NATO STANDARD

AJP-2

ALLIED JOINT DOCTRINE FOR INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY

Edition B Version 1

JULY 2020

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

24 July 2020

1. The enclosed Allied Joint Publication AJP-2, Edition B, Version 1, ALLIED JOINT DOCTRINE FOR INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY, 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 2190.

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

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

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

Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

Intentionally blank

Reserved for national promulgation letter

Intentionally blank

RECORD OF NATIONAL RESERVATIONS

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

Intentionally blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
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

Related documents

a.	MCM-0077-2000	Military Committee Guidance on the Relationship between NATO Policy and Military Doctrine
b.	MC 0064/10	NATO Electronic Warfare Policy
c.	MC 0101	NATO Signals Intelligence Policy and Directive
d.	MC 0114	Procedures for Production of NATO Agreed Intelligence
e.	MC 0128	Policy Guidance for NATO Intelligence
f.	MC 0133	NATO's Operations Planning
g.	MC 0166	NATO Intelligence Warning System (NIWS)
h.	MC 0296	NATO Geospatial Policy
i.	MC 0327	NATO Military Policy for Non-Article 5 Crisis Response Operations
j.	MC 0402	NATO Military Policy on Psychological Operations
k.	MC 0422	NATO Military Policy for Information Operations
l.	MC 0472/1	MilitaryCommittee Concept for Counter-Terrorism
m.	MC 0582	NATO Joint Intelligence, Surveillance and Reconnaissance (JISR) Concept
n.	MC 0596	NATO Imagery Intelligence (IMINT) Policy
o.	MC 0605	NATO Human Intelligence (HUMINT) Policy
p.	MC 0628	NATO Military Policy on Strategic Communications
q.	MC 0646	NATO Joint Intelligence, Surveillance and Reconnaissance (JISR) Policy
r.	MC 0647	Policy on Open Source Intelligence (OSINT)
s.	Bi-MNC	Reporting Directive Volume II – Intelligence Reports
t.	AJP-01	Allied Joint Doctrine
u.	AJP-2.1	Allied Doctrine for Intelligence Procedures
v.	AJP-2.2	Counter-Intelligence and Security Procedures
w.	AJP-2.3	Allied Joint Doctrine for Human Intelligence (HUMINT)
x.	AJP-2.4	Allied Joint Doctrine for Signals Intelligence (SIGINT)
y.	AJP-2.6	Allied Joint Doctrine for Imagery Intelligence (IMINT)
z.	AJP-2.7	Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance (JISR)

aa.	AJP-2.8	Allied Joint Doctrine for Measurement und Signature Intelligence (MASINT)
bb.	AJP-2.9	Allied Joint Doctrine for Open Source Intelligence (OSINT)
cc.	AJP-3	Allied Joint Doctrine for the Conduct of Operations
dd.	AJP-3.8	Allied Joint Doctrine for Comprehensive Chemical, Biological, Radiological, and Nuclear Defence
ee.	AJP-3.9	Allied Joint Doctrine for Joint Targeting
ff.	AJP-3.10	Allied Joint Doctrine for Information Operations
gg.	AJP-3.10.1	Allied Joint Doctrine for Psychological Operations
hh.	AJP-3.11	Allied Joint Doctrine for Meteorological and Oceanographic Support to Joint Forces
ii.	AJP-3.14	Allied Joint Doctrine for Force Protection
jj.	AJP-3.15	Allied Joint Doctrine for Countering Improvised Explosive Devices (C-IED)
kk.	AJP-3.17	Allied Joint Doctrine for Geospatial Support
ll.	AJP-3.20	Allied Joint Doctrine for Cyberspace Operations
mm.	AJP-3.21	Allied Joint Doctrine for Military Police
nn.	AJP-3.22	Allied Joint Doctrine for Stability Policing
oo.	AJP-5	Allied Joint Doctrine for the Planning of Operations
pp.	AAP-06	NATO Glossary of Terms and Definitions
qq.	AAP-03	Production, Maintenance and Management of NATOs Standardization Documents
rr.	AAP-47	Allied Joint Doctrine Development
ss.	AAP-32	Publishing Standards for Allied Publications
tt.	C-M(2002)49	Security within the North Atlantic Treaty Organization
uu.	C-M(2002)50	Protection Measures for NATO Civil and Military Bodies
vv.	C-M(2002)60	The Management of Non-Classified NATO Information
ww.	AD65-5	Intelligence requirements management and collection management
xx.	AD65-11	Intelligence Production Management
yy.	AD70-01	Security Directive
zz.	COPD V2	Comprehensive Operations Planning Directive

aaa. AC/35-D/2002 Directive on the Security Information

bbb. AC/35-D/1040 Supporting Document on Information and Intelligence Sharing with Non-NATO Entities

Intentionally blank

Table of contents

Figures and tables:

PREFACE

SCOPE

AJP-2 is the keystone NATO doctrine for intelligence. It provides the fundamental principles and guidance for intelligence support to joint operations. Within the subordinated publications more details are provided for example in conjunction with intelligence procedures, JISR and intelligence collection disciplines.

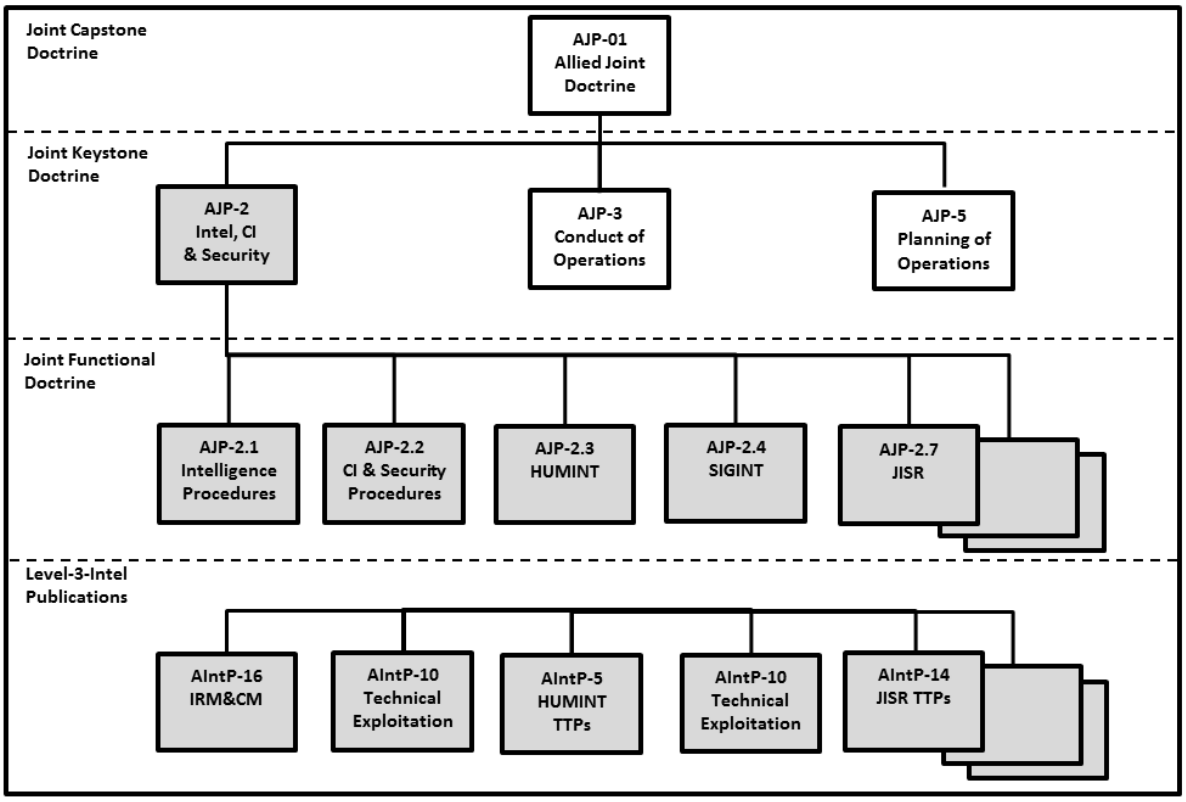

Figure 1. NATO Joint Doctrine Architecture and the hierarchy of Intelligence Doctrine & Publications

PURPOSE

AJP-2 provides a clear understanding of the critical importance of intelligence, counter-intelligence and security in order to optimize their contributions during the planning and conduct of operations.

APPLICATION

AJP-2 is intended primarily for commanders and staff at the joint operational level. The doctrine also provides a general framework to facilitate a common understanding of the intelligence function throughout all levels of NATO, partner nations and other joint force compositions.

Intentionally blank

Chapter 1 INTRODUCTION

1.1 PURPOSE OF INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY

Current operational complexities require commanders to regard intelligence as a critical prerequisite for operations rather than simply a means of determining the obstacles to accomplishing a mission. At the same time, the intelligence staff should consider a greater number of actors[1], an increasing number of intelligence support systems, a wider range of intelligence requirements and larger numbers of collection capabilities. It must be understood that intelligence guides operations planning. Commanders and staffs at every level require intelligence to plan, direct, conduct, and assess campaigns and operations. Intelligence is crucial in setting strategy, identifying and selecting specific objectives and targets, associating those objectives and targets with desired effects, and determining the means to accomplish the overall mission. Intelligence is to contribute to a continuous and coordinated understanding of the operating environment (OE), and to support commanders in decision making by helping to identify conditions required to achieve desired objectives. Intelligence belongs to the framework of joint functions at all levels in addition to manoeuvre, fires, command and control, information, sustainment, force protection and civil-military cooperation[2].

Security is the condition achieved when designated information, materiel, personnel, activities, and installations are protected satisfactorily against terrorism, espionage, sabotage, subversion, organized crime (TESSOC[3]) as well as against damage, loss or unauthorized disclosure. This is achieved through the measures implemented to protect satisfactorily against threats to security, in accordance with the requirements of the NATO Security Policy documents, C-M(2002)49 and C-M(2002)50. Measures for the maintenance of Security and the measures of counter-intelligence are implemented for counteracting the threat to security posed by hostile intelligence services and subversive, criminal or terrorist groups or individuals or other actors. Security at all levels will be command led. Within NATO, security staffs are established at all levels of command. Host nations are primarily responsible for the external protection of NATO installations located in their territory. National plans therefore should be developed and close liaison maintained between national staffs and NATO commands. The threat is met by making proper provision for the maintenance of security at the earliest possible stage of planning, particularly in the construction of installations.

Counter-intelligence (CI) is to protect personnel, information, activities, plans and resources, both at home and when deployed, against threats posed by hostile intelligence services, and subversive, terrorist and criminal groups or individuals. CI aims to provide knowledge and understanding of the prevailing situation to keep privileged information secret, equipment secure and personnel safe. CI should be proactive and preventative in its approach.

---

1 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.)

2 See Allied Joint Publication (AJP)-01.

3 This abbreviation will be processed to NATO agreed status.

1.2 INTELLIGENCE AS A JOINT FUNCTION

Common to joint operations at all levels, intelligence is one of the eight defined joint functions[4]: Manoeuvre, fires, command and control, intelligence, information, sustainment, force protection and civil-military cooperation (CIMIC). The joint functions are a framework that provides commanders and staffs the means to visualize the activities of the force and to ensure all aspects of the operation are addressed. They are a point of reference, as well as a description of the capabilities of the force. Commanders need to consider the joint functions, both when determining the capabilities required for a joint force and when conducting the operation. Joint functions provide a sound framework of related capabilities and activities grouped together to assist commanders to integrate, synchronize, and direct various capabilities and activities in joint operations. Using joint functions, commanders, in conjunction with the strategic level of command, can determine force requirements.

All joint functions are defined with regard to their subordinate tasks and related capabilities. Some of them can apply to other functions, so they can be intermingled. Intelligence is not an exception and can be also related with other joint functions. In any joint operation, commanders may choose from a wide variety of joint and service capabilities and combine them in various ways to perform joint functions to accomplish the mission. Intelligence capabilities can often be used sequentially while executing a single task or in multiple functions simultaneously.

Joint functions underpin planning and organizing the conceptual framework that permits force integration and synchronization, which is called joint action. Joint action is described as the deliberate use and orchestration of military capabilities and activities to affect an actors´ understanding, capability and will, and the cohesion between them[5]. Joint action focuses on affecting adversaries through the combined application of the joint functions. Consequently, intelligence is one of the main drivers of the process by integrating intelligence (understanding of the OE) and joint intelligence, surveillance and reconnaissance (JISR) capabilities into joint operations planning. Intelligence as a joint function should be used in any operation, although its contribution and demands will vary, dependent on the type of operation and complexity of the operating environment.

Intelligence as a joint function has a unique role in the comprehensive analysis and understanding of the OE, which is the starting point of the operations planning process (OPP). Commanders must build and foster an understanding of the OE throughout all phases of the joint operation. Intelligence staff is also engaged in the planning process by identifying operational requirements with regard to intelligence and JISR capabilities as part of crisis response measures and combined joint statement of requirements (CJSOR).

Intelligence contributes to a continuous and coordinated understanding of the OE:

- to identify conditions required to achieve desired objectives,
- avoiding undesired effects and
- assessing the impact of adversary, friendly and neutral actors on commanders' concept of operations.

[4] See AJP-3
[5] See AJP-3

Intelligence is an aid to provide situational awareness, develop understanding and is a critical tool for decision-making. Operations should be intelligence-driven by providing the commander with timely and accurate intelligence that supports their particular needs and is tailor-made to those requirements. These roles are supported by a series of specific responsibilities of the intelligence staff, including:

- inform commanders,
- describe the operating environment,
- identify, define, and nominate objectives,
- support planning and execution of operations,
- counter adversary deception and surprise and
- assess the effectiveness of operations.

Therefore, intelligence is a key component for planning and conducting operations throughout the entire OPP and execution of operations. It provides timely and accurate information, describes the OE, contributes to preparing operations design concept, and is actively engaged in all stages of planning activities. The changing character of conflicts emphasizes the need to place intelligence within the wider concept of understanding, where commanders must get a holistic view of the OE, with a particular emphasis on the human environment in which adversaries and other actors will compete with and confront each other. Intelligence is not only for assessing adversaries' forces and their preparedness to engage in conflict. Intelligence is an enabling capability whose value is largely realized through joint operations.

Intelligence requires systems, architectures and practitioners flexible enough to operate in a complex environment.
The intelligence staff provides accurate, timely and relevant intelligence to meet the commander's operational, intelligence and security requirements within the joint operations area (JOA) and maintaining situational awareness and understanding in the area of intelligence interest and area of intelligence responsibilities. As such the intelligence staff establishes an all-source intelligence cell (ASIC) to correlate and fuse all available, relevant data, information, JISR results and intelligence.[6]

The intelligence process[7] supports all phases of the OPP with the J2-contribution which is called joint intelligence preparation of the operating environment (JIPOE)[8]. The JIPOE process is a disciplined analytical methodology conducted by the intelligence staff that produces intelligence assessments, estimates, and other intelligence products to support operations planning. JIPOE is a 3-step process that informs joint planning by providing planners and decision makers with a comprehensive understanding of the operating environment and the actors within the operating environment. JIPOE is to develop a comprehensive understanding of the operating environment covering all elements of the political, military, economic, social, infrastructural and informational (PMESII) spectrum[9], including associated opportunities, 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 operating

[6] The ASIC (all-source intelligence cell) is an organizational element. Not every command might implement an ASIC and call it like that but will install an element which will fulfill the function.
[7] The intelligence process is also called the intelligence cycle, because it is a cyclic process.
[8] See also Allied Intelligence Publication (AIntP)-17 JIPOE
[9] See also closer description in Chapter 5.2 on PMESII spectrum. See also AJP-01.

environment including its maritime, land, air and space, and cyberspace[10] domains; as well as the PMESII factors of the main adversaries, friends and neutral actors that may influence joint operations. The close alignment of the intelligence process and the J2-contribution to the planning process through JIPOE means that intelligence produced at any level can be used seamlessly throughout the command chain, and ultimately contributes to operational success by providing better situational awareness to assist commander's decision making.

The complexity of modern operations produces a greater need for all-encompassing intelligence, which uses a wide range of sources and agencies to develop understanding of the operating environment. This relies upon all available capabilities (i.e., geospatial, cultural, linguistic, etc.) for collection, the subsequent processing, and dissemination of fused intelligence to satisfy intelligence requirements. There is an increasing need for intelligence that draws upon a wide range of sources and collected data and information to provide a comprehensive understanding of the operating environment. These requirements should also be included into CJSOR planning.

1.3 FACTORS AFFECTING INTELLIGENCE

Within the context of the operating environment, intelligence staffs will be affected by a number of factors that will influence the way they operate. Commanders should consider those factors when creating their intelligence architecture and resourcing their intelligence staffs. The three main areas of impact are:

a. **Complexity of Operations**. The complexity of operations will influence the way that intelligence staffs operate. For example, the nature of adversaries may be different in the operating environment in that they may have no fixed infrastructure, uniforms and tangible military assets or they may operate in the geospatially and politically unconstrained cyberspace. In addition, intelligence methods should change to reflect the greater availability of data and information, the growing sophistication of intelligence capabilities as well as sophistication of actors in the environment and the impact of changing network capabilities.

b. **Information Abundance**. Information in today's world exists in overabundance and makes it difficult to direct limited resources to focus on the appropriate areas in a timely manner. Therefore, NATO's ability to find and manage relevant information is critical[11]. This requires a well-coordinated and joint approach that is efficient and dynamically adaptive. It also means that the required information is most likely hidden in a clutter of readily available material, data or information. The ability to produce and disseminate timely and reliable intelligence in relevant context is the defining feature of an intelligence organisation. Consequently, commanders at all levels need to ensure that they have adequate structures in place which include effective intelligence requirements management and intelligence production and disseminate to mitigate information saturation and overload.

c. **Blurring of Traditional Boundaries.** The flow of information across what have been previously viewed as traditional administrative, social, and political boundaries has

[10] The cyberspace domain is the global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.

