeting cycle is explained in detail in Allied Joint Publication (AJP)-3.9, *Allied Joint Doctrine for Joint Targeting*. It should also be noted that the land targeting cycle is similar to this model but has only five stages – decide, detect, track, deliver and assess; it is described in detail in AJP-3.9.2, *Land Targeting*.

commander wants to accomplish, under what circumstances and within which parameters based upon political, strategic, and operational-level guidance. Phase 1 is supported by the intelligence staff.

b. **Phase 2 – Target development.** Target development identifies eligible targets that can be influenced to achieve the joint commander's objectives. It also includes target analysis, vetting, validation, nomination and prioritization.

c. **Phase 3 – Capabilities analysis.** Analysis of prioritized targets from Phase 2 and recommends to the joint commander the synchronized combination of the most appropriate capabilities (lethal and non-lethal) that can be applied to generate the desired effects.

d. **Phase 4 – Commander's decision, force planning and assignment.** Integrates the outputs of capabilities analysis with any further operational considerations, which is supported by the intelligence staff. The joint commander then issues final approval for prioritized targets, which are then assigned to specific components for planning and execution.

e. **Phase 5 – Mission planning and force execution.** This phase deals directly with planning and execution of tactical activity and is largely the responsibility of the components. This phase requires the gaining of positive identification of the target and the coordination of collection assets and initial assessments.[89]

f. **Phase 6 – Assessment.** Assessment is defined as: *the process of estimating the capabilities and performance of organizations, individuals, materiel or systems*.[90] The assessment phase within the joint targeting cycle seeks to measure if the planned effects have been realized after tactical activities have been executed. It contributes to the wider campaign assessment process and so assists the commander's future decision-making. The phase is supported by the intelligence staff.

4.6. Intelligence support is used throughout the joint targeting cycle but is particularly relevant to the following phases.

a. **Phase 1 – Commander's objective, guidance and intent.** Targets are developed once the commander has selected their objectives. Intelligence provides the commander with an understanding of the adversary in terms of probable intent, objectives, strengths, weaknesses, probable courses of action and any critical factors. This is conducted as part of the intelligence estimate

[89] Target execution consists of seven steps: find, fix, track, target, engage, exploit and assess (F2T2E2A).

[90] Note: In the context of military forces, the hierarchical relationship in logical sequence is: assessment, analysis, evaluation, validation and certification. AAP-06(2014).

and joint intelligence preparation of the operational environment (JIPOE) and supports comprehensive preparation of the operational environment (CPOE).

b. **Phase 2 – Target development.** Critical to the success of the entire targeting process is the establishment of intelligence requirements at all levels, which in turn drive the collection effort. The adversary's systems will be analyzed by the intelligence staff using various methods to support centre of gravity analysis and the determination of exploitable vulnerabilities. The target clearance process may also generate additional requests for information or collection requirements not previously identified.

c. **Phase 5 – Mission planning and force execution.** Intelligence support to mission planning confirms whether the assessments and decisions made during the target approval process remain valid or not. If not, the original engagement decision must be revisited. During execution, the situation may change as the adversary responds. The JISR staff should also coordinate collection capabilities to support initial and follow-on assessment.

d. **Phase 6 – Assessment.** This is focussed on assessment by gathering information that is critical for the evaluation of measures of effectiveness and assessing campaign progress.

Section 3 – Deliberate targeting

4.7. At the operational level, commanders and their staff establish the objectives and guidance for targeting, including the approved target sets and target engagement authority. Deliberate targeting is the process by which planned targets known to exist in an operational area are prosecuted with lethal or non-lethal actions. Targets may be engaged in accordance with a timed schedule or held on call to engage if the situation demands it. In all cases, target data has sufficient detail to allow the capability matching and force assignment of elements of the joint targeting cycle to be planned and conducted.

Section 4 – Dynamic targeting

4.8. Dynamic targeting normally prosecutes targets known to exist in the area of operations. They have received some target development but were not detected, located or selected for action in sufficient time to be included in the deliberate process. For anticipated dynamic target engagements, a planned JISR operation may be developed in conjunction with available strike assets. The intelligence staffs conduct intelligence requirement management (IRM) and collection management (CM) to prepare the appropriate collection asset to focus on the area of operations during the time that strike assets are positioned to engage identified targets.

Unanticipated dynamic targets may require rapid tasking and rapid execution of the intelligence cycle, including JISR planning.