[11] Especially for example to handle mass data or identify wrong data and information

increased exponentially, blurring those boundaries and creating numerous implications for the allied force. One way this change has manifested itself in military operations is in the reduced relevance of traditional boundaries between the levels of warfare (strategic, operational, and tactical) in relation to intelligence and intelligence collection. Enhanced joint intelligence, surveillance and reconnaissance (JISR) collection capabilities and improved communications have resulted in tactical commanders often having instant access to strategic intelligence, while tactical intelligence has the potential to generate strategic ramifications.

1.4 THE COMPREHENSIVE APPROACH

NATO's engagement in operations has shown that often there is a mutual dependence and synergy between military and non-military contributions to operations and their output, which is at the heart of the notion of a comprehensive approach. From a military perspective, a comprehensive approach is founded on a shared understanding and recognition that in cases where a mutual dependency exists, non-military actors may support the military and vice versa.

To contribute to the comprehensive approach, intelligence staffs must produce intelligence based on a wide range of factors. Intelligence staffs need to reach out for expertise (e.g., scientific expertise, etc.) to support their analysis or they may need to rely on reach-back[12] to supporting Alliance and national commands and agencies, including non-military and non-governmental organizations. The collaborative process described above is consistent with NATO intelligence and operational principles related to the comprehensive approach[13].

By considering a holistic spectrum like PMESII to produce complete J2-contributions and relevant intelligence for commanders, the J2-staff is able to incorporate any kind of data or information available. It may be a challenge for the intelligence staff to reach out to non-military and non-governmental organizations and to share information with them without violating information security regulations. Commanders and their intelligence staffs can improve the ability to work effectively internally through civil-military interaction with planning staffs and externally with partner countries, international organizations (IOs), governmental organizations, non-governmental organizations (NGOs), host nations (HNs) and local authorities, thus enhancing synergy at all levels.

Key actors, adversaries, environment and threats. NATO may be required to face complex and challenging operating environments where defined actors, threats and key factors are (and not limited to the following examples):

a. **Terrorism.** Terrorism is the unlawful use or threatened use of force or violence, instilling fear and terror, against individuals, organizations or property to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives.

b. **Organized crime.** Organized crime is a category of transnational, national, or local groupings of highly centralized enterprises run by criminals who intend to engage in illegal

[12] Reach-back provides products, services, applications, capabilities or material from commands, agencies and facilities that are not deployed and available in the area of operation.

[13] See AJP-3, Chapter 1.

activity, most commonly for money and profit. Governmental organizations can be involved. Such groups can be used as proxies in a conflict between two states or non-state actors where neither entity directly engages the other. While this can encompass a breadth of armed confrontation, its core definition hinges on two separate powers utilizing external strife to somehow attack the interests or territorial holdings of the other. Organized crime could enhance the capabilities of terrorists, some of whom could turn to criminals for cyberspace activities, weapons, human, organs and drugs trafficking, false documents, hard currency and other contraband (i.e., historic artifacts, energy resources smuggling). Similarly, radicalized groups may support organized crime, terrorism or violent extremism.

c. **Hostile[14] entities.** Entities (incl. nations) whose characteristics, behaviour or origin indicate that they pose a threat to friendly forces.

d. **Adversary[15] entities**. Entities (incl. nations) acknowledged as potentially hostile and against which the legal use of force may be envisaged.

e. **Vulnerable, failing, failed, post-crisis or recovering states.** States unwilling or unable to provide security and basic services to a significant portion of the population or are unwilling to protect and govern the population or are recovering from these conditions[16]. Poor governance, economic deprivation and inequality that characterizes fragile, failed and failing states pose greater risk to neighbouring states.

f. **Hybrid threats.** Hybrid threats[17] occur where military and non-military conventional, irregular and asymmetric threats[18] are combined in the same time and space. Conflict could involve a range of trans-national, state, group and individual participants operating globally, regionally or locally. Some conflicts may involve concurrent inter-communal violence, terrorism, cyberspace attacks, insurgency, pervasive criminality and widespread disorder.

g. **Environmental and humanitarian disasters.** Unpredictable natural and human-made phenomena can cause major environmental, health and humanitarian disasters such as floods, droughts, earthquakes and tsunamis, pandemics, resulting in hardship, turmoil and instability. This could require the mounting of humanitarian missions to provide the necessities of life and to mitigate the potential for conflict.

h. **Proliferation.** The proliferation of weapons of mass destruction (WMDs), and their means of delivery, threatens incalculable consequences for global stability and prosperity. Also of proliferation concern are dual-use commodities or controlled and uncontrolled commodities that may be used to support a WMD program, as well as other commodities that violate United Nations (UN) Security Council Resolutions (e.g., small arms and light weapons). Of particular concern is the likelihood that proliferation will be most acute in some of the world's most volatile regions.

---

14 In accordance with NATOTerm to „hostile“

15 In accordance with NATOTerm to „adversary“

16 See AJP-3.4.5

17 A type of threat that combines conventional, irregular and asymmetric activities in time and space (NATO Agreed).

18 For definition of “asymmetric threats” see lexicon.

i. **Actors.** Today's operating environment may consist of any combination of conventional forces, irregular fighters, criminal armed groups, any kind of threat actors[19], IOs, NGOs, and HN actors. These elements, and the interactions between them, form the human network in the OE. Human Network Analysis[20] (HNA) is one of the most decisive methodologies for defining human networks, describing human network's impact in the environment, and identifying ways to engage the network to achieve mission success. HNA is the key to assessing and understanding the relationships between persons, groups, and elements, and their impact inside the JOA.

j. **Adversary activities within cyberspace and information space.** Adversaries will not only act inside the physical domains, but in the cyberspace as well (deception, adversary information activities, adversary computer network attacks, etc.). These activities may also be conducted by one of the above described individuals, groups or entities.

k. **Peer Threats.** A peer threat is an adversary or hostile entity with capabilities and capacity to oppose NATO forces across multiple domains world-wide or in a specific region where they enjoy a position of relative advantage. Peer threats possess roughly equal combat power in geographical proximity to a conflict area with NATO forces. A peer threat may also have a cultural affinity to specific regions, providing them relative advantages in terms of time, space, and sanctuary. Peer threats generate tactical, operational, and strategic challenges that are an order of magnitude more challenging militarily than those NATO has faced since the end of the Cold War.

1.5 UNDERSTANDING

Understanding is defined as the perception and interpretation of a particular situation in order to provide the context, insight and foresight required for effective decision-making. Whatever the context, understanding involves the acquisition and development of knowledge to such a level that it enables insight (= knowing why something has happened or is happening) and foresight (= being able to identify and anticipate what may happen). Developing understanding relies first on having the situational awareness to identify the problem. Interpretation of this situational awareness provides greater comprehension (insight) of the problem; applying judgement to this comprehension provides understanding of the problem (foresight). Situational awareness and interpretation = comprehension (insight). Comprehension and judgement = understanding (foresight).

Intelligence contributes to a continuous and coordinated understanding of the operating environment, to identify conditions required to achieve desired objectives; avoid undesired effects; and assess the impact of adversary, friendly and neutral actors on the commanders' concept of operations.

Understanding flows from developing the most inclusive perspective of an actor, group, environment or situation. Building understanding takes time; rarely will understanding of an area of intelligence interest be available at the outset of a potential crisis. The approach should be sufficiently inclusive, flexible and adaptive to accommodate a wide range of experts, both

[19] Actors that by intent, capability and motivation are an existing or potential threat to the Alliance, their troops, materiel or mission.

[20] See AIntP-13

within and external to the formal NATO structure. Such experts may hold the key to understanding the operating environment.

Situational awareness is the general term used when a decision-maker at any level has sufficient knowledge of the elements in the operating environment to put new data and information into context to make rational decisions and actions.

Basic intelligence provides input to support the level of situational awareness required to create and maintain understanding of the operating environment to the commander.

Intelligence supports operations by providing timely, relevant and accurate information to commanders and staff to support their particular requirements.

Commanders' understanding is built on the JIPOE, which is an intelligence process that supports all phases of the OPP. It develops an integrated understanding of the main characteristics of the OE including its maritime, land, air, space and cyberspace[21] domains, as well as the elements of the whole PMESII spectrum's main adversaries, friends and neutral actors that may influence joint operations. The close alignment of the intelligence process and the J2-contribution to the planning process via JIPOE means that intelligence produced at any level can be used seamlessly throughout the chain of command, and ultimately contribute to operational success by providing better situational awareness to assist commanders in decision making[22].

[21] The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data..

[22] See chapter 5. on JIPOE

Chapter 2 FUNDAMENTALS AND PRINCIPLES OF INTELLIGENCE

2.1 DISCUSSION OF INTELLIGENCE

Intelligence is the product resulting from the directed collection and processing of information regarding the operating environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers. This term "intelligence" is often also applied to the activity which results in the product and to the organizations engaged in such activity.

Role of Intelligence. Intelligence contributes to a continuous and coordinated understanding of a complex global environment, to provide new knowledge and enable appropriate decisions.

Despite the blurring of boundaries between the levels of warfare, an enduring requirement for intelligence has to be categorised based on its intended use. Consequently, intelligence will be produced that fits the requirements of different levels of operations:

a. **Strategic Intelligence.** Intelligence required for the formulation of policy, strategy, military planning and the provision of indications and warning, at the national and/or international levels. Strategic intelligence focuses on providing intelligence that aids in the formulation of military policies, plans and direction that affect NATO force commitments and strategic objectives.

b. **Operational Intelligence.** Intelligence required for the planning, conduct, and assessment of campaigns at the operational level. It is used in the planning, conduct, and assessment of a campaign or operation, focusing on detailed reporting regarding the capabilities and intentions of actors and threats to develop the commanders' understanding and to assist in their decision-making.

c. **Tactical Intelligence.** Intelligence required for the planning and execution of operations at the tactical level. It focuses on threat and hazard reporting that permits commanders to accomplish tactical missions or particular short-term tasks or actions. In most cases, intelligence assets providing tactical intelligence belong to the sending state and may be part of the tactical headquarters involved.

2.2 NATO COMMAND STRUCTURE INTELLIGENCE ORGANIZATION AND RESPONSIBILITIES

NATO Intelligence Organization and Responsibilities. Each level and each command is supported by an intelligence staff to enable the commander´s decision making.

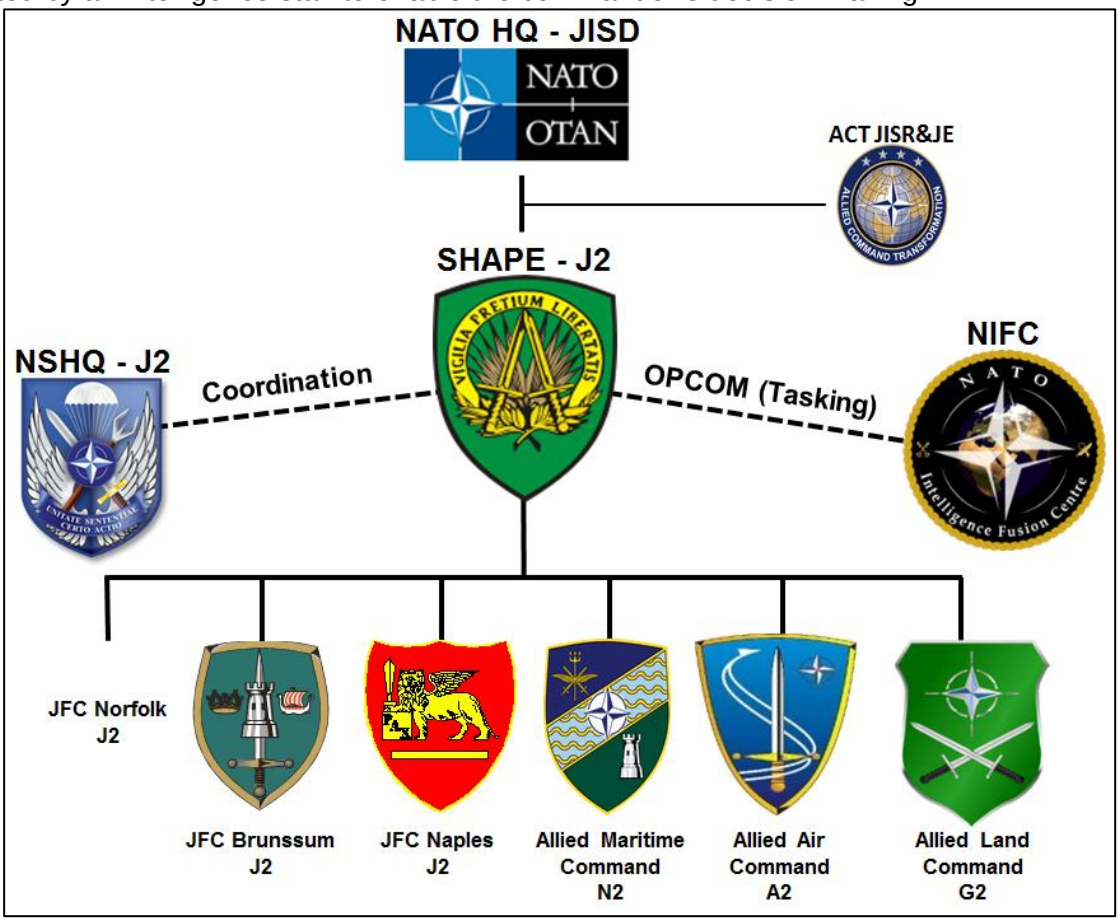

Figure 2. NATO Intelligence Organization

The Assistant Secretary General for Intelligence and Security (ASG-I&S) is the strategic leader of the NATO intelligence enterprise. The ASG-I&S is accountable to the Secretary General for leading the Joint Intelligence and Security Division (JISD) and responsible to the North Atlantic Council (NAC) and the Military Committee (MC) for the provision of intelligence at the NATO Headquarters (HQ). The principle task of the JISD is to provide NATO HQ customers with timely, reliable, impartial, relevant and coherent all-source non-agreed[23] intelligence. The ASG-I&S, as the requirements setting authority, chairs the Intelligence Steering Board (ISB). The ISB coordinates the work of NATO intelligence structures and committees, makes recommendations to the NAC and MC on matters of intelligence coordination and cooperation, as well as processes and procedures, and improves the setting of requirements for the NATO intelligence-producing bodies. The ASG-I&S is also co-chair of the Civilian Intelligence Committee (CIC) and Military Intelligence Committee (MIC); the primary advisory bodies on intelligence matters to the NAC and MC respectively. The ASG-I&S operates in accordance

[23] Intelligence produced by JISD but not agreed explicitly by every nation

with the NATO Overarching Intelligence Plan (OIP) and implements the Intelligence Production and Development Plan (IPDP).

Joint Intelligence and Security Division (JISD): The principal intelligence task of the JISD is to provide NATO HQ intelligence users with timely, reliable, impartial, relevant and coherent all-source Intelligence. The JISD is responsible for staffing intelligence policy development to constantly improve policies, working methods and procedures based on best practices and lessons learned. The principal security task of the JISD is to ensure that a state of security exists, such that NATO is able to conduct its business without hindrance, through the control of a series of seamless, linked responsibilities and relationships[24].

ACT Joint Intelligence, Surveillance and Reconnaissance & Joint Effects (JISR&JE): The ACT JISR&JE branch leads the ACT's capabilities improvement for the joint intelligence, surveillance and reconnaissance and joint effects military functional areas. The JISR&JE Branch develops and coordinates overall capability development process in accordance with DOTMLPFI[25] methodology and capability delivery governance model. It is responsible for defining capabilities performance requirements, capability programme establishment and management. In addition, it supports organization of individual intelligence training for the Alliance and develops JISR&JE related concepts and experiments.

SHAPE J2: On behalf of SACEUR, SHAPE J2 exercises strategic direction and oversight over the Allied Command Operations (ACO) intelligence community to enable SACEUR and ACO to develop strategy; execute operations; manage programmes and activities; respond to and manage crises; and identify future security challenges. To fulfill this mission, the SHAPE J2 coordinates with the intelligence elements of the Joint Force Commands, Single Service Commands (Land, Air and Maritime) and the organization of the NATO Special Operations Headquarters[26] (NSHQ) J2. On behalf of SACEUR, SHAPE J2 is also the tasking authority for the NATO´s Intelligence Fusion Centre[27] (NIFC) within the scope of ACO priority intelligence requirements (PIRs). The roles of the ACO intelligence community are defined by ACO directives.

National Intelligence Cells. Because of limited intelligence capabilities, NATO commanders are dependent on intelligence support from the nations. This support is often provided via a national intelligence cell (NIC). A NIC is a capability that is equipped and staffed by a nation to provide national intelligence support within a NATO command. It can be attached to a permanent or deployed NATO HQ. The use of a NIC provides means for direction and timely exchange of national and theatre intelligence at the operational level.

Agencies. In intelligence usage, an agency is an organization engaged in collecting or processing information. An agency may be capable of collecting and processing information or may simply have the capability to collect information and has to pass that information to another agency for processing. Agencies can be supporting or contributing organizations within NATO, nations or international organizations. They can be contacted by reach-back or be collocated with NATO forces.

---

[24] See PO(2016) 0454-Final: The NATO Overarching Intelligence Policy

[25] DOTMLPFI = doctrine, organisation, training, materiel, leadership development, personnel, facilities, and interoperability.

[26] NSHQ is a MoU organization

[27] NIFC is a MoU organization

The aims of intelligence. The primary aims of intelligence are to[28]:

a. **Enable understanding.** The intelligence staff presents actionable intelligence[29] about the operating environment and actors, including their intent, capability and motivation. The intelligence staff should strive to put this actionable intelligence into context, thereby enabling the commanders' understanding[30] based on the commanders' critical information requirements. This context includes the production of human network analysis to explain and predict why particular groups take particular actions; the production of threat assessments and security intelligence to support force protection; the production of target intelligence to support the targeting process, etc. at the respective level of command.

b. **Produce predictive assessments.** Intelligence should be forward looking, enabling commanders to maintain the initiative. Predictive assessments both involves risks and identifies opportunities. Risk is mitigated by the explicit anticipation of ranges of most likely and most dangerous outcomes, rather than the unrealistic expectation of precise outcomes. Reviews of both past and present activities may indicate future intentions and should be utilized accordingly. The focus of the intelligence staff is on situational awareness and understanding to enable commanders to assess implications and consequences of possible courses of action (COA's). Intelligence staff should think ahead and establish the relevant structures and technology as well, to make it possible to inform the commanders.

c. **Provide indications and warning (I&W).** Intelligence activities detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the Alliance. It includes forewarning of adversary actions or intentions, the imminence of hostilities, insurgency, nuclear/non-nuclear attacks on the Alliance forces, terrorists attacks; and other similar events.[31]

d. **Provide support to strategy formulation.** Intelligence plays a significant role in the development of military strategy. This role is largely defined within the context of assessing the OE including adversaries and neutral actor's capabilities and intent, but includes assisting in the articulation of a desired end state, goals, objectives and an appraisal of the resources needed.

---

[28] This paragraph does not deliver a comprehensive list of aims and does not focus on different aims of intelligence at the strategic, operational and tactical levels. Even though the levels of war have become increasingly blurred, the aims of intelligence at the strategic level (e.g., strategic indication and warning (I&W), strategy formulation) are hugely different from the aims of intelligence at the tactical level (e.g., threat assessments, target intelligence, human network analysis).

[29] Intelligence usable without delay as situational information available in due time and appropriately processed especially for the tactical level. Note: It can be used directly by commanders for the planning and execution of operations and so helps meet commanders' information needs immediately. Actionable intelligence is produced through a permanent dialogue between those who use situational information in the planning and conduct of operations and those who generate relevant situational information and make it available. Consequently, actionable intelligence differs from often descriptive and retrospective intelligence products which contain neither predictions nor recommendations worth mentioning. But actionable intelligence can be of both categories – basic and current intelligence.

[30] See closer description in Chapter 1.5

[31] For definition of "indicator" see lexicon.

e. **Support operations assessment.** Intelligence is used to evaluate and monitor operations. It can be a tool for determining whether actions and state changes meet objectives, decisive conditions, and a desired end state.

2.3 COMMANDERS, INTELLIGENCE AND DECISION-MAKING

At all levels, the relationship between the commanders and their staff is critically important for effective decision-making. Commanders provide the leadership, judgement and energy to focus the staff and the forces under their command towards the goal of accomplishing the mission.

Commanders' responsibilities. The ultimate responsibility for intelligence rests with the commanders. Commanders are the key individuals in the planning and conduct of intelligence activities. Commanders organize and assign their own staff, configuring them to meet the information, intelligence and operational requirements they set. They should be familiar with the intelligence process and have sufficient situational awareness to articulate their critical information requirements. It is commanders' responsibility to provide direction and guidance, to define priorities, to resource intelligence collection and production effectively, to demand the highest standard of products and to review the effects of their chosen actions. Commanders' key responsibility for intelligence encompass the following tasks:

a. Understand intelligence capabilities and limitations.

b. Synchronize intelligence processes with other staff cross-functional activities and procedures.

c. Set priorities and direct intelligence effort to meet operational objectives.

d. Integrate intelligence effort and capabilities with operation planning and execution.

e. Define area of intelligence responsibility (AIR) and area of intelligence interest (AII).

f. Understand and articulate priority intelligence requirements.

g. Comply with the law with regard to intelligence activities.[32]

Commanders and decision-making. Planning and decision making is a combination of science and art. Commanders are solely responsible for the decision-making process. Supported by personal experience and judgement, the commander will provide direction and guidance to the staff (e.g. J2) to drive the conduct of staff activities to support decision-making. Intelligence staffs assist in understanding the OE, specifically infrastructure installations, economics, actors, networks and their behaviour. This understanding is used by commanders to make intelligence-based decisions. Effective decision-making combines judgement with information; it requires knowing if to decide, when to decide, and what to decide. The mission analysis will highlight gaps in information and intelligence, including that which is critical for subsequent commanders' decisions. Time is a critical factor for commanders and intelligence, as any information may be of limited value the older it gets. On time collected information may

[32] See Chapter 2.7 for more detail of legal compliance requirements.

have limited value if it is not exploited by the right specialists. Timeliness is the speed required to maintain the initiative over the adversary. Intelligence delivered too late will have no impact on commanders' decisions.

Commander's vision. Vision is the ability to create a mental image of the future using imagination and wisdom. It provides the context for the development of knowledge at all levels, and for determining the level of intelligence support required. At the strategic and operational level, vision determines campaign design, how commanders prosecute the campaign, how they allocate resources and the operational priorities. At the tactical level, vision helps explain the context and purpose of an operation.

Commander's intent. Intent is a mix of the commander's vision and operational framework for the conduct of the operation. It is a commander's clear and concise expression of what the force must do and the conditions the force must establish to accomplish the mission. Commander's intent is a succinct expression in terms of priority (main effort), phase, time and space, outlining the nature, sequence and purpose of the main operational activities leading logically to the achievement of the operational objectives. Intelligence provides both information for building vision and capabilities to fulfill a commander's critical information requirements.

Operations design. Intelligence also fits extensively into the operations design process, which helps in considering and constructing viable approaches to operations. Operations design results in describing ends, ways, means and risks to take creating effects, achieving objectives and attaining the end state[33]. Intelligence staff is responsible for the development of operations design by providing intelligence, enabling the commanders understanding of the adversary and the wider OE to answer the CCIRs. These questions concern own objectives' conditions, ways and means to attain the end state and risks relate to time, space, forces/actors and information factors within the operational area.

Promoting access to intelligence. A challenge for commanders is to focus the intelligence effort and to achieve timely dissemination consistent with respective national disclosure policies. This includes ensuring the exchange of intelligence among all echelons and components. Unity of effort is essential to ensure comprehensive, accurate and current intelligence while reducing unnecessary redundancy and duplication. That implies all individuals, groups and agencies collaborate to achieve a common objective. Therefore, access to intelligence capabilities to support mission requirements should be prioritized by need and established authorizations not restricted by organizations or command configurations. If higher priority or competing tasks affect optimization of intelligence activities, commanders should make alternative provision from within their assigned resources or request assistance from other agencies through their chain of command.

Informing commanders. To maintain the initiative, commanders will seek to make decisions quickly. This requires the ability to assess the adversary's decision-making cycle, identify opportunities for exploitation and to disseminate critical information. Intelligence directly supports commanders by producing assessments and reports that aid decision-making in the context of the likelihood of adversary courses of action.

[33] See AJP-5

2.4 INTELLIGENCE CONTRIBUTION TO OPERATIONS PLANNING AND CONDUCT OF OPERATIONS

An effective contribution to operations is based on the production of focused intelligence[34] that supports decision-making related to planning, preparation and execution.

a. **Contribution to contingency planning**[35]. In the military context, contingency planning means developing plans for potential operations. The starting point for all contingency plans is to develop understanding on the strategic environment and the nature of the potential problem. Intelligence contributes to this understanding if there is a coherent framework in which the intelligence requirements are recorded in a manner that allows easy recovery in the event of a crisis. This can provide the foundation data that is required when activating or revising contingency plans.

b. **Contribution to operations planning.** The designated operational-level commanders and planning staffs require intelligence assessment on all aspects of the adversary and the operating environment of the mission area. This intelligence contributes to mission analysis and provides commanders with an understanding of possible opportunities, threats and challenges that will be faced during force employment as well as during following phases of own operations. Moreover, it assists commanders in determining the optimum composition of forces required to accomplish the mission.

c. **Contribution to preparation of forces.** As those forces or elements identified to constitute the deployed force are organized, trained, and prepared for deployment, they require intelligence assessment of the adversary and the operating environment. Intelligence influences the tactics, techniques, and procedures of the force and the manner in which it will be organized and equipped to meet its operational tasks.

d. **Contribution to execution of operations.** Intelligence enables commanders to conduct their decision-making based on a comprehensive understanding of the situation. It helps to both frame problems and illuminate their specific elements. Historically, intelligence has focused on two overlapping and complementary subjects, the adversary (their characteristics, culture, capabilities, locations, intentions, relationships and objectives) and the operating environment within which they operate. In every kind of operation the intelligence staff should provide commanders with:

(1) Intelligence that locates a target and indicates its vulnerability and relative importance. At the operational and tactical levels, intelligence will support the deliberate and dynamic targeting process for the full spectrum of lethal and non-lethal options to meet a commander's objectives.

(2) Intelligence that supports on-going tactical offensive and defensive operations should have an emphasis on the timely passage of intelligence for target development and indications and warnings of adversary actions. This includes advice on the selection of targets based on commander's priorities.

[34] Always guided by the intelligence requirements. See also Chapter 4.6

[35] AJP-2.1 contains detailed guidance on the contribution of intelligence to the operations planning process (OPP).

(3) Intelligence that supports those activities seeking to affect the will, behaviour or capabilities of an individual, group or organization. This includes a comprehensive and systemic understanding of the operating environment across the PMESII spectrum to support influence and counter-command activities.

(4) Situational awareness and analysis of acts of deception conducted by an adversary.[36]

e. **Intelligence contribution to counter-insurgency and other operations.** Intelligence staff can also provide vital support to counter-insurgency operations (i.e. insurgent networks and the threat to rear areas) and other specialized types of military activities (i.e., strategic communication, information activities). In addition, intelligence makes a significant contribution to cyberspace operations, civil-military cooperation (CIMIC)[37], stability policing activities[38] and countering improvised explosive devices (C-IED).

f. **Intelligence contribution to targeting.** Intelligence lays the foundation for joint effects, which includes targeting.[39] Processing conducted by the intelligence staff will provide commanders and targeting staff with details on how and where an adversary may be vulnerable or susceptible to influencing. Specifically, intelligence provides the target analysis[40], which is the basis of effective target development. Integral to target development is target validation. This process ensures the joint forces commander's (JFC's) objectives, guidance, intent and desired effects, compliance with relevant international law and rules of engagement and the accuracy and credibility of sources used to develop a target. Once potential targets are identified and validated, they are then nominated, through the proper channels for approval. Targets are prioritized based on the commander's objectives and guidance.

g. **Intelligence contribution to counter-proliferation.** Intelligence is a key enabler in preventing the illicit proliferation of ballistic missiles, weapons of mass destruction, related chemical, biological, radiological and nuclear (CBRN) threats and hazards, and other related commodities. This includes the provision of intelligence regarding proliferation networks and pathways (i.e., who, what, where, when, and how), their possible use and the timely exchange of threat information. This activity requires close cooperation between intelligence analysts and CBRN staffs utilizing CBRN reach-back to produce and disseminate intelligence assessments.[41]

h. **Intelligence contribution to operations assessment.** Intelligence can support an evaluation of progress, based on subjective and objective measurement to inform decision-making. In partnership with other staff branches, intelligence staffs at strategic and operational levels will be required to contribute to the operations assessments for the commander. The focus for the intelligence staff will be the impact of joint operations on an adversary. This entails methods such as measures of performance (MOPs), measures of effectiveness (MOEs), and battle damage assessment (BDA), resulting in an informed narrative assessment; for example, the success of an air campaign, etc.

---

[36] For definition of "deception" see lexicon.
[37] Intelligence procedures in support of C-IED operations are contained in AJP-3.15.
[38] See also AJP-3.22
[39] Details on joint targeting are contained in AJP-3.9.
[40] Target analysis incorporates target system analysis and target audience analysis.
[41] See AJP-3.8 Allied Joint Doctrine for Chemical, Biological, Radiological and Nuclear Defence.

(1) MOPs and MOEs are developed during the planning phase of an operation,[42] and measurements for later comparison are collected and recorded prior to commencement of operations. MOPs evaluate the accomplishment of actions and whether planned activities have been carried out successfully. MOEs evaluate how an adversarial system's behaviour or capabilities have been affected and help determine if we are doing the right things. Intelligence will be required to assist in their development as members of the operations planning group. During the execution phase, Intelligence will use relevant MOPs and MOEs to gather and report to the assessment working group (AWG).

(2) Battle damage assessment (BDA) consists of physical damage assessment, functional damage assessment and target systems assessment. It is the assessment of effects resulting from the application of military action, either lethal or non-lethal, against an adversary objective. Such assessment is primarily an intelligence staff responsibility, but links into the targeting process. The production of battle damage assessments will give rise to a series of post-attack intelligence requirements. Intelligence staff should establish effective procedures to support the BDA.

2.5 CATEGORIZATION OF INTELLIGENCE

Intelligence may be divided into the two following categories[43]:

Basic intelligence. Basic intelligence is intelligence, derived from any source, that may be used as reference material for planning and as a basis for processing subsequent information and intelligence. It is produced as part of routine monitoring or on a contingency basis, for example: Orders of Battle; equipment capabilities and performance; or profiles of personalities, infrastructure factors, socio-political descriptions, environmental aspects, etc. Basic intelligence, continuously reviewed and updated, is useful reference material on which to develop current intelligence. Basic intelligence provides the context and backdrop against which current intelligence is reviewed.

Current intelligence. Current intelligence reflects the current situation at either strategic, operational or tactical level. It should tell the decision-maker why it is relevant (the "so what" factor) and include a predictive assessment. It can offer greater granularity than basic intelligence, but is normally a time sensitive snapshot and is perishable. Intelligence reports and summaries provide current intelligence at any level, e.g. to the common operational picture (COP) and predictions for possible developments.[44]

---

[42] For more on MOPs, MOEs, and assessment, see AJP-5, the NATO operations assessment handbook, and the Comprehensive Operations Planning Directive (COPD).

[43] Products of both categories of intelligence are used in Strategic Anticipation (FRA to provide a defining sentence), horizon scanning (GBR to provide a defining sentence), Indication and Warning and for Planning/Execution of operations.

[44] Current intelligence may become or will contribute to different kinds of basic intelligence over time.

2.6 PRINCIPLES AND GUIDELINES OF INTELLIGENCE

Command-led. Setting the conditions for effective intelligence is a fundamental responsibility of command. Good intelligence flows from a command-led process that constantly defines what is important as well as what is urgent. Commanders should set priorities and direct the intelligence effort to meet operational requirements and to integrate intelligence with operations planning. Intelligence staffs are responsible for organizing the collection and the production of intelligence. Unless intelligence staffs thoroughly understand the commander's intent, they will be unlikely to satisfy their requirements.

Objectivity. Intelligence must be unbiased, undistorted, intellectually honest and free of prejudice. This requires commanders and staffs with open minds. Intelligence staffs should not distort their assessments to fit preconceived ideas or provide the answer that they think commanders want, or conform to fit existing plans. A methodical and determined exploitation of all available information and intelligence will help objectivity.

Perspective. The intelligence staff should also get inside the mind-set of the key actors, particularly adversaries and try to think like them. This given to commanders and staffs creates a better perception of separated action of adversaries to develop a better understanding of the operating environment.

Flexibility/agility. The intelligence staffs should establish an overall picture that provides timely, relevant, integrated and focused intelligence, suited to CCIRs and evolving security challenges. This requires a robust intelligence structure that can support intelligence driven operations. Look ahead, identify threats and opportunities, develop the flexibility to react to changing situations and be ready to exploit opportunities as they arise are relevant aspects. Agility is not about absolute speed: it is an ability to exploit information in context at the right tempo.

Timeliness. Intelligence should be delivered on time. Staffs provide intelligence on time, even if incomplete, to enable commanders to make decisions at a pace that maintains the initiative. This will often produce tensions between speed, high quality and comprehensiveness. However, even the best intelligence is rendered useless if it arrives after the event, so timeliness has a special importance. It is better to provide 80% of the intelligence on time rather than 100% of the intelligence too late. Similarly, commanders must accept that when less time is available for an assessment, the uncertainty associated with it will inevitably increase. This is inextricably tied to the risks that commanders might wish to take. Quality assessments take time to produce and commanders should always aim to provide intelligence staff with the earliest notification of an intelligence requirement. Time restrictions could influence the quality of an intelligence product, its level of uncertainty, and the way it is reported to commanders and other consumers.[45]

Fusion. Wherever possible and whenever possible intelligence consists of all relevant and available data, information, JISR results and other intelligence in order to provide a higher accuracy and a higher confidence level. An all source approach (in the perception of the usage of every available source/data/information) utilizes the concept of intelligence fusion to

[45] See AJP-2.1 on confidence levels

optimize the value of various sources of information (to use confirmation of independent sources of information to provide a higher confidence level). This approach blends the respective strengths of the various sources of information into a stronger and more robust product, that provides the most accurate and complete picture possible of what is known and assessed. While the level of detail in a single-source report could sometimes be sufficient to meet more immediate and narrowly defined requirements, all-source reporting is essential to gain in-depth understanding and avoid deception and misinformation. Intelligence should be comprehensive in nature and should explain the inter-related elements of a complex OE in an unbiased and undistorted manner. Additionally, it should examine situations broadly, from a wide variety of sources and in depth, getting beneath the surface of issues and examining inherent complexities. It should also consider the situation from the perspective of key actors, thus improving the predictive content of any assessment.

Accessibility. Relevant information and intelligence must be processed by intelligence staffs and be readily available to intelligence users. Intelligence is of no value if it is not disseminated or accessible to those who require it.

Sharing/collaboration. Intelligence has the capability to draw on the skills of a wide spectrum of experts and specialists in a variety of organizations, across all commands and at all levels of operations. Mechanisms are required whereby intelligence can be gathered and shared in a timely manner, within NATO and with non-NATO entities guided by the idea of responsibility to share in accordance with NATO´s existing security policy. The source of the information might be protected and the information itself might be sanitized to protect the source to share information with others.[46] NATO information exchange and classification procedures must encourage and enable concerted effort, collaboration and cooperation wherever possible. The general need-to-know principle[47] must be taken into account at all times; however, there is also a responsibility to share intelligence. This means exchange of data, information, JISR results and intelligence to the ones who may require the information. If applicable the product may have to be written at a different classification level to ensure that the information will be to those who need it; this is called “writing for release”, a key concept of coalition operations. There is the duty to share as well as to protect information.[48]

Security. Security must permeate the entire intelligence enterprise, but should balance the need to share with the need to protect people and plans. Information systems with which NATO shares intelligence must be designed, and remain, secure against all forms of intrusion and cyberspace attacks.

Responsiveness. Intelligence will be influenced by any new situation or information; therefore, the intelligence staff, supporting agencies and nations should be pro-active to meet the intelligence requirements at all times. Intelligence staffs should be able to quickly analyze, fuse, process and present products for military and non-military decision makers.

---

[46] Distribution of intelligence and information has to be performed taking into account the need-to-know principle at any time, without exception. Need-to-share must be consistent with appropriate security guidelines.

[47] See Chapter 6

[48] See AD70-01, Part3, Ch.2.:” NATO Information Management Policy establishes that information shall be managed with an emphasis on the ‘responsibility-to-share’ balanced by the security principle of ‘need-to-know’, and managed to facilitate access, optimize information sharing and re-use, and reduce duplication, all in accordance with security, legal and privacy obligations. Accordingly, NATO information should be clearly marked to facilitate information sharing as required.”

Interoperability. Common or interoperable processes, networks and systems are required to support intelligence direction, collection, processing and dissemination, and the management of the intelligence organization. NATO owned or controlled intelligence assets should be centrally coordinated to avoid duplication of effort, provide mutual support and ensure the efficient, economic use of all resources.

Anticipation. Intelligence is more than trend assessment; its true value resides in warning and forecasting to be relevant to decision making and operations. Although intelligence warning and forecasting are not exact, intelligence staffs should utilize the most recent data and information for all warning or forecast-related intelligence. Further, because information gaps routinely limit our ability to predict with complete accuracy, it is incumbent on intelligence planners, collectors, and analysts to effectively apply tradecraft methodologies and standards to optimize their ability to anticipate.

Guidelines: The challenges of complex areas of operation force intelligence staffs to adapt and operate in ways that match these challenges. To be successful intelligence staffs should apply the following guidelines:

a. A comprehensive view of the dynamics of situations is required. Intelligence assessments should include the physical, cognitive and virtual dimensions of the information environment (that exists within the operating environment) and should consider all actors and threats within the wider area of interest. A comprehensive understanding of the information environment requires a close relationship with information related capabilities (e.g. PsyOps, Mil PA) and functions (e.g. StratCom, Info Ops). This relationship enables an assessment of the information environment from different perspectives.

b. Levels of Intelligence. The levels of warfare should not be used to constrain the operation of intelligence. The boundaries between strategic, operational and tactical intelligence are increasingly blurred.

c. Threat/Adversaries. Adversaries are as likely to be low-contrast or low-resolution as they are to be clearly defined and categorised. Intelligence gathering requires precision and accuracy to generate the required contrast and resolution.

d. Commanders and their intelligence staff. The links between commanders and their intelligence staff must be strong and immediate. Commanders cannot afford merely to set their critical information requirements and then leave the intelligence staff to feed them independently. They personally must drive the meeting of those requirements.

e. Data and information sharing. Information should be passed horizontally as well as vertically within a command structure. Too often, a vertical command structure means that not all of the staffs have the necessary situational awareness. Staffs should be encouraged to pull the intelligence they require from networked systems and the intelligence staff should routinely push the intelligence to users.

2.7 LIMITATIONS OF INTELLIGENCE

Management of expectations. Even when exploited fully, intelligence will not produce complete certainty. Commanders and intelligence staffs should be realistic about what can be achieved through intelligence activities especially when resources are limited. Their expectations must be managed while doing all they can to optimize available resources.

Incomplete intelligence. Intelligence may not meet the commander's requirements exactly and may not be entirely accurate, complete, or easily corroborated. Rather intelligence estimates are mostly assessments with various levels of probability. Nevertheless, commanders will have to make judgements and decisions based on it. While there is the risk of misinterpretation or deception[49], exploiting information is critically important. Intelligence staffs must articulate where there are gaps in knowledge enabling commanders to place appropriate weight on the assessments.

Relevance/obsolescence. Current intelligence can time expire very quickly and this is a limitation of intelligence that needs to be recognised. Permanent validation and updating existing current intelligence as well as the production of new current intelligence will preserve relevance of information given to commanders and staffs. For basic intelligence a permanent updating with new incoming data and information is necessary as well; otherwise extensive and important basic products (i.e., human network analysis) will lose relevance rapidly.

Actors/adversaries capabilities and intentions. Historically, intelligence staffs have often determined an opponent's capabilities principally by the size, shape and quality of their military and the performance of their equipment. However, it has always been exceptionally difficult to determine an opponent's intentions. In the contemporary and future OEs, where the size of an opponent's military capability may be less relevant due to unconventional or hybrid tactics, intelligence staffs should ensure commanders understand that determining adversaries' capabilities, center of gravity, networks and intentions is no longer limited by purely physical strength, hence non-military skills and non-physical capabilities must also be considered.

Collection, processing and exploitation capabilities. All collection, processing and exploitation capabilities have limitations. Intelligence staff must provide commanders and all staff branches with a realistic appraisal of collection, processing and exploitation capability. This includes the limitations of each collection asset, its vulnerability to physical and electronic attack as well as deception, its coverage and the response time to meet requirements. Commanders need to understand that intelligence requirements are likely to exceed the availability of collection or exploitation capabilities and that there will be a need to prioritize their requirements to make the best use of available intelligence resources[50]. Additionally, commanders should be provided with the strengths and weaknesses of adversary collection capabilities.

Source protection. Source protection is critical, especially where covert collection capabilities are involved.[51] Therefore, source protection may require disguising the origin of the information or allocating a higher classification level than normal. The compromise of a source could result

[49] Deception is one of the biggest challenges in intelligence collection and processing. A well organized attempt of deception by an adversary or any other actor may be difficult to reveal.

[50] See also AJP-2.1 and AIntP-16

[51] For example source protection is a vital issue during signals intelligence (SIGINT), CI and human intelligence (HUMINT) activities.

in the information no longer being available, the source being used to pass deceptive information or the source being physically harmed or removed. Commanders must always consider intelligence gain/loss before risking to compromise an intelligence source, especially without compromising the operators in the field; e.g., HUMINT, (position, mission, identity).

Legal compliance. Intelligence, counter-intelligence and security activities must be conducted in accordance with the relevant applicable law. The applicable legal framework will depend on whether the activity takes place in peacetime including situations under the threshold of an armed conflict such as riots, internal disturbances or tensions or isolated and sporadic acts of violence or in an armed conflict (international or non-international). Accordingly, the domestic law of the respective nation(s) and international law (e.g. the Law of Armed Conflict (LOAC) or international human rights law, such as the European Convention on Human Rights (ECHR)) may be applicable. Many nations have specific laws governing the collation and use of open-source intelligence and the collection, use and storage of biometric data. All biometric collection, storage and use must be conducted in line with national and international law. The law of the host nation may also be applicable. The legal framework is likely to be complex, where breaches may result in severe sanctions, reputational damage, problems with disclosure, etc. and it is for these reasons that specialist and timely legal advice, for operators and commanders alike, must be obtained during the planning and conduct of intelligence operations. For example, the legal adviser (LEGAD) will be involved in the assessment of intelligence used for targeting, in the conduct of legal assessments (based on proportionality and necessity) and in the conduct of OSINT operations where specific laws govern its collation and use. The LEGAD(s) will advise on the applicable Human Rights law (both domestic and international) and, in addition, on issues associated with laws related to privacy, copyright, intellectual property, private and state property, cyberspace, data sharing, etc. which could all generate legal issues. To ensure strict compliance with the law, it is important that the intelligence staffs, especially J2 and J2X, and commanders develop a close working relationship with LEGAD(s).

Chapter 3 INTELLIGENCE COLLECTION DISCIPLINES AND PRODUCTS

3.1 INTELLIGENCE COLLECTION DISCIPLINES

In some cases intelligence is based on a single source. However, there are significant advantages to be derived from the use of all-source intelligence. All-source intelligence is the deliberate application of two or more intelligence collection disciplines (e.g. human Intelligence and signals Intelligence) or other JISR capabilities seeking for confirmation to improve the quality of the intelligence product. Devoting time and effort to corroboration during intelligence collection activities increases the confidence level and reduces risk. Corroboration is achieved by comparing intelligence derived from one intelligence collection discipline with that derived from at least one other intelligence collection discipline so that common features or contradictions can be identified. The nature of difficult and complex environments means the fusion of all available data, information and JISR results will be the only way that the commander can be provided with sufficient understanding to make decisions. Single-source information and single discipline results may answer separated and limited requirements (often without any confirmation) but cannot replace all-source-intelligence to satisfy the IR.

Intelligence collection disciplines are the means or systems used to observe, sense, and record or convey information of conditions, situations, threats, opportunities and events. The intelligence collection disciplines are[52]:

a. **Acoustic intelligence**[53]. Acoustic intelligence (ACINT) is intelligence derived from signals or emissions. This is intelligence derived from sound. Examples of ACINT sensors are hydrophones, geophones, sonars, integrated underwater surveillance systems and artillery sound ranging systems. Due to the nature of the origin of sound, ACINT is primarily concerned with the identification of the objects signaling or emitting and their movement and the intelligence that can be derived from its detection.

b. **Human intelligence.** Human intelligence (HUMINT) is Intelligence derived from information collected by human operators and primarily provided by human sources. It includes the systematic and controlled exploitation, by interaction with or surveillance of, human sources, objects, or individuals. It has the unique ability to provide information regarding an actor's intentions, morale, and relationships among individuals and organizations. HUMINT activities involve collection, reporting and analysis integrated with all-source-intelligence to provide decision makers with timely and accurate information necessary for conducting successful military operations.

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

[52] See Annex A for a more detailed description of each.
[53] Some nations consider ACINT to be part of MASINT.

d. **Measurement and signature intelligence.** Measurement and signature intelligence (MASINT) is intelligence derived from the scientific and technical analysis of data obtained from sensing instruments or exploitation process for the purpose of identifying any distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification. MASINT is derived from the collection and comparison of a wide range of emissions and evidence with a database of known scientific and technical data in order to identify the equipment or source.

e. **Open-source intelligence.** Open-source intelligence (OSINT) is intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access. OSINT is collected from sources such as radio, television, newspapers, state propaganda, journals and technical papers, the Internet, social media, technical manuals and books, and other media. The intelligence community has always used open sources as an element of situational awareness and in the production of intelligence. OSINT is likely to remain a significant source of basic intelligence.

f. **Signals intelligence.** Signals intelligence (SIGINT) is intelligence derived from the collection and exploitation of foreign electromagnetic signals or emissions. It is the generic term used to describe communications intelligence (COMINT) and electronic intelligence (ELINT) when there is no requirement to differentiate between these two types of intelligence, or to represent their fusion. COMINT and ELINT are respectively described as:

(1) **COMINT** is intelligence derived from electromagnetic communications and communications systems by other than intended recipients or users. COMINT is 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 downlinks.

(2) **ELINT** is intelligence derived from electromagnetic, non-communication transmissions. ELINT 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. By comparing information about the parameters of the emission that has been intercepted with equipment signatures held in databases, valuable intelligence can be derived about the equipment and its operator.

3.2 SPECIALIZED INTELLIGENCE PRODUCTS

The intelligence collection disciplines contribute to products that are not mutually exclusive; aspects of one may also be considered as part of another. Specialized intelligence products include, but are not limited to:

a. **Armed forces intelligence**. Armed forces intelligence concerns all aspects of foreign space, land, maritime and air forces including Order of Battle, command and control, weapons systems, training, personnel, doctrine, strategy and tactics, engineering, logistics, arms trade, defence industry and defence spending.

b. **Chemical, biological, radiological and nuclear (CBRN) – related Intelligence.** Intelligence regarding the capabilities, locations, movement, means of delivery, infrastructure, and key persons, use or other types of illicit commodities of proliferation concern of chemical, biological, radiological or nuclear material or weapons of mass destruction is known as CBRN-related Intelligence.

c. **Biometrics-enabled Intelligence**. Biometrics-enabled intelligence (BEI) is the intelligence resulting from the capture, processing, analysis, interpretation and dissemination of biometric data, the contextual information associated with that data, and other associated information and intelligence.[54]

d. **Identity Intelligence.** The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest (biographic, biometric and contextual characteristics).

e. **Document and media exploitation (DOMEX).** The processing, translation, exploitation, and dissemination of collected hardcopy documents and electronic media that are under NATO physical control and not publicly available.

f. **Human network analysis (HNA).** HNA is an all-source intelligence analytic methodology that provides basic intelligence, which is providing detailed information on networks, relationships, and intentions.[55] These networks can be complex, multi-tiered, and transnational; they try to create physical and psychological effects through the use of both physical and cyber capabilities. They are not generally organized in a manner of conventional armed forces. The capability to understand these physical and virtual networks and to influence key individuals and groups, their network connections and specific roles is crucial to achieve NATO objectives and to protect Alliance interest, forces and security.

g. **Geospatial intelligence (GEOINT).** Geospatial intelligence is intelligence derived from the combination of layered geospatial information with other intelligence data, products and layers. The layered geospatial information is quality assured. The geospatial and imagery communities provide quality assured information that may be combined with other intelligence and analyzed to produce geo-referenced intelligence products and datasets for compliance with a requirement.

[54] See AIntP-15
[55] See AIntP-13

h. **Medical intelligence (MEDINT).** Medical intelligence is derived from the processing of medical, bio-scientific, epidemiological, environmental and other information related to human or animal health.[56] This intelligence, being of a specific technical nature, requires informed medical expertise throughout its direction and processing within the intelligence cycle. In the operating environment, MEDINT can also be used as a collection discipline to obtain and analyze information relating to disease, biological warfare threats or health concerns. Knowledge of the health impact of adversary capabilities and weapon systems is valuable when planning medical support.

i. **Scientific and technical intelligence (STI).** Scientific and technical intelligence concerns foreign developments in basic and applied scientific and technical research and development including engineering and production techniques, new technology as well as improvised products, and weapons systems and their capabilities. Technical intelligence (TECHINT) is intelligence concerning foreign technological developments, and the performance and operational capabilities of foreign and adversary materiel, which have or may eventually have a practical application for military purposes. There are intelligence products derived from the scientific examination and testing of materiel including computer hardware and operating system software. Testing is centered primarily on determining the capabilities and limitations of adversary equipment and in support of the development of countermeasures to that equipment.

j. **Security intelligence (SI).** Security intelligence is intelligence on the identity, capabilities and intentions of adversary organizations or individuals who are or may be engaged in terrorism, espionage, subversion, sabotage and organized crime. These organizations or individuals pose, or may pose a threat in peace, emergency or conflict, to the security of the resources, activities, operations, personnel and information of NATO nations and forces. It includes intelligence on foreign intelligence systems and organized crime and is especially related to CI activity. CI 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-informed decisions on security measures[57].

k. **Target intelligence.** Target intelligence is intelligence produced for the targeting process. It portrays and locates the components of target or target complex and indicates its vulnerability and relative importance.

[56] See also Details of Medical Intelligence in Allied Joint Medical Publication (AJMedP)-3.
[57] See chapter 6 and AJP-2.2

Chapter 4 THE INTELLIGENCE CYCLE, IRM&CM AND THE JISR PROCESS

4.1 INTRODUCTION

The intelligence cycle[58] is the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available for users. These activities are focused through the four intelligence core phases of direction, collection, processing and dissemination shown in Figure 3. While the intelligence cycle outwardly appears to be a simple process, in reality it is a complex set of activities comprised of many different processes and management functions operating at different levels and speeds. Some tasks overlap and coincide so that they are often conducted concurrently, rather than sequentially. For example the intelligence requirements management and collection management (IRM&CM)-function and the JISR process.[59]

The intelligence cycle consists of 4 phases:

a. **Direction**. Direction is described as the determination of intelligence requirements, planning the collection efforts, issuing of orders and requests to collection agencies, and maintenance of a continuous check on the productivity of such agencies. Direction is the key to the intelligence process.

b. **Collection.** Collection is described as 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. JISR assets conduct the bulk of all collection activities, but non-dedicated JISR assets can also contribute.[60] Collection activity requires close collaboration with both intelligence and command staff to optimize the use of collection assets.

c. **Processing.** Processing is described as the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation. Processing is iterative and may generate further requirements for collection before dissemination of the intelligence.

d. **Dissemination.** Dissemination is described as the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. It also requires security, conformity to the customer's requirement and a mechanism for feedback.

---

[58] The intelligence process is also called the intelligence cycle, because of the cyclic model shown in figure 4. Some nations use different national intelligence processes in accordance with their national doctrines.

[59] The JISR process consists of five steps: Task, collect, process, exploit disseminate (TCPED). Sometimes the last three steps process, exploit disseminate (PED) are focused combined as a major part in after collection step. See Chapter 4.6 on IRM&CM, Chapter 4.7 on JISR and Chapter 2.8.6 on information theory. For further description see AJP-2.1, AJP-2.7, AIntP-16 and AIntP-14.

[60] See 4.3.c.(6)

As depicted in the diagram below, the effective monitoring of the intelligence cycle and the coordination of the four core phases is undertaken through the IRM&CM process.

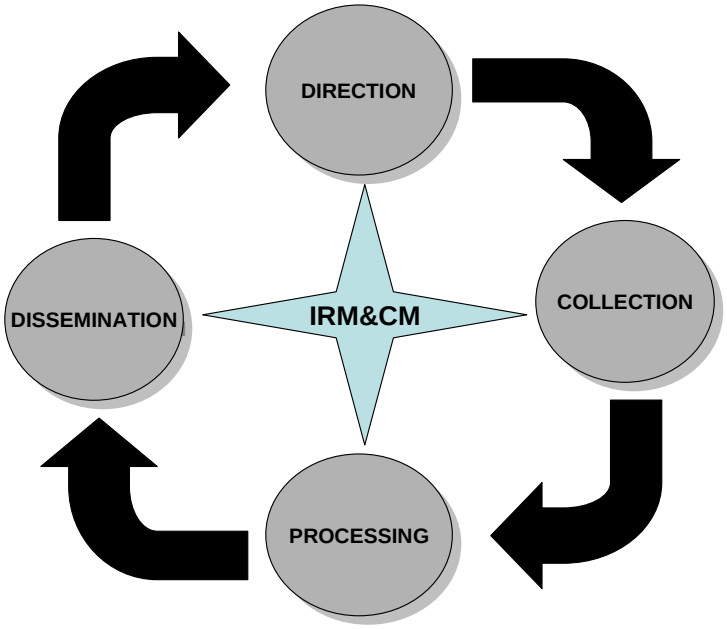

Figure 3. The intelligence cycle

4.2 DIRECTION

Direction is the first phase of the intelligence cycle during which the commander's intelligence requirements are identified and prioritized. Commanders should prioritize their intelligence requirements and direct their intelligence staff by giving clear instructions concerning the intelligence needed and the time limits on its provision.[61] External direction comes from commanders at each level and sets the parameters for intelligence requirements and objectives. Internal direction comes from the senior intelligence officer to each specialist element of the intelligence staff. This direction should be specific and, wherever feasible, should highlight those factors that are critical to the planning process. Therefore a continuous dialogue should be established between commanders and their senior intelligence officer to come to a rigorous direction for the intelligence cycle.

In accordance with the commander's direction the intelligence staff, in conjunction with the operations and planning staff, must direct the collection process to meet the commander's requirements. This involves:

a. Deciding what information and intelligence is required and how the commander's intelligence requirements can be met.

[61] Details of intelligence requirements management are contained in Chapter 4.6.

b. Tasking JISR capabilities, JISR assets and agencies and, where appropriate, coordinating their activities, to collect the necessary information.

c. Monitoring intelligence activity to ensure that the right information is being collected, analyzed and disseminated.

d. Ensuring that intelligence activities are conducted in a timely manner and where delays are occurring re-tasking or reprioritizing as required.

e. Planning the production inside intelligence cycle in combination with IRM&CM and the influence on all phases of the intelligence cycle.

4.3 COLLECTION

Collection is the second phase of the intelligence cycle during which information is obtained to meet the commander's intelligence requirements. During the collection phase, the appropriate JISR capabilities, assets and agencies are tasked[62] to collect and exploit information. Those JISR capabilities, assets and agencies with an exploitation capability may respond with single-source or single-discipline-intelligence or information.

There are two parts to the collection process. Primarily, intelligence staff will use JISR capabilities, assets and collection agencies to obtain the information required. Secondly, they will ensure the timely delivery of the JISR results into the processing step in the intelligence cycle. It is important that intelligence staff make sure that commanders and their staffs understand the capabilities, limitations, vulnerabilities and response times of JISR capabilities, assets and agencies likely to be available to them, along with their susceptibility to deception.

There are several types of collection capabilities[63]:

a. **Datamining own intelligence staff database.** Datamining own force databases is done to use all available data, information, JISR result and intelligence to satisfy an IR.

b. **Request for Information (RFI).** RFIs are issued to higher and adjacent commands to obtain data, information, JISR results and intelligence without tasking own JISR capabilities directly.

c. **Intelligence collection disciplines**.[64] Intelligence collection capabilities and assets have the ability to collect and exploit data and information within their intelligence collection discipline. For example the collection and exploitation of HUMINT collected by human intelligence units or SIGINT collected and exploited by signals intelligence units.

d. **Surveillance.** Surveillance is the systematic observation of aerospace, surface or subsurface areas, places, persons or things, by visual, aural, electronic, photographic or other means. Surveillance is conducted against known and potential adversaries and threats as well as in support of operations in current and potential future crisis areas. It can be passive or active, covert or overt. It can be coarse grained to provide early warning of

[62] In line with the direction phase and managed by the IRM&CM function.
[63] See AJP-2.7, AIntP-14 and AIntP-16
[64] See also Chapter 3.1 and Annex A: Intelligence Collection disciplines

activity over a wide area, or fine grained to cover a particular location or facility. Surveillance over extended periods enables patterns of life and habits to be identified, which leads to deeper understanding of other potentially threatening activities or behaviour.

e. **Reconnaissance.** Reconnaissance is a mission undertaken to obtain information, by visual observation or other detection methods, about the activities and resources of an adversary or potential adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. It is a focused method of collecting information about specific locations, facilities or people. Reconnaissance tasks are not confined to specific reconnaissance units, but may be undertaken by other force elements in the course of their duties.

f. **Non-dedicated JISR capabilities.** Non-dedicated JISR capabilities and assets are capabilities not assigned to a specific JISR tasks, but can contribute to the intelligence cycle as part of their routine operations (e.g., the use of a patrol to obtain information during their routine activities).[65]

g. **Other.** All other possible inputs are collected as well – even when the originator cannot be tasked to deliver and is not part of the RFI process (This applies i.e. for non-governmental organizations (NGOs), etc.) or the information is obtained unintentionally. Inside the collection phase all available data and information is used to improve the respective intelligence products. In no case will available relevant information intentionally not be used by the intelligence staff.

All of these capabilities will disseminate data, information or JISR results back to the analysts within the intelligence staff to proceed with the processing phase.

4.4 PROCESSING

Processing[66] 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. Processing is a multi-faceted phase of the intelligence cycle consisting of collation, evaluation, analysis, integration and interpretation in order to produce intelligence. Throughout the steps of processing the traceability of the used data, information and JISR results and the retrievability of the product has to be assured. During the processing phase the production of intelligence takes place. All the relevant results of the analytical process are continuously structured and integrated into the intelligence products.

---

[65] Sources of collected materiel and information can include tactical activities and can also include collection by technical and electronic means. Technical exploitation is a methodological, integrated and collaborative set of capabilities used to derive data and information from collected materiel to satisfy a commander's information requirements. Technical exploitation begins with the collection of information and materiel and through applied forensics and scientific analysis, using state-of-the art capabilities, provides empirical and quantifiable data. Deployable technical exploitation capabilities are typically scalable and can make extensive use of reach-back biometric, forensic, and DOMEX capabilities, and other technical exploitation capabilities as required. Technical exploitation results can then be further processed, analyzed, and fused with all-source intelligence products within the intelligence cycle. See also AJP-2.7, AIntP-14 and AIntP-10

[66] See AIntP-18

4.4.1 Collation

Collation is the first step in the processing phase in which the grouping together of related items of data, information, JISR results or intelligence provides a record of events, which facilitates further processing. In general this first step is sorting out irrelevant from relevant data, information, JISR results and intelligence to answer specified intelligence requirements. In practice, it is comprised of the procedures for receiving, grouping and recording all reports, and involves:

a. Registering the receipt of each incoming piece of data, information, JISR results and intelligence.

b. Placing each piece of data, information, JISR results or intelligence into an appropriate category or group through logging, marking on a map or chart, filing, or entry into an electronic database.

Collation may involve no more than the maintenance of a paper log and a marked map or chart, but is increasingly likely to be automated, involving databases linked to graphical interfaces and automatic data transmission between headquarters. The categories or groups into which data, information, JISR results and intelligence will be placed during collation must be related to the commander's intelligence requirements and their area of responsibility.

4.4.2 Evaluation

The evaluation step follows identification of the relevant data, information, JISR results and intelligence for answering an intelligence requirement within the collation step. 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 source or originator and the credibility of the information. A judgement must be made on the reliability of the source or the originator and the credibility of the information. There are many reasons, including deception and subjectivity, why information may not be reliable or credible.

Evaluation allocates an alphanumeric rating to each piece of information or intelligence indicating the degree of assurance, which may be placed upon it.[67] This rating is based partly on the subjective judgement of the evaluator, on the experience of other information produced by the same source and, in the case of information produced by a sensor, on knowledge of the accuracy of the particular sensor system.

Reliability and credibility should be considered independently of each other to ensure that the rating allocated to the reliability of the source does not influence the rating given to the credibility of the information, or vice versa. For example, not every piece of information produced by a normally impeccable source is correct; neither does information, which is demonstrably true, indicate that its source is completely reliable. Figure 4 provides an example of the values used for allocating ratings for the reliability of the source and the credibility of the information.

[67] The use of digraphs to evaluate information is not always necessary for strategic and operational intelligence due to the source of the intelligence. However, when digraphs are not formally used analysts should continue the mental process of evaluation.

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

Figure 4. Evaluation and Rating

Ratings are produced by combining the values; a piece of information from a source known to be usually reliable and judged probably true would be rated B2. A factor analysts should also consider, which affects their assessment of both reliability and credibility, is the source's access to the information involved.[68] This method of evaluation provides an indication over time of the capabilities of various sources and agencies and aids the selection of those best suited for particular tasks.

4.4.3 Analysis

Analysis, the third step in the processing phase, is when information is reviewed in order to identify significant facts for subsequent interpretation. Analysis breaks a complex problem into parts that are easier to assess and uses different techniques to analyze different coherences. The different groups of already collated and evaluated data, information, JISR results and intelligence are scanned for significant facts to answer single parts of a specific intelligence requirement. In practice, integration follows on from analysis without a break and the two steps have to be seen in coherence and not strictly separated.[69]

4.4.4 Integration

During analysis, collated and evaluated information is scanned for significant facts. During the integration step, analyzed data, information, JISR results and intelligence on specific topics from diverse sensors, capabilities and all available sources are fused[70]. Integration will then be the fourth step in the processing phase whereby the analyzed parts of the underlying information and/or intelligence is selected and combined into a pattern in the course of the production of further intelligence. In this step the significant facts that are found are compared to other known facts, and deductions are drawn. Integration is the drawing together of the deductions, and the determining of a pattern of intelligence, such as a sequence of events or

[68] For example, details of the capability of a weapons system provided by a technician would carry more weight than information provided by a casual observer outside the production facility.

[69] Huge steps have been made in NATO, national militaries and within private industry into the digital automation of analysis and integration and to develop software tools to enhance intelligence analysis.

[70] See Chapter 2.6. Fusion as one of the principles of intelligence

the profile of an individual. This aspect of integration, as with evaluation and analysis, is almost totally based on human judgement, informed by subject-matter expertise, and is a critical point in the intelligence cycle. Despite advances in technology, there is currently no substitute for the experience and judgement of the analysts inside the intelligence staff.

4.4.5 Interpretation

Interpretation is the final step in the processing phase where the significance of information or intelligence is judged in relation to the current body of knowledge. Interpretation is an objective mental process of comparison and deduction based on common sense, life experience, and military knowledge, covering both opponent and friendly forces, and existing information and intelligence. New data, information, JISR results or intelligence is compared with, or added to, that which is already known, giving rise to new or updated intelligence. At the end, these activities result in all-source-intelligence products. This mental process can be broken down into a sequence of four principal elements, which should address to each piece of information or intelligence being considered:

a. **Identification**. This is not merely matching an identity to an actor, or a name to a piece of equipment; it is the consideration of 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 actor or entity being reported on. This understanding will provide insight into the likelihood of the intelligence and why such actions or events may have occurred.

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

c. **Significance.** The analyst must be sure that the piece of information has been fully exploited. Each deduction should be challenged, taking into account the original intelligence requirements, so the final product is relevant and useable.

d. **Deception.** Deception consists of those measures designed to mislead the adversary by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. Intelligence staffs are a primary target for adversary deception and the analyst should always be cautious of the information in front of him. In short, the analyst should seek confirmation[71] of even the most credible information.

Continuous review. Once information has been processed, the resultant deductions and conclusions must be inserted into the intelligence picture. However, the resultant intelligence will seldom be conclusive and further information and intelligence should be acquired to confirm or refute it. The need to meet these new requirements dictates the cyclical character of the intelligence cycle and the continuous nature of the intelligence collection plan and shows the main characteristic of the entire intelligence cycle.

[71] Information can be confirmed by several sources, but that doesn't mean that it is undoubtedly true. There always remains a degree of uncertainty. On the other hand, falsification of information provides far more certainty. That is one of the reasons why intelligence is never conclusive and continuous review a logical necessity.

It is the analysts' responsibility to maintain and to integrate used/available meta-data, data, information, JISR results, etc. of their product to ensure traceability along the whole processing chain.

Generally the product includes a final assessment to satisfy the IR (to "answer the question") reflecting the commanders needs and anticipating follow-on questions of commanders. Predictive assessments satisfying the commanders' needs are the key output of the processing phase of the intelligence cycle.

4.5 DISSEMINATION

The fourth phase of the intelligence cycle is dissemination. 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 collection agencies, resulting in *circular reporting*. Advances in technology are also affect dissemination. 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 real-time or near real-time basis, vastly increasing their responsiveness[72]. It is possible and advisable to produce different versions of the same product (i.e. different classification after adjustment of content or different version with/without displayed references and sources).

Dissemination Formats. Intelligence should be provided in a form that the recipient readily understands and is directly usable. This should be in a timely manner without overloading the user and minimizing the load on communications capabilities. Dissemination consists of both 'push' and 'pull' control principles. The 'push' concept allows the intelligence staff to push information to satisfy intelligence requirements to other staff elements or other headquarters. 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. This includes operational support pages, which link related intelligence products and operational information together on a single web page. Intelligence sharing and dissemination is further enhanced by modern communications systems equipped with an electronic publishing capability. The format selected should be appropriate to the requirement and the recipient.

NATO Reporting Formats.[73] NATO uses standard report formats and message sets to guarantee multinational interoperability.[74] Wherever possible, written and web-based intelligence reports should follow NATO formats. Examples of these formats include:

a. **Intelligence Reports (INTREPs)**.[75] An INTREP may be originated at any level of command and is a report that is sent without regard to a specific time schedule, whenever the information it contains is considered likely to require the urgent attention of the receiving

[72] Disadvantage: Too much speed in the process from collection to dissemination involves the risk that little or no processing or exploitation/analysis has occurred.

[73] See also Bi-SC reporting directive 80-3

[74] Further details on NATO intelligence report formats are contained in NATO standardization agreement (STANAG) 7149/APP-11.

[75] The short title, INTREP, is always used in reports.

commanders or their staff. The INTREP should include any relevant deductions made in the time available. Threat warnings are one of the most important types of intelligence report. The distribution of an INTREP will conform to explicit instructions laid down at each level of command. These will normally limit distribution to the next higher, lower and adjacent command echelons, but depending on content, a wider distribution will sometimes be necessary. The format of an INTREP must comply with agreed NATO reporting procedures.

b. **Intelligence Summaries (INTSUMs)**.[76] An INTSUM may be originated at any level of command and is a concise periodic summary of intelligence on the current situation within a commander's area of intelligence responsibility designed to update the current intelligence picture and highlight important developments during the reporting period. It should therefore include any information that may be relevant to the intelligence requirements of any commander to whose headquarters it is disseminated, and should contain an appraisal based on evaluation and interpretation of that information. At the higher echelons, emphasis should be placed on appraisal and not on detail. The INTSUM is disseminated to higher, lower and flanking command echelons at the discretion of the originating commander or according to directions received from higher headquarters. Its distribution should include all those whose responsibilities and interests may be affected by the contents. The INTSUM formats must comply with agreed NATO reporting procedures.

c. **Supplementary Intelligence Reports (SUPINTREPs)**. A SUPINTREP is designed to provide detailed reviews and analyses of all the intelligence data on one or more specific subjects that have been collected over a given period. They may be produced periodically, on special request, or in preparation for particular operations. The content of each SUPINTREP will determine its distribution. There is no set format for these reports, but the word *SUPINTREP* must appear at the beginning of the report.

d. **Counter-Intelligence Reports**. Counter-intelligence (CI) reports are similar to other report formats. They are divided into counter-intelligence reports (CI-INTREPs), counter-intelligence summaries (CI-INTSUMs) and counter-intelligence supplementary reports (CI-SUPINTREPs). Counter-intelligence staffs may also produce threat assessments and threat warnings, by which commanders are informed of specific security threats.

e. **Thematic Reports**. Thematic reports address particular aspects of the OE, such as a region or town, a political or religious movement or a particular adversary organization, sometimes covering longer time-scales.

[76] The short title, INTSUM, is always used in reports.

4.6 INTELLIGENCE REQUIREMENTS MANAGEMENT AND COLLECTION MANAGEMENT

Conducted at all levels in NATO, intelligence requirements management and collection management (IRM&CM)[77] is a set of integrated management processes and services to satisfy the intelligence requirements by making best use of the available collection, PED[78] and intelligence processing capabilities and therefore pictured at the center of the intelligence cycle. It ensures IRs are answered and the collection, PED and processing capabilities available are focused and prioritized. A common understanding of the IRM&CM function allows higher and lower headquarters within NATO and nations to share intelligence information and to make best use of collection and exploitation capabilities.

Specific personnel from within the intelligence staff conduct IRM&CM. These personnel work closely with the commander's operations, intelligence and planning staff to satisfy intelligence requirements. They provide a vital link between commanders and the large number of agencies and collection capabilities and assets which are available to contribute to building relevant intelligence as a basis to make decisions.

IRM&CM must be able to coordinate the intelligence capabilities to support any particular operation at the operational and tactical levels, have the ability to influence and access national and strategic level information, and forge links to relevant sources outside of the command chain. The IRM&CM process[79] also requires visibility of activity within all flanking and lower commands.

4.6.1 Intelligence requirements management (IRM)

IRM describes a set of integrated management processes and services that summarize, prioritize and validate incoming intelligence requirements; initiate the collection of associated information; quality control processed outputs and oversee dissemination of intelligence products. This management process is led by the intelligence staff or agency. In any operation or planning situation, commanders will determine the type of information required to allow them to plan and conduct their mission in the most effective manner. These information requirements can generally be divided into two groups:

a. Requirements that contribute to the success of the mission.

b. Requirements that identify and quantify the threat to the mission.

These requirements 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.

It is the role of the IRM&CM functions to help validate and refine the intelligence requirements, to determine how they can best be satisfied, and then to coordinate activities associated with meeting the requirement. IRM is central to the management of this process and is supported

[77] See also AJP-2.1 and AIntP-16

[78] Process, exploit, disseminate (PED). The last three steps out of the JISR process.

[79] IRM&CM process is further described in AJP-2.1 and AIntP-16.

by collection management (CM), which is the function to convert intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection and exploitation capabilities, monitoring results and retasking, as required.

Intelligence requirements (IRs). Commander's critical information requirements (CCIRs) cover information concerning areas that are either critical to the success of the mission or represent a critical threat. CCIR cover all aspects of the commander's concern including friendly forces information requirement (FFIRs), essential elements of friendly information[80] (EEFI)[81] and the priority intelligence requirements (PIRs). The two key elements of CCIRs are priority intelligence requirements (PIRs) and friendly force information requirements (FFIRs). PIRs are derived from the CCIRs and their identification and drafting initiates and drives the intelligence process. Intelligence requirements should cover the broad scope of information on the PMESII spectrum and include the following types:

a. **Priority intelligence requirements (PIRs).** Commander's PIRs are a vital part of the CCIRs and are normally formulated by the intelligence staffs in close cooperation with commanders. The PIRs encompass those intelligence requirements for which commanders have an anticipated and stated priority in their tasking of planning and decision-making and normally involve identification and monitoring of areas that represent opportunities and threats to the mission plan. They are a standing set of requirements that drive the collection and production effort, and provide the focus of the overall intelligence mission. They should be limited in number and provide comprehensive and coherent groupings of key issues and should be linked to commander's decision points. They may be enduring or limited to a particular phase or situation.

PIRs should be coordinated and consistent with upper and complementary to lower commands' PIRs. They should be written in such a way as to support a decision commanders must make, such as what forces to employ or when.

By formulating a collection strategy (an overarching concept for intelligence and information gathering) the intelligence staff can both determine how PIRs are most effectively satisfied using all possible sources and assets available, and how intelligence gaps may be addressed.[82]

b. **Specific intelligence requirements (SIRs).** SIRs support and complement each PIR and provide a more detailed description of the requirement. SIRs are used by the intelligence staff to determine what intelligence asset, source or discipline can best satisfy the requirement, and to identify the coordination required to ensure that the appropriate assets are deployed. The SIRs allow collection and analysis agencies to develop their response or collection toward that best suited to the stated requirement. SIRs are divided in the same manner as PIRs. Some collection requirements may be submitted by other organizations to the intelligence staff.

c. **Essential elements of information (EEI).** SIRs are broken down into more detailed questions known as EEI. The EEI add the details to the SIRs and allow the production of

[80] Some nations no longer recognize EEFI as a component of CCIR in their doctrine.
[81] FFIR and EEFI are not in the responsibility of intelligence staffs.
[82] The Joint Intelligence Estimate is considered in Chapter 5.

a collection task list based on an intelligence collection plan (ICP[83]). EEI could be related to several SIRs and should provide enough guidance to allow analysts to give a complete and satisfactory answer to each requirement. EEI are the basis for creating collection requirements and establishing relevant tasking and coordination with organic sources, sources or relevant agencies.

Intelligence requirements management (IRM). All intelligence requirements should contain details of the nature of the information required, its desired priority and other governing factors. It is the IRM element's responsibility to determine if the request is valid. The IRM element will consider:

a. If the information is already held and therefore provided immediately.

b. If the information is available from an external source.

c. If it requires collection.

The methods pursued to answer these questions form the basis of the ICP.

Requests for information (RFIs). The term RFI is used to describe a requirement for information that is passed to the intelligence requirements manager at higher, lower or adjacent levels. A RFI is used when commanders do not have sufficient allocated collection capabilities or the intelligence staff is unable to answer a question through research or other means, and thus commanders require information from a superior, adjacent or subordinate command. The receiving organization will treat the incoming RFI as an intelligence requirement, the only difference being that the intelligence requirement is undertaken on behalf of another organization. A single intelligence requirement may generate a number of separate RFIs for different providers or other intelligence resources such as national JISR capabilities, agencies or adjacent headquarters.

Intelligence indicators. Before beginning the collection process the intelligence staff should identify the indicators appropriate to the particular operation or threat. Indicators are items of information that reflect the intention or capability of a potential adversary to adopt or reject a course of action. Indicators are normally categorised under four headings:

a. **Horizon scanning**. Horizon scanning is the systematic search across the global environment for potential threats, hazards and opportunities. Horizon scanning may also provide an innate audit function to identify weaknesses in current assessments or policies, but it is not amenable to specific tasking requirements.

b. **Alert or warning indicators**. These relate to preparations by an adversary for offensive action. At the strategic level, this could include the collapse of negotiations or issue of ultimatums while at the operational level it could include the re-supply or re-deployment of adversary capabilities.

c. **Tactical or combat indicators**. These indicators reveal the type of operation the adversary is about to conduct. Indicators linked to these preparations can potentially be defined well in advance and should be reflected in the PIRs. For example, tactical indicators

[83] In other documents the abbreviation ICPP for intelligence collection and processing plan may be found in similar usage. See AIntP-16.

could include the increasing number of naval ships in port or the purchase of particular types of weaponry by insurgents.

d. **Identification indicators**. Identification indicators are those that enable the identity and role of a formation, unit, installation or irregular adversary grouping to be determined from its order of battle, equipment and tactics.

Selection of indicators appropriate to the operational situation is the responsibility of the intelligence staff. The nature of the indicators that they select depends upon the intelligence collection plan[84].

4.6.2 Collection management

Collection management (CM) describes the process of converting intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection capabilities or agencies; and monitoring results and re-tasking, as required by making best use of the collection capabilities. CM also encompasses activities related to the execution and coordination of the JISR process. CM is implemented by the theatre collection manager who exercises collection management authority for a given mission and area of intelligence responsibility and who directs collection requirements management and collection operation management functions to synchronize JISR task, collect, process, exploit, disseminate (TCPED) activities among NATO commands and organizations and participating nations and partners.

The intelligence collection plan (ICP). The ICP is used to identify, plan and oversee the intelligence requirements for a given commander and for a specific phase of an operation, and breaks down in detail how each intelligence requirement is to be satisfied. Additionally it shows timelines to which products have to be finalized and disseminated. Normally in matrix or table form, the ICP indicates the preferred method for satisfying intelligence requirements. The ICP indicates the general level of detail required and should list the organizations, agencies, capabilities or assets best suited to the task. The ICP is a planning tool for collection managers at each level of command and includes the RFIs as well as the requirements for collection based on the collection requirements list (CRL). The overall collection effort is managed through the implementation and control of the ICP alongside the collection task list (CTL) and the collection exploitation plan (CXP). For the analysts the ICP is used to overview the incoming data, information and JISR results and connect this with the processing to deliver intelligence on time.

[84] See AIntP-16

4.7 JOINT INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE[85]

Joint intelligence, surveillance and reconnaissance[86] (JISR). JISR describes 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. JISR aims to satisfy information gaps identified by NATO commanders and staffs via the execution of the JISR process which synchronises collection and exploitation activities[87] making the best use of available JISR resources and, timely disseminates the resulting information to the requester. JISR essentially supports two main functions: contribute to Intelligence production and provide up to near real time support to operations and decision making. Hence, the JISR process supports intelligence cycle, mainly occurs within the collection step of the intelligence cycle, and contributes to the processing step of the intelligence cycle. However, it is also a tool in the hands of NATO Commanders for the direct and time-sensitive provision of information for the preparation, execution and assessment of operations and manoeuvres. The JISR process and related TCPED steps are further described in AJP-2.7 and AIntP-14. The relationship between the intelligence cycle and the JISR process is displayed in Figure 5. Annex B on information theory gives an additional overview to the used terms and their application.

Joint intelligence surveillance and reconnaissance (JISR) architecture. NATO's JISR Architecture consists of the organizations, processes and systems connecting collectors, databases, applications, producers and consumers of intelligence and operational data in a joint environment. This architecture facilitates the management of intelligence, enables joint intelligence, surveillance, and reconnaissance including the conduct of the intelligence requirements management (IRM) and collection management (CM) functions, and optimizes

---

[85] The "J" in the term JISR stands for "Joint", which describes 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 (ISR) capabilities. The "I" stands for the intelligence collection disciplines and/or collection capabilities/assets and the results these disciplines/capabilities/assets can deliver to the commander and/or staff elements. The "S" stands for surveillance which describes the systematic observation of aerospace, surface or subsurface areas, places, persons or things, by visual, aural, electronic, photographic or other means. Surveillance is designed to provide indications and warning (I&W) of adversary initiative and threats and to detect changes in adversary activities. The "R" stands for reconnaissance which describes 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 characteristics (i.e. meteorological, hydrographic, or geographic) of a particular area. See also AJP-2.7

[86] Additional details on the JISR process are contained in AJP 2.7, A*llied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance* and in AIntP-14, *Joint Intelligence, Surveillance and Reconnaissance Procedures in support of NATO Operations*

[87] Including technical exploitation. Technical exploitation is a methodological, integrated and collaborative set of capabilities used to derive data and information from collected materiel. Technical exploitation begins with the collection of information and materiel and through applied scientific analysis, using state-of-the art capabilities, provides empirical and quantifiable data. Deployable technical exploitation capabilities are typically scalable and can make extensive use of reach-back biometric, forensic, and DOMEX capabilities, and other technical exploitation capabilities as required. The outcomes of technical exploitation may support JISR results and the intelligence cycle. See also AIntP-10.

intelligence and operations functions at all levels. The Intelligence System Support Architecture (ISSA)[88] is an essential, integral part of the JISR Architecture.

JISR in full spectrum of NATO operations. JISR capabilities and activities have to fulfill the broadening scope of information and intelligence requirements for planning, preparations, conduct of operations and mission review by NATO at the strategic, operational, and tactical level and in all phases of operations. Decision makers and commanders at all levels will benefit from the output of the intelligence cycle by improved and more effective JISR capabilities. The full spectrum (or continuum) of operations extends from traditional combat operations to other operations that may include peace support, humanitarian assistance, and non-combatant evacuation or cyberspace operations, as well as stabilization, reconstruction operations, crisis management missions, and other missions.

JISR interoperability. JISR is multidisciplinary and is intended to draw intelligence, surveillance and reconnaissance collection capabilities into a coherent whole, providing a framework for the coordination and tasking of these assets. JISR should be interoperable with other domains and functions including their respective systems. Therefore network-communications and information sharing procedures need to assure the interoperability within the JISR Architecture and with its consumers. JISR also provides the means through which time-sensitive information and intelligence are relayed to assets that can make immediate use of it in target engagement (a highly responsive sensor to effector link) and to provide immediate threat warning to friendly forces. The JISR process helps develop situational awareness by contributing to the common operating picture.

JISR Planning. Ensuring the commander's access to the right set of JISR capabilities before and during mission execution is as vital as providing data, information, JISR results and intelligence during operations planning. Thus, it is essential to develop the necessary JISR strategies, operations design, tasks, plans, capabilities, and architecture required for mission execution during operations planning. These requirements will feed directly into the operations plans and detailed annexes, as well as the combined joint statement of requirements (CJSOR) and the force generation task list.
JISR planning is collaborative and occurs simultaneously across all levels of command to synchronize missions, tasks and capabilities. Understanding the OE, the assigned mission and the array of JISR capabilities facilitates effective coordination among all elements.
NATO staffs at all levels of command need to have the ability to define, develop and articulate the requirements for JISR assets and capabilities, command and control (C2), personnel and the communication and information systems (CIS) required for data exchange.
From the initial decision on NATO involvement in any operation, staffs at all levels of command need to have the ability to:

a. Define the JISR Architecture needed to efficiently execute JISR.

b. Articulate the necessary CIS support for the required data exchange.

c. Assess and match the abilities and limitations of JISR assets available against capabilities required.

[88] The intelligence system support architecture consists of intelligence related networks, applications, databases and metadata, including their structure, processes, and the required connectivity.

d. Coordinate between intelligence, operations, plans, and CIS staff divisions and other relevant staff divisions.

e. Manage time critical events.

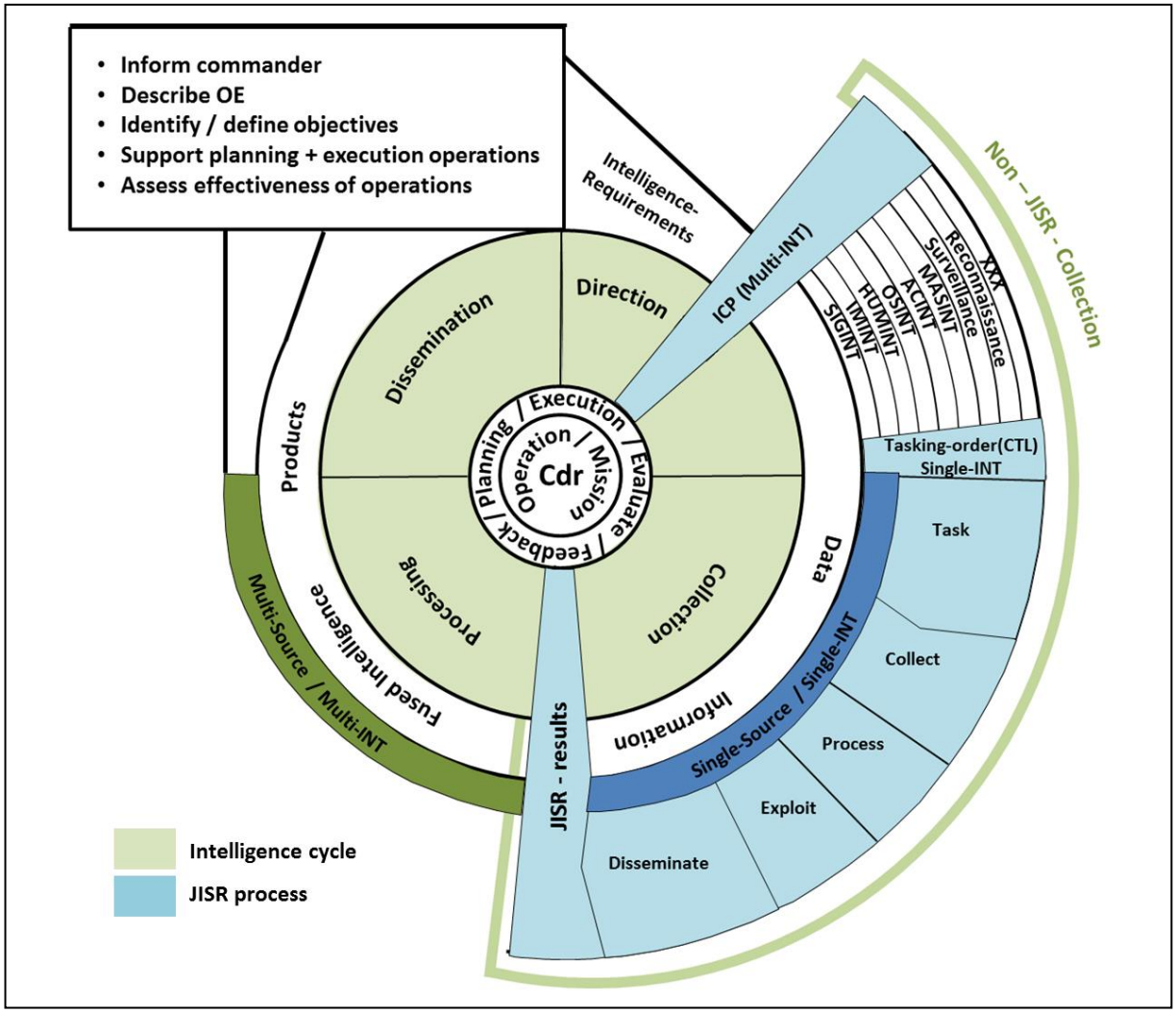

Figure 5. Relationship between intelligence cycle and JISR process

Chapter 5 JOINT INTELLIGENCE SUPPORT TO PLANNING

5.1 OPERATIONS PLANNING PROCESS

NATO's operations planning process (OPP) is described in AJP-5 and in the Allied Command Operations Comprehensive Operations Planning Directive. The OPP is applicable to any strategic, operational or tactical headquarters. Requirements out of the OPP generate a lot of IRs that are fed back into the intelligence cycle.
J2-contribution to the OPP is one of the major outputs out of the intelligence cycle. This output seeks to contribute to understanding and support situational awareness of the operating environment during the whole OPP with various injects to the different phases of the OPP.[89]
In NATO the OE is usually described by the interconnected elements of the PMESII spectrum. The use of this elements ensures that intelligence staff can meet the intelligence requirements of the decision-makers, planners and operators. For some environments, there might be other elements of relevance such as geographics, health and legislation. Intelligence professionals may need assistance from specialists in some PMESII elements (political advisor, engineers and civil military cooperation, etc.) to support their analysis or they may need support from other headquarters, agencies and organizations, including non-military and non-governmental organizations. This collaborative process is necessary for intelligence to be successful in NATO missions.

5.2 JOINT INTELLIGENCE AREAS

To enable commanders and their intelligence staff to focus their intelligence effort, the joint operational area is divided into three areas:

a. **Area of operations (AOO).** An area within a joint operations area defined by the joint force commander for conducting tactical level operations.

b. **Area of intelligence responsibility (AIR):** An area allocated to commanders, in which they are responsible for the provision of intelligence, within the means at their disposal.

c. **Area of intelligence interest (AII):** An area (geographic, political, logical, boundaries) for which commanders require intelligence on the factors and developments that may affect the outcome of operations.

Operating environment. The OE is a composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander. It is the environment directly affected by the crisis in which the JOA is defined. It is inclusive of all actors and actions. It encompasses the physical and non-physical domains and factors relating to air and space, land, maritime, information environment and cyberspace. Intelligence plays a pivotal role within the entire OPP, especially with regard to building/fostering an understanding of the OE from the very beginning of planning and maintaining this understanding throughout the process. Thus understanding of the OE is a critical prerequisite for operations design, as the operations design delineates the own approach in an operation and all activities of the force are deduced from it.

[89] See also AJP-2.1 and AIntP-17

Intelligence contribution to understanding of the OE throughout all phases of OPP is joint intelligence preparation on the operating environment (JIPOE). JIPOE is a crisis-specific, cross-headquarters process, led by the intelligence staff to develop a comprehensive understanding of the OE covering all PMESII factors, including associated potential threats and risks, in support of planning and the conduct of a campaign or operation.
JIPOE is a systematic, cyclical and dynamic process, which is closely connected to the individual stages of the commanders' decision-making process and those related to intelligence processes.

PMESII spectrum[90]**.** Modern crises are characterized by complex interdependencies; conflicts are underpinned by a combination of historical, political, military, social, cultural and economic issues. These issues are generally interdependent and, consequently, the solutions required to address these issues are of a varied nature. NATO recognizes six fundamental PMESII factors within an OE. They are:

a. **Political.** Any grouping of primarily civil actors, organizations and institutions, both formal and informal, that exercises authority or rule within a specific geographic boundary or organization through the application of various forms of political power and influence. It includes the political system, parties and main actors. It must be representative of the cultural, historical, demographic and sometimes religious factors that form the identity of a society.

b. **Military.** The armed forces, paramilitary capabilities and supporting infrastructure, acquired, trained, developed and sustained to accomplish and protect national or organizational security objectives. This also covers the internal security aspects of a country.

c. **Economic.** Composed of the sum total of production, distribution and consumption of all goods and services for a country or organization. It includes not only economic development of a country, but also the distribution of wealth.

d. **Social.** The interdependent network of social institutions that support, enable and inculcate individuals and provide participatory opportunities to achieve personal expectations and life-goals within hereditary and nonhereditary groups, in either stable or unstable environments. It covers the social aspects such as religion, a society's structure, the legal and judicial system, policing and supporting infrastructure, humanitarian, history, etc.

e. **Infrastructural.** The basic facilities, services, and installations needed for the functioning of a community, organization, or society. Includes logistics, communications and transport infrastructures, schools, hospitals, water and power distribution, sewage, irrigation, geography, etc.

[90] The operating environment can be initially viewed through several conceptual models. The most common in NATO are the six listed PMESII elements. But modification or other models are admitted (geospatial + PMESII (GPMESII), PMESII + health (PMESIIH), or areas, structures, capabilities, organizations, people and events (ASCOPE), or actors, audiences, adversaries and enemies (A3E), etc..) and may fit to describe a certain OE or support a planning process.

f. **Informational.** The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. Encompasses the information and communication media.

Cyberspace. Within the overall operating environment, cyberspace transcends our concepts of geographic and political boundaries. It forces commanders to consider operational functions and/or responsibilities rather than traditional geopolitical concepts. Cyberspace is a global domain in its own right. The virtual global domain consisting of all interconnected networks of information technology and including systems and networks which are separated or independent is called cyberspace. Cyberspace is different from the physical domains. Cyberspace, however, is embedded in all the physical domains. Cyberspace exists by virtue of physical components on land, sea, in the air and in space. Vice versa, the traditional physical domains can function effectively by virtue of cyberspace. Consequently, they are dynamically interlinked; a change in one domain usually has implications for the situation in the other domains.

5.3 JOINT INTELLIGENCE PREPARATION OF THE OPERATING ENVIRONMENT

Joint intelligence preparation of the operating environment (JIPOE) provides an understanding of the operating environment and is a basis for planning.[91] The strategic and the operational-level commander typically will provide initial planning guidance based upon current understanding of the OE, the problem, and the politically directed mission. Drawing on the joint intelligence estimate, it focuses the intelligence effort and delineates the prioritization of intelligence requirements. It is a living product and in addition to contributing to the early stages of the operational estimate, assists in the implementation of the plan by identifying opportunities to promote decisive action.

JIPOE should be a process that allows for:

a. Easy and speedy updating.

b. The presentation and prioritizing of large quantities of information and intelligence, usually in graphical form.

c. Easy assimilation of information, incorporating changes to the intelligence picture, and identifying areas containing threats and opportunities.

d. Situational awareness and understanding.

JIPOE relies upon the constant interaction of a headquarters' intelligence, operations and plans staffs to ensure current and future activities of friendly, neutral and adversary actors are properly represented. It is exploited widely across headquarters for a variety of purposes and should:

a. Describe the OE.

b. Analyze the actors including those who are potentially targets.

[91] The JIPOE Process is also highlighted inside AJP-2.1 and in AIntP-17

c. Initiate the development of an intelligence collection plan to satisfy intelligence requirements.

d. Identify places where friendly forces can influence events or opinions through lethal or non-lethal means.

e. Identify when commanders must act to influence the outcome of the operation.

JIPOE is a systematic, cyclical and dynamic process, which is closely connected to the individual stages of the commander's decision-making process. The results of the process are represented graphically on a series of overlays. These overlays include basic data on terrain, meteorological and oceanographic (METOC) conditions, the adversary's tactical doctrine or preferred scheme of maneuver and any other actors impacting the operations, all of which can be prepared well in advance. Just before and during operations, current updates are to be included to reflect changes in key factors that may affect force activity across the spectrum of conflict.

The JIPOE Process. The NATO JIPOE process covers in general, three aspects that are described below:[92]

a. **Step 1** – Describe and evaluate the OE. The first step assesses the effects of relevant factors concerning the operating environment on the activities conducted by both friendly and opposing forces are to be assessed. In relation to counter-terrorism and force protection, this will include the threats to NATO-operations, (e.g. the ethnic distribution of the population and its loyalties). Some of the principal factors affecting the operating environment are terrain, infrastructure, information environment, protected areas, METOC conditions and medical factors.

b. **Step 2** – Evaluate actors in the OE. The aim is to identify an actor's doctrinal courses of action independent of terrain and weather constraints, (i.e. how actors operate according to their tactical doctrine or based on experience from previous operations). Threat evaluation consists of finding the actor, identifying the actor's tactical doctrine or methods of operation and determining their doctrinal course of action.

c. **Step 3** – Determine actor courses of action. The results of step 1 and 2 are combined with the doctrinal course of action and other overlays developed in the threat evaluation. The aim is to identify how the operating environment will shape doctrine and turn it into practice. Predictive assessment of adversary COAs is one of the key outputs of the JIPOE process.

Validation. Validation involves setting up "red" team(s) to get into the mind of an opponent to think through in a structured manner their likely policy or strategy. The military approach to red teaming specifically involves playing the adversary as effectively as possible to test plans, capabilities and concepts. Red teaming can help planners avoid a number of biases; in particular mirror imaging, which is the tendency to assume that others will act much in the same way like ourselves would act under similar circumstances. The involvement of red team members who share the socio-cultural background of the protagonist or who at least have experience of the culture enhances the output of red teaming activities.

[92] Some individual member states use different JIPOE processes with a different number of steps.

JIPOE and the intelligence cycle. JIPOE meshes closely with the intelligence cycle. During the JIPOE process, new intelligence requirements are identified and entered into the intelligence cycle. These requirements will then be translated into questions, and appropriate sources and agencies will be tasked with the collection of information in response to them. This information will then be processed, thereby producing intelligence. This new intelligence is used in the various steps of the JIPOE process in the planning phase and in operations.

JIPOE and the Joint Targeting Process. The joint targeting process closely parallels JIPOE while supporting the integration of joint effects. Initial targeting data is refined through the JIPOE process. Additional intelligence requirements arise during the targeting process and these are integrated into the ICP. The JIPOE supports the identification, selection and location in time and space of targets. In particular, the JIPOE process will identify high value targets and high pay-off targets. Details on the targeting process are contained within AJP-3.9 Allied Joint Doctrine for Joint Targeting.

With the JIPOE process the injects/contributions to the OPP[93] and the Intelligence Estimate are established. 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.

5.4 JOINT INTELLIGENCE ESTIMATE

The joint intelligence estimate describes the operating environment in relation to METOC conditions, adversary, other key actors, cyberspace and terrain, etc. The joint intelligence estimate results in a forecast based on degrees of probability. It is a series of logical deductions drawn from the information available and is influenced by the knowledge and experience of the author. The joint intelligence estimate enables commanders to decide how to accomplish their mission. It should encompass situational awareness and understanding, what is to be achieved and by when, the courses of action available and the desired end-state.

As intelligence is gathered, the joint intelligence estimate increases in detail and provides significant input to the operational-level planning process.[94] The principal outputs of the joint intelligence estimate are:

a. Providing commanders with the intelligence required for the operational estimate.[95]

b. Providing the starting point for intelligence planning by identifying intelligence requirements.

c. Highlighting intelligence-sharing requirements between nations to support the operation.

[93] See AJP-2.1, Chapter 2, Section 3

[94] The joint intelligence estimate can be done using the joint intelligence preparation of the operating environment as a method, or as a straight text document.

[95] The intelligence produced by the joint intelligence estimate should include basic intelligence on the adversary's centre of gravity, his potential courses of action and his high value targets etc.

Production of the Estimate. The creation of the Joint Intelligence Estimate is a process that comprises an analysis of the situation and an assessment.[96] It requires analytical and logical thought processes. The joint intelligence estimate should include:

a. An assessment of the adversary's capabilities, intent and opportunities based on the available intelligence.

b. Identification of the adversary's probable courses of action and the probability of their adoption.

Factors to be considered. When compiling the Joint Intelligence Estimate, the following factors should be taken into account:

a. The commander's mission and tasks.

b. METOC conditions and terrain.

c. The general situation of the adversary and their conduct of operations to date, including their center of gravity.

d. The activities, capabilities and vulnerabilities of the adversary to include possible reinforcements and any forces in adjacent area which are able to influence operations.

e. The options and the adversary's doctrinal norms.

f. The adversary's likely intentions including their aims and objectives in immediate and follow on operations.

g. Socio-cultural factors of the friendly, neutral and adversary persons, groups and networks as part of the population in the JOA.

Assumptions. Assumptions may be used when there are gaps in the intelligence staff's knowledge and the assumption is necessary to continue the planning process. It is a basic principle to avoid speculation. Assessments have to be based on the best possible intelligence. To avoid any misunderstanding, assumptions must always be clearly identified as such and labeled. Assumptions should be regularly revisited and checked against new and emerging intelligence. Logical consistency of thought and a clear separation of facts from assumptions are essential for the production of a reliable assessment. There should always be close liaison between intelligence, plans and operations staffs, particularly when considering the CCIRs and preparing the intelligence requirements arising from them, which shape the intelligence estimate. Many facts and conclusions from the joint intelligence estimate will also be used in an operational appreciation (e.g. actors´ strengths, capabilities, vulnerabilities, intentions, possible courses of action and the most likely course of action). As operations planning is evolving some assumptions may become risks and handled by J5 accordingly (risk assessment).

[96] See also AJP-2.1 *Intelligence Procedures*.

Chapter 6 COUNTER-INTELLIGENCE AND SECURITY

6.1 INTRODUCTION TO COUNTER-INTELLIGENCE AND SECURITY

This chapter provides an overview of security and counter-intelligence including their role, functions, responsibilities, the CI principles and countermeasures. Additionally, details on Counter-Intelligence and Security are contained in the Allied Joint Doctrine for Counter-Intelligence and Security Procedures.
Security is the condition achieved when designated information, materiel, personnel, activities and installations are protected against terrorism, espionage, subversion, sabotage, organized crime (TESSOC) activities as well as against damage, loss or unauthorized disclosure.

Counter-intelligence (CI) includes information gathered and those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or individuals engaged in TESSOC. CI 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-informed decisions on security measures[97]. In reality, there are likely to be compromises between what is needed and what is feasible.

Responsibility for counteracting the threat. CI organizations, military or civilian, of the member states (including law enforcement organizations) of the Alliance are responsible for counteracting the threat to security posed by hostile intelligence services and subversive, criminal or terrorist groups or individuals.

6.2 THE THREAT TO SECURITY

Threats to security can originate from both external and internal sources. The threat is met by making proper provision for the maintenance of security at the earliest possible stage of planning. Security staffs should pay particular attention to insider threats as they have access and opportunity to cause grave damage to information, resources, and personnel and critically impact upon operations.[98] These threats may be acting with or without outside influence in any domain.

The threats to security can be categorized as:

a. **Terrorism**. Terrorism is the unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives.

[97] See AJP-2.2

[98] The *insider threat* comes from personnel who have privileged access to classified or official data and subsequently abuse this access to destroy damage, remove or disclose the data. It also includes those personnel who have legitimate access to NATO facilities and use this access to conduct acts of terrorism or sabotage.

b. **Espionage**. Espionage is an intelligence activity directed towards the acquisition of information through clandestine means and proscribed by the law of the state against which it committed.

c. **Sabotage**. Sabotage includes any acts falling short of a military operation, or any omission, intended to cause physical damage in order to assist an adversary or to further a subversive political objective.

d. **Subversion**. Subversion consists of action or a coordinated set of actions of any nature intended to weaken the military, economic or political strength of an established authority by undermining the morale, loyalty or reliability of its members. An attack on individual or collective loyalty is designed to be disruptive and is difficult to detect and to counter. Methods of subversion may include:

(1) Propaganda and agitation, demonstrations and riots, distribution of pamphlets.

(2) Use of *cover organizations* to conceal real activities.

(3) The recruiting of supporters who operate either consciously or unconsciously on the behalf of their recruiters.

(4) The creation of a climate of mistrust and disillusion which leads to the discrediting of governments and individuals.

(5) The spreading of false rumors or distorted truth (disinformation) aimed at destroying confidence in leaders or allies.

e. **Organized crime.** Organized crime constitutes any enterprise, or group of persons, engaged in continuing illegal activities which has as its primary purpose the generation of profits, irrespective of national boundaries.

6.3 COUNTERACTING THE THREAT TO SECURITY

The role of CI. To ensure successful military operations commanders should deny the adversary the opportunity to conduct TESSOC against friendly forces. This requires identification of the friendly force's vulnerability to an adversary's intelligence gathering operations. This information is used to inform OPSEC, counter surveillance and deception planning including protective security policy. In addition, CI also supports force protection efforts, cyberspace operations, information operations, security, psychological operations, targeting, biometrics, and other parts of operations, functions and tasks. Details of the spectrum of routine and non-routine activities conducted in NATO are described in AJP-2.2.

NATO CI organization. The organization of CI within NATO nations varies. Therefore, CI staff elements should liaise with their points of contact at national ministries of defence with superior, lateral and subordinate headquarters to ensure familiarity with neighbouring CI structures.

National responsibilities. Each nation should designate one organization as the single point of contact for CI matters. Within each national organization, a national counter-intelligence adviser (NCIA) will be nominated. As some of these NCIAs are unlikely to be permanently

available, nations will nominate National counter-intelligence representatives (NCIRs) for assisting the NCIAs or for being deployed at the various levels of command during exercises or operations. The NCIR's function is to coordinate CI activities with their national authorities and to support CI staffs in these HQs. Where national intelligence cells are established in theatre to support NATO operations, elements of the national CI organizations should be present in these cells to ensure the rapid exchange of warning messages with the appropriate NATO CI Cell. The NATO strategic commanders and their CI advisers will be able to meet their responsibilities only if they receive the close co-operation of national authorities since it is the latter who retain control of their CI agencies (other than those assigned to the NATO forces). Co-operation in time of conflict can only be ensured by good peacetime liaison arrangements. It must be made clear that during a time of conflict NATO nations are responsible for meeting general and specific CI requirements specified by strategic commanders, in accordance with national caveats.

CI coordinating authority. When NATO forces are deployed on operations, the designated counter-intelligence coordinating authority (CICA) will supervise all aspects of CI and will be the commander's principal advisor in CI matters. The CICA coordinates and de-conflicts national and NATO CI operations and investigations in the joint operations area.

J2X. J2X is the J2 staff element that coordinates, de-conflicts, and conducts collection management, exploitation and dissemination of CI and HUMINT on behalf of a NATO commander within a joint operations area (JOA). It supports operations and provides a bridge between the All Source Analysis Cell and the operators on the ground.

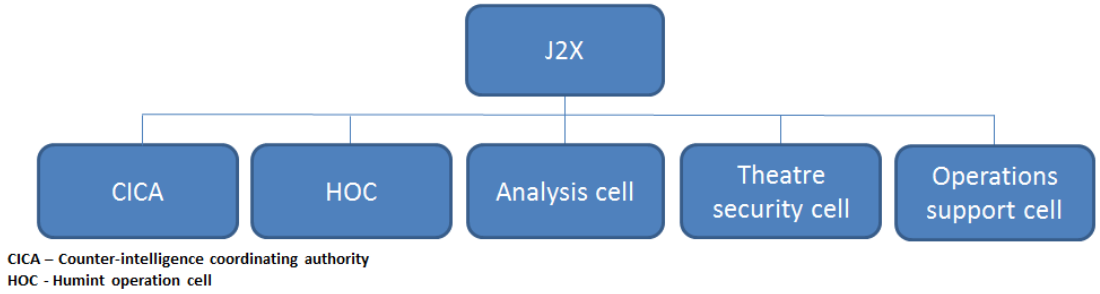

Figure 6. J2X Structure

Normally, CI will be coupled with security and HUMINT under the staff direction of an appointed J2X. During operations, the direction, co-ordination and supervision of deployed military CI and HUMINT elements are the responsibility of the J2X within the Intelligence Branch. J2X staff will maintain source registry and de-conflict both CI and HUMINT activities with regard to national reservations and caveats. The J2X will provide advice to commanders on CI and HUMINT operations, and security. The J2X ensures that information sharing agreements and methods are in place in order to increase situational awareness and the efficiency of the entire security, CI and HUMINT efforts.
J2X Staff function is a vital tool for the commander to provide timely, accurate and often unique intelligence on intentions, capabilities and threats.
The J2X structure is mission-dependent; a ‘2X’ element should be established at each echelon of command. J2X retains the technical control of the subordinate tactical 2Xs to ensure a consistent theater-wide security/CI/HUMINT picture.

CI and HUMINT. Within J2X, the CI cell coordinates the full spectrum of CI activities (functional services, investigations, collections, analysis and production, and operations)[99]. CI activities often occur alongside those involving HUMINT and many of the skills and capabilities are common. CI and HUMINT should be regarded as being complementary and must not become competitive. Even if CI and HUMINT personnel may use similar methods, their missions are separate and distinct. CI is focused on TESSOC threats while HUMINT is focused on collecting intelligence to satisfy other intelligence requirements.

Security staff. The principal responsibilities of the security staffs at all levels of command are:

a. Advise commanders on all security threats, to include those assessed by CI.

b. Manage and support operations to counteract the security threats.

c. Collect, process and disseminate information relative to CI requirements and produce and disseminate current threat assessments.

d. Contribute to the operations security (OPSEC) process, including the planning, coordination and application of protective security measures throughout the formation.

e. Establish and maintain liaison with civil law enforcement and CI authorities.

f. Ensure there is a clear classification guide and disclosure procedure that complies with the NATO security policy.

Need-to-know principle. "Need-to-know" describes the legitimate requirement of a prospective recipient of data to know, to access, or to possess any sensitive information represented by these data. The fundamental security principle is that knowledge or possession of classified information should be strictly limited to those, who are cleared to the appropriate security level, and who clearly have a need-to-know to carry out their duties. No person is entitled by virtue of rank or position to have access to classified information. The enforcement of the need-to-know principle limits the damage that can be done by an insider threat, while failures in enforcing the need-to-know principle can significantly damage security.[100] However, because there is also a responsibility to share information with coalition partners, products should be written for release (balancing the need-to-know principle with the responsibility to share).

Governing security operations. Security operations are to be conducted according to the following principles:

a. Commanders at all levels are responsible for security.

b. Security operations must be coordinated with the intelligence staff, in consultation with the operations and other staffs, and must be integrated with the overall intelligence effort.

c. There should be a single focus at each level of command for security policy.

d. Security teams must be established to engage threats and to give security advice to commanders at each level of command.

[99] For further details regarding the full spectrum of CI activities see AJP-2.2.

[100] Nations have a responsibility to maximize sharing of information.

e. Threat information should be produced by intelligence, counter-intelligence and security personnel as warnings, threat assessments and statements of the threat level. These must be given the lowest possible security classification and disseminated as widely as possible.

f. The collection of security related information should be coordinated at each level of command and integrated with the overall intelligence collection effort.

g. Responsibility for the establishment and maintenance of security intelligence databases must be clearly defined and wherever possible integrated with the overall intelligence effort.

CI principles:

a. Proactiveness. CI activities must aim at identifying vulnerabilities and risks, and at predicting of potential threats to security posed by hostile intelligence services, terrorist group or individuals, to enable superiority over existing and future adversaries. The primary role of CI staff is to proactively find and understand threats to the force and to then subsequently identify own vulnerabilities in order to maintain operational resilience and freedom of action.

b. Continuousness. CI process needs to be sustainable in nature to ensure continuous monitoring, awareness and understanding of the threats to security.

c. Sensitiveness. CI products containing sufficiently sensitive information, which may detrimentally impact any current investigation or operation, or may be intended to be bilateral in nature, do not merit widest dissemination.

d. Interoperability. Common or interoperable processes, networks and systems are required to support CI direction, collection, processing and dissemination and the management of the counter-intelligence organization. CI assets should be centrally coordinated to avoid duplication of effort, provide mutual support and ensure the efficient use of all resources.

Operational-level planning. The assistance of CI staff at the outset of the initial planning phase of the operation is essential. During operational-level planning commanders should ensure that CI staffs pay particular attention to the identification of friendly force vulnerabilities that may be exploited by adversary collection assets and towards the determination of appropriate countermeasures.

Exchange of information. It is a national responsibility to decide the level of exchange of CI information. However, nations are responsible for providing CI information to enable NATO commanders to react against the threat. During operations the need to counter the existing and constantly changing threat will require timely exchange of all available CI information. The sharing of security information amongst NATO nations and NATO partner nations improves security of multi-national operations.

CI liaison. Liaison between national CI organizations at the various levels and the appropriate NATO military commands will lead to greater awareness and understanding of the overall threats and related problems in peacetime. Such liaison will establish the framework for a changeover from peacetime to crisis operations. The success of security measures will depend also on the maintenance of effective liaison between CI organizations and:

a. National and NATO military commands.

b. National and NATO security and CI staffs.

c. Local law enforcement and customs authorities.

d. Public administration or other civilian authorities.

e. Organizations dealing with cyberspace issues.

CI operations. CI operations can make a significant input to force protection and OPSEC. Primary activities are liaison, investigations, casework, screening of locally employed civilians and intelligence collection.[101] Liaison is conducted to obtain and corroborate information, develop sources of information and foster both goodwill and understanding. A technical agreement (TA) or/and memorandum of understanding (MOU) should be signed between the host nation and NATO so that legal issues be effectively addressed. Investigations are conducted into the activities of an adversary and into personnel security matters, in this case, a special request will be first addressed to the NCIA of the person concerned. CI casework may exploit opportunities to develop a greater understanding of security threats or weaknesses. Investigations and casework may employ interviews, record checks, technical measures, computer forensics, covert search and covert passive surveillance to develop understanding of the situation.[102] CI operations require a high degree of integration with intelligence and HUMINT staffs.

Security awareness and education. All individuals who are authorised access to, or required to handle NATO classified information, shall initially be made aware, and periodically reminded of the dangers to security arising from indiscreet conversation with persons having no need-to-know, their relationship with the media, and the threat presented by the activities of intelligence services which target NATO and its member states. Individuals shall be thoroughly briefed on these dangers and must report immediately to the appropriate security authorities any approach or maneuvre which they consider suspicious or unusual. The maintenance of high standards of security education is of particular importance in all NATO countries to counter terrorism, espionage, sabotage, subversion, organized crime and computer network attacks.

Threat assessment. A threat assessment evaluates across a broad range of identified threats and provides a basis to determine physical and operational mitigation measures for protection from those threats. An assessment may assign a numerical or other type of rating to signify the level of a particular threat such as high, medium or low. Threat assessments generally focus on threat from TESSOC.[103] Threat assessments should contain the following at a minimum: identification of the threat, key intelligence judgements concerning the threat, and the degree of confidence in the assessment of the specific threat. The threat assessment should contain an overview statement or executive summary that stresses key elements of the assessment and provides a synopsis of the total assessment. The summary should be specific and sharply focused to provide key intelligence judgements. If the threat assessment is

[101] This includes dealing with persons who arrive at a base and make an unsolicited offer to provide intelligence (known as *walk-ins*) and people identified during screening tasks.

[102] It is essential that the appropriate NCIA is notified of any investigation into personnel from a NATO member state.

[103] See AJP-2.2

updated from previous versions, it should indicate changes in the threat. Generally this summary is short, concise, and to the point. [104]

6.4 THE COUNTER-INTELLIGENCE ESTIMATE

The CI estimate is an integral part of the joint intelligence estimate and draws upon its factors, deductions and risks to identify threats (actors and methods) and own vulnerabilities.

The CI estimate supports and complements the joint intelligence estimate to:

e. Provide an estimate of friendly force vulnerabilities to an adversary's JISR operations; thereby informing counter surveillance, OPSEC and deception planning.

f. Give an insight into the information supporting the adversary's decision-making process will assist in the selection of the adversary's most likely course of action.

[104] See AJP-2.2

Intentionally blank

ANNEX A - INTELLIGENCE COLLECTION DISCIPLINES

This annex includes a closer consideration of the intelligence collection disciplines that are described shortly in Chapter 3.1.

1. Acoustic intelligence[105] (ACINT)

a. ACINT describes intelligence derived from acoustic signals or emissions. It represents a prime intelligence source for decision-making at all levels in NATO as a collection intelligence discipline. Commanders should ensure that ACINT contributions as a JISR result are taken into account during operations planning, especially in naval warfare aspects.

b. ACINT uses broadband and narrowband analysis of acquired acoustic signals to classify and identify an underwater or surface contact at sea or low-flying aircraft such as helicopters. The term is generally used in reference to undersea intelligence gathered by sensors on submarines and ships. This form of intelligence involves listening to the sea and categorising the sounds which are heard. Passing warships, submarines, etc. create cavitation waves which leave a distinctive signature, and they may also emit various sounds and generate noise as they engage in various activities. ACINT subject matter experts (SMEs) can differentiate between natural sounds, and human-generated sounds. ACINT also involves the study of how sounds move in the ocean. The knowledge accumulated in this field allows acoustic technicians/operators to distinguish between different types of sounds, filtering out the characteristic acoustic signatures of contacts which are viewed as non-threatening. Learning to distinguish the different types of underwater and surface noises is very important, as is learning to identify noises which probably pose a threat, like the ultra-quiet engines of advanced diesel/nuclear submarines, or the sounds of incoming torpedoes. ACINT data serve numerous important purposes. They can help identify threat acoustic vulnerabilities; vulnerabilities which may be exploited by new sensors, processors and equipment. Therefore, they help in the improvement of detection capabilities and the development of new tactical doctrine.

c. ACINT Examples. ACINT is an intelligence collection discipline that collects and processes acoustic phenomena. Broadband analysis concerns the overall noise created by a platform, while narrowband analysis examines the spectra of the received energy at a more accurate level. Broadband analysis is useful for identifying any vessel at a long range, while narrowband analysis is generally more useful for identifying the category, type and ideally the individual vessel name. The category might be for example differentiating between a commercial vessel and a warship; the type might be narrowing this down to an individual class and hence identifying nationality, and the individual name might identify the specific ship or submarine. Narrowband analysis might identify whether a subject of interest has single or multiple propeller shafts; the number of blades per shaft and other salients that may help identify the platform. This may include the fundamental or harmonic emissions based on the electric services used, the gearing between shaft and engine and also the combination of gear teeth used in the ratio(s). ACINT also supports mine warfare

[105] Some NATO member states consider ACINT to be part of MASINT.

countermeasures. Most naval mines use acoustic sensors. To counter this threat, a good knowledge of vessels acoustic signature is necessary. ACINT can help the nations to control their signatures and establish effective acoustic countermeasures. Moreover, acoustic intelligence should provide knowledge about the threat useful for setting mine countermeasures systems (acoustic spectrum for jamming and sweepers, mine acoustic index for hunters).

d. Requirements for an effective ACINT System. ACINT allows the classification of vessels at a long range providing indication and warning. It is used to provide information like the category, type and even the specific ship or submarine (depending on the acoustic signatures archived in the system database). For the successful identification of a platform the following are required:

(1) Advanced technology (sonars, hydrophones, geophones, etc.) to acquire the acoustic signals.

(2) Sophisticated algorithms to process and analyze the acquired signals.

(3) An updated and detailed acoustic classification system (acoustic intelligence database).

(4) Highly trained acoustic operators/technicians/specialists. It should be noted that despite the expanding array of sophisticated technology and tactics, it is still the ears and the minds of the specialists that are the final determiners of effective ACINT.

e. ACINT and Acoustic Environment. ACINT is the discipline that uses broadband and narrowband analysis of acquired acoustic signals or emissions to classify and identify an underwater or surface contact at sea. It is an essential as part of naval warfare knowledge. ACINT primarily provides intelligence to joint decision-makers and naval warfare commanders at all levels in support of situational awareness to include:

(1) Threat warning and force protection at sea,

(2) Identification of vessels and submarines,

(3) Provision of information on an adversary naval force in support of decision-making process including mines acoustic systems,

(4) Prediction of an adversary’s movements or intentions.

f. ACINT and Acoustic Warfare relationship.

(1) ACINT and acoustic warfare are closely related; in an underwater environment, acoustic warfare is the use of acoustic energy to provoke, exploit, restrict or prevent adversary use of the acoustic spectrum and the implementation of any measures taken to restrict its use to friendly forces. Both focus on operations in the acoustic spectrum. The primary aim of acoustic warfare is to create offensive and defensive effects.

(2) ACINT allows acoustic warfare support measures as actions taken to search for, intercept and identify radiated acoustic energy for the purpose of exploiting such radiation. ACINT allows classifying vessels at a long range, category, type and finally the specific ship or submarine. Based on advanced technology to acquire and condition the signal, sophisticated algorithms process and analyse the signal which is compared with an acoustic intelligence database.

(3) Acoustic warfare countermeasures in an underwater environment are actions taken to prevent or reduce the use of the acoustic spectrum by adversary forces. Acoustic warfare countermeasures involve intentional underwater acoustic emissions for deception and jamming.

(4) Acoustic warfare counter-countermeasures are taken to ensure effective friendly use of the acoustic spectrum by countering adversary acoustic warfare measures. Acoustic warfare counter countermeasures involve anti-acoustic warfare support measures and anti-acoustic warfare-countermeasures, and may not involve underwater acoustic emissions.

(5) ACINT reports are used to support the creation and maintenance of acoustic databases.

g. Advantage for commanders

(1) ACINT can be passive (only listen) so you can avoid the detection of your platform

h. Disadvantages for commanders

(1) Requires sophisticated systems

(2) Requires highly trained operators

(3) Requires a frequently updated acoustic signature database (every change you make on a ship/submarine, like for example the installation of new equipment, changes the acoustic signature so you need to collect its acoustic data again).

2. Human intelligence (HUMINT)

a. Human intelligence (HUMINT) is described as intelligence derived from information collected by human operators and primarily provided by human sources.

b. HUMINT is unique because it can provide insights into intentions, morale, and motivations of individuals as well as details on relationships among individuals/organizations of intelligence interest, and places with exclusive human access. Human sources may also serve to obtain materiel of intelligence importance, such as weapons, documents, computer data, media, and photographs, for further technical exploitation.

c. HUMINT plays a major role in modern warfare and crisis response operations, where other indicators and warnings may be absent.

d. The HUMINT spectrum[106] is divided into:

(1) Framework Activities, which represent the exploitation of collection opportunities arising from activities involving force components[107] – "every soldier is a sensor". Any member of the Force who interacts with the local population in the joint operations area (JOA) as part of his normal duties, may obtain information of Intelligence value. Such information is to be reported in order to be processed and inserted into the Intelligence channels. These methods should not hinder the Force members' capacity to perform their primary duties.

(2) HUMINT activities, which represent source and non-source operations, conducted by trained HUMINT operators.

e. The need to protect intelligence sources and methods gets extraordinary significance in case of HUMINT. The compromise of such information can lead not only to loss of intelligence, but also to physical harm/death of the human sources (and possibly HUMINT operators) or even to severe damage to the entire mission. Due to high sensitivity and overall implications, HUMINT requires centralized control over all information that may reveal source identity and operational methodology, in order to ensure operator and source protection.

f. HUMINT in operations. The HUMINT staff supports the operations planning process (OPP) by contributing to the joint intelligence estimate (with the HUMINT estimate[108]) and to joint intelligence preparation of the operating environment (JIPOE), as well as addressing the HUMINT critical capabilities in concept of operations (CONOPS) and operation plans (OPLANs)[109].

g. HUMINT collection in NATO operations is driven by the intelligence requirements management & collection management (IRM&CM) processes and is directed by J2X, based on the intelligence collection plan (ICP). In this respect, the collection assets shall provide accurate, relevant and timely information to be conveyed to the J2X analysis section. Nevertheless, HUMINT source operations require patience and time[110]. Therefore, intelligence requirements must be developed with sufficient lead-time for collection.

h. The main output of HUMINT collection activities is the human intelligence report (HUMINTREP). HUMINT production is pushed to the Intelligence staff, which will incorporate it into a fused, all-source Intelligence product, in a time scale that meets planning and operational priorities.

---

[106] The full description of HUMINT activities is reported by specific publications.

[107] But still needing the J2X oversight and supervision.

[108] The strength and organization of the HUMINT elements will depend on the HUMINT Estimate in accordance with: type, mandate, and nature of the operation; CCIRs/PIRs; composition and size of the Force; operating environment; adversary; expectations of the number of human sources; available HUMINT elements and required skill sets, etc.

[109] Commanders should consider a series of limitations (deriving from legal constrains, lengthy and complex source exploitation processes, compartmentalization of work to ensure source and operator protection, etc.) affecting the HUMINT collection planning.

[110] This is valid especially in initial phases of mission when source networks may not be established yet.

i. J2X applies a rigorous process for determining the reliability of human sources and the credibility of information provided by them. Even so, military decision making based on information from a single human source should be carefully considered. It is always a good practice to have such information confirmed by a second source, preferably belonging to a different discipline (IMINT, SIGINT etc.), before any decisive action is taken.

j. HUMINT is relevant for all operating environments. With its particular insight and cross-cueing[111] with other Intelligence disciplines, HUMINT is a valuable enabler for different functional areas, like identity intelligence (I2), biometrics-enabled intelligence (BEI), human networks analysis and support to targeting (HNAT), etc. HUMINT is of paramount importance for special operations forces, providing actionable Intelligence, enabling their orientation to target and enhancing force protection.

k. J2X is the J2 staff element responsible for coordination, de-confliction, collection management, analysis and dissemination of HUMINT and CI on behalf of a NATO commander within a JOA. It supports operations and provides a bridge between the All Source Analysis Cell and the operators on the ground.

l. HUMINT staff organization. Human intelligence operations cell (HOC) is the J2X[112] staff element responsible for management, coordination and de-confliction of HUMINT activities within a JOA, in accordance with national caveats and mission constraints.

m. Field human intelligence teams (FHTs) are the HUMINT collection elements. Their organization, tactics, techniques and procedures are described in specific publications[113].

n. FHTs form a versatile capability readily deployable to support mission commanders in all types of operations, at any scale of complexity, for any command structure, across the full spectrum of conflict intensity and throughout all phases of operation. HUMINT needs to be employed from the earliest phases of the operation and be appropriately covered in the Agreements with the Host Nation to achieve full effectiveness. According to the mission and operating environment, HUMINT elements have specific requirements[114] in order to gain the necessary low profile and maintain adequate mobility and survivability; in this respect, HUMINT may entail specific exemptions from general force protection rules.

o. Re-deployment from an operation during rotations and even at its termination does not annul the obligation to protect human sources related data. Archived human source data must not be disclosed by any organization in any context without prior formal consent of the data owner.

---

[111] HUMINT uses cross cueing for enhancing its collection, by coordinating with other Intelligence assets that can provide further detail when additional information is required concerning a collection opportunity. HUMINT may also need to cross cue information for its own operational purposes.

[112] A '2X' element should be established at each echelon of command and serves as a bridge between the J2 All-Source Analysis and the HUMINT collection assets.

[113] See