Section 5 – Time-sensitive targets

4.9. Time-sensitive targets (TST) are specific targets designated by the Joint Force Commander, who should provide guidance and prioritization for all TSTs within the operational area. TSTs are targets that have been developed through the same procedures as planned targets and require an immediate response. TSTs can be prosecuted using both the deliberate and dynamic approach.

4.10. A TST requires a target execution cycle comprising find, fix, track, target, engage, exploit and assess (F2T2E2A). An identified TST will be placed on the intelligence collection plan (ICP) with a high priority. Once a potential TST is identified, the target has to be positively identified. The execution of TSTs requires the high priority (through inclusion in the intelligence collection plan), rapid re-tasking of JISR collection assets, and rapid processing and dissemination of relevant information and intelligence by the intelligence staff.

Section 6 – Battle damage assessment

4.11. 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*.[91]

4.12. 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.

4.13. BDA is composed of three phases.

a. **Phase 1.** A quick assessment to quantitatively estimate the amount of physical damage or behavioural influence achieved against a target.

b. **Phase 2.** Reviews and amplifies the Phase 1 BDA providing a functional assessment by estimating how the physical or psychological effect on a target has degraded its ability to perform its intended mission or shifted a behavioural pattern.

c. **Phase 3.** Makes an assessment of the effect of the engagement on the entire target system. This assessment is based upon the understanding of an individual target role within the target system and depends on the target system

[91] AAP-06 (2014).

analysis (TSA) conducted at the beginning of the targeting process. This type of BDA is normally undertaken at the operational level.

4.14. All phases of BDA are planned activities and analysis is directed to specific intelligence support either by target or by target category. Thus, even dynamic targets that require BDA are assigned to an analysis unit in advance of the strike. Intelligence staff should establish effective procedures to support BDA.

4.15. BDA requires all three intelligence core activities:

- IRM to determine where and when collection needs to occur;
- JISR/collection to gather the required information; and
- processing and dissemination to provide analysed information to the operations/intelligence staff, particularly in target support cells (TSC) or TST coordination elements (TCE), in order to support their activities.

ANNEX A – INTELLIGENCE CAPABILITIES AND STANDARDIZATION

A.1. Although Allied Joint Doctrine (AJP)-2.1, *Allied Joint Doctrine for Intelligence, Procedures* aims to describe generic intelligence procedures, without detailing specific processes relating to individual disciplines, it is important to briefly highlight the different intelligence collection capabilities available and the associated standardization agreements (STANAGs) for completeness, and to promote collaboration. In addition, reference is made to the NATO Intelligence Fusion Centre and National Intelligence Centres, these are both outside of the NATO Command Structure, but have been referred to as examples of supporting agencies.

A.2. **Counter-intelligence (AJP 2.2, *Counter-intelligence and Security Procedures*, STANAG 2192).** Counter-intelligence (CI) is defined as: *those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in espionage, sabotage, subversion or terrorism*.[92] The counter-intelligence effort aims to protect personnel, information, plans and resources, both at home and when deployed, by a combination of defensive and offensive measures. It aims to provide knowledge and understanding of the prevailing situation to keep privileged information secret, equipment secure and personnel safe. Counter-intelligence should be proactive and preventative in its approach. Counter-intelligence is an intelligence function that provides commanders at all levels with a detailed understanding of threats, vulnerabilities and risks to enable them to make well-reasoned decisions on security measures.

A.3. **Human intelligence (AJP 2.3, *Allied Joint Doctrine for Human Intelligence*, STANAG 2537, Allied Intelligence Publication (AIntP)-5, *Doctrine for Human Intelligence (HUMINT) Procedures*, STANAG 2578).** Human intelligence (HUMINT) is defined as*: intelligence derived from information collected by human operators and primarily provided by human sources*.[93] HUMINT includes the systematic and controlled exploitation, by interaction with human sources, or individuals. It has the ability to provide information regarding an actor's intentions, morale, and relationships among individuals and organizations.

A.4. **Signals intelligence (AJP 2.4, STANAG 6504 (NR)).** Signals intelligence (SIGINT) is defined as: *intelligence derived from electromagnetic signals or emissions*.[94] SIGINT is the generic term used to describe communications intelligence (COMINT)

[92] NATO Agreed – NATOTerm.

[93] NATO Agreed – NATOTerm.

[94] Note: The main subcategories of signals intelligence are communications intelligence and electronic intelligence. NATO Agreed – NATOTerm.

and electronic intelligence (ELINT) when there is no requirement to differentiate between them. COMINT and ELINT are respectively defined as follows.

a. **Communications intelligence.** Communications intelligence is defined as: *intelligence derived from electromagnetic communications and communication systems*.[95] Typically derived through the interception of communications and data links. Such information may be collected in verbal form by the reception of broadcast radio messages, by the interception of point-to-point communications such as telephones and radio relay links, or as data through the interception of either broadcast or point-to-point data down links.

b. **Electronic communications.** Electronic communications is defined as: *intelligence derived from electromagnetic, non-communications transmissions*.[96] It is derived from the technical assessment of electro-magnetic non-communications emissions such as those produced by radars and by missile guidance systems. It also covers lasers and infrared devices and any other equipment that produces emissions in the electromagnetic spectrum.

A.5. **Captured personnel, material and documents (AJP 2.5(A), *Captured Personnel, Material and Documents*[97], STANAG 2195).** Intelligence exploitation activities are conducted at three levels ranging from the site of the capture or recovery to exploitation facilities within the theatre of operations to highly specialized facilities located outside the theatre of operations, for example, on the territory of a lead capability nation. At the lowest level, materiel is recovered or seized, and designated persons are captured or otherwise detained. Ideally, specialist personnel should support tactical units in the field in order to ensure the correct handling of recovered and seized materiel as well as captured persons (CPERS). At the higher levels, specialized exploitation capabilities further extract information of intelligence value.

A.6. **Geospatial intelligence.** Geospatial intelligence (GEOINT) is defined as: *intelligence derived from the combination of geospatial information, including imagery, with other intelligence data to describe, assess and visually depict geographically referenced activities and features on the earth*.[98]

A.7. **Imagery intelligence (AJP 2.6, STANAG 6507).** Imagery intelligence (IMINT) consists of intelligence derived from imagery – 'a picture being worth a thousand words' is especially true in intelligence. The information conveyed by an image is

[95] NATO Agreed – NATOTerm.

[96] NATO Agreed – NATOTerm.

[97] A rewrite of AJP-2.5 is underway with its study title changed to: *Intelligence Exploitation of Information from Materiel and Captured Persons*.

[98] NATO Agreed – NATOTerm.

generally clear, concise and in the main unequivocal and will often serve to support or confirm intelligence derived from other intelligence disciplines. The bulk of IMINT is derived from satellites and manned or unmanned aircraft.

A.8. **Measurement and signature intelligence[99].** Measurement and signature (MASINT) intelligence is defined as: *scientific and technical intelligence derived from the analysis of data obtained from sensing instruments for the purpose of identifying any distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification*.[100] MASINT is divided into eight sub-disciplines in NATO: biometrics, radio, geophysical, electro-optical, nuclear, materials, multi/hyper-spectral, and radar.

A.9. **Open source intelligence[101].** Open source (OSINT) intelligence is defined as: *intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access*.[102] OSINT is derived from sources such as radio, television, newspapers, state propaganda, journals and technical papers, the Internet, technical manuals and books and other media. OSINT is most likely to be the source of basic intelligence, however, there will be occasions when OSINT is used to produce current intelligence.

A.10. **Biometrics[103] (AIntP 15, STANAG 6515).** Biometrics is the automated recognition of individuals based on their behavioural (for example, gait or signature) and biological characteristics (fingerprint, face, iris, voice, DNA). Biometrics is an enabling capability for intelligence and aims together with other information/intelligence to create identity intelligence. The technical standards for the interchange of biometric data and watch listing are set by STANAG 4715.

A.11. **Technical exploitation (AIntP-10, STANAG 6502).** Technical exploitation is the application of scientific methods to gain further knowledge and insight from information, materiel and captured persons (CPERS). Materiel may include documents, electronic components and storage media, weapons, explosives and other pertinent materiel. Technical exploitation builds understanding of threat capabilities, feeds intelligence and supports a proactive posture to minimize, neutralize and/or defeat threats. Effective application of technical exploitation capabilities supports follow-on operations (targeting, enhanced force protection and

[99] MASINT AJP and associated STANAG expected to be endorsed by NATO (AJOD) shortly.
[100] NATO Agreed – NATOTerm.
[101] OSINT AJP and associated STANAG expected to be endorsed by NATO (AJOD) shortly.
[102] NATO Agreed – NATOTerm.
[103] A rewrite of AIntP is underway with its study title changed to: *Countering Threat Anonymity: Biometrics in Support of NATO Operations and Intelligence.*

law enforcement operations) while enabling rapid adaptation of technologies and tactics, techniques and procedures into operations and training.

A.12. **Acoustic intelligence.** Acoustic intelligence (ACINT) is defined as*: intelligence derived from acoustic signals or emissions*.[104] Examples of ACINT sources are hydrophones, geophones, SONAR, integrated underwater surveillance systems and artillery sound ranging systems.

A.13. **Space-based systems.** These intelligence, surveillance and reconnaissance (ISR) systems have a unique advantage of near global coverage that allows observation of areas of interest over great distances, especially those remote or hostile areas where other ISR systems cannot be employed. Other advantages include mission longevity and relative immunity from opponent action. Additionally, these systems can often cue or be cued by other ISR systems to watch a specific area of interest, enhancing accuracy and reaction times for the users of that information.

a. **Military systems.** These ISR systems employ a variety of sensor suites and provide a broad range of capabilities. Space systems routinely support training activities, ongoing operations, monitor indicators and warnings and provide early detection of ballistic missile attack. Environmental monitoring systems provide military forces with detailed geographic and meteorological data that enhances mission planning capabilities and aids the commander in anticipating environmental conditions which make affect operations.

b. **Non-military systems.** These systems normally complement military space systems and include civil and commercial capabilities. They possess a variety of capabilities, but their availability may be limited and thus should not be relied upon as a primary source of data. Examples include weather and multi-spectral imagery satellites, which commanders may be able to task directly, depending on the terms of share-use agreements with the owners.

A.14. **Special operations forces.** Special operations forces (SOF) conduct clandestine or low profile special surveillance and reconnaissance by maritime, land or air activities in support of joint operations. The information they provide can generally contribute to the intelligence picture at all levels and may be used to cue other ISR systems. SOF can often interpret what they see and provide important judgment. SOF also have the skills to reach and communicate with civilians and indigenous forces in order to gather information.

A.15. **Human network analysis and support to targeting (AIntP-13, STANAG 6508).** Human network analysis and support to targeting[105] (HNAT) is an intelligence

[104] NATO Agreed – NATOTerm.

[105] MCM-0064-2011 describes this concept which aims to provide a standardized capability to understand human networks and provide targetable information.

function that is a component of NATO's approach to attacking the networks (AtN). HNAT is defined as: *an intelligence process that provides understanding of the organizational dynamics of human networks and recommends individuals or nodes within those networks for interdiction, action, or pressure*.[106] HNAT consists of human network analysis (HNA) and HNA support to operations, targeting, and effects that influence, attack, neutralize and influence networks.

A.16. **NATO Intelligence Fusion Centre.** The NATO Intelligence Fusion Centre (NIFC) is based in Molesworth, United Kingdom. The NIFC is a military led, US sponsored memorandum of understanding organization, relying on the framework nation and national commitment to maintain it. It is not therefore, directly in the NATO Command Structure and relies on individual nations to support its work and the delivery of operational intelligence. It provides Supreme Allied Commander Europe (SACEUR) and subordinate commanders with timely and fused all-source intelligence in support of the planning and execution of the NATO Response Force, a combined joint task force, or other formation as required. The NIFC supports peacetime requirements and current and crisis operations in NATO area of responsibility/area of interest. It hosts a core of allies experienced in common tactics, techniques and procedures to create functional partnerships and maximize analytical capabilities. It also defines critical threats, and evaluates changes to technological, political and military trends which may impact NATO and the support it provides.

A.17. **National intelligence cells.** NATO nations may retain national command and control of assets which are operating as part of or alongside NATO operations. In order that associated national commanders have direct access to intelligence, national intelligence cells (NICs) may be established. Operational-level NICs are equipped and staffed by the relevant nation and can be attached to a permanent or deployed NATO Headquarters. They provide a means for direct and timely exchange of national intelligence and should be considered as part of the routine headquarters lay down for each of the nations involved in the operation.

[106] NATO Agreed – NATOTerm.

Intentionally blank

LEXICON

Part 1 – Acronyms and abbreviations

AAP	Allied administrative publication
ACINT	acoustic intelligence
ACO	Allied Command Operations
AII	area of intelligence interest
AJP	Allied joint publication
AWG	Assessment Working Group
BDA	battle damage assessment
CCIR	commander's critical information requirement
CCIRM	collection co-ordination and intelligence requirements management
CJSOR	combined joint statement of requirement
CM	collection management
COA	course of action
COG	centre of gravity
COMINT	communications intelligence
CONOPS	concept of operations
COPD	comprehensive operations planning directive
CPERS	captured persons
CPOE	comprehensive preparation of the operational environment
CRL	collection requirement list
CTL	collection task list
EEI	essential elements of information
ELINT	electronic intelligence
F2T2E2A	find, fix, track, target, engage, exploit and assess find fix track target exploit analyse
GEOINT	geospatial intelligence
HNAT	human network analysis and support to targeting
HUMINT	human intelligence
ICP	intelligence collection plan
IMINT	imagery intelligence
INTREP	intelligence report
INTSUM	intelligence summary
IRM	intelligence requirement management
ISR	intelligence, surveillance and reconnaissance

ISSA	intelligence system support architecture
JCB	joint coordination board
JCMB	joint collection management board
JIE	joint intelligence estimate
JIPOE	joint intelligence preparation of the operational environment
JISR	joint intelligence, surveillance and reconnaissance
JOPG	joint operations planning group
JPTL	joint prioritized target list
JTCB	joint targeting coordination board
MASINT	measurements and signatures intelligence
MC	military committee (NATO)
MOE	measurement of effectiveness
MOP	measurement of performance
MRO	military response option
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NIC	national intelligence cell
NRF	NATO response force
OLPP	operational-level planning process
OPLAN	operation plan
OPP	operations planning process
OLRT	Operational Liaison and Reconnaissance Team
OSINT	open source intelligence
PIR	priority intelligence requirement
PMESII	political, military, economic, social, infrastructural and information
RFI	request for information
SAB	situational awareness brief
SACEUR	Supreme Allied Commander Europe
SHAPE	Supreme Headquarters Allied Powers Europe
SIGINT	signals intelligence
SIR	specific intelligence requirement
SOF	special operations forces
SOR	statement of requirement
TA	Target audience
TAA	Target audience analysis
TCE	TST coordination element
TCSOR	theatre capability statement of requirements

TSA	target system analysis
TSC	target support cell
TST	time-sensitive target
TTP	tactics, techniques and procedures

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 is 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. (NATO Agreed.)

area of intelligence responsibility
An area allocated to a commander, in which he is responsible for the provision of intelligence, within the means at his disposal. (NATO Agreed)

area of operations
An area defined by the joint force commander within a joint operations area for the conduct of specific military activities. (NATO Agreed.)

asymmetric threat
A threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting his weaknesses to obtain a disproportionate result. (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. (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 converting intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection sources or agencies, monitoring results and re-tasking, as required. (NATO Agreed.)

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

deception
Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (NATO Agreed.)

evaluation
In intelligence usage, a step in the processing phase of the intelligence cycle constituting appraisal of an item of information in respect of the reliability of the source, and the credibility of the information. (NATO Agreed.)

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
In intelligence usage, 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. (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
Intelligence architecture consists of the overall space, condition, surroundings, 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. (This term is a new term and definition will be processed for NATO Agreed status.)

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 requirements management
The complex management function which validates and prioritizes incoming intelligence requirements, coordinates the collection of associated information, quality controls processed outputs, and oversees dissemination of intelligence product. (This term and definition is only applicable to this publication.)

interpretation
In intelligence usage, the final step in the processing phase of the Intelligence cycle in which the significance of information and/or Intelligence is judged in relation to the current body of knowledge. (NATO Agreed.)

joint intelligence, surveillance and reconnaissance
(JISR)
A set of intelligence and operations capabilities, to synchronize and integrate 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. (This term is a new term and definition will be processed for NATO Agreed status.)

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. [AAP-39 (not 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
Specific intelligence requirements support and complement each PIR and provide a more detailed description of the requirement. (This term is a new term and definition and will be processed for NATO Agreed status.)

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 of aerospace, surface on subsurface areas, places, persons or things by visual, aural, 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: person includes their mindset, thought processes, attitudes and behaviours. (This term and definition is a modification of an existing NATO agreed term and/or definition in AJP-3.9 and is being processed for NATO Agreed status.)

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
Time-sensitive targets (TSTs) are derived from North Atlantic Council-approved (NAC) TST categories and, from these, specific targets are designated by the joint force commander (JFC). TSTs are 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. [MC 471/1, 15 June 2007 (not NATO Agreed.)]

AJP-2.1(B)(1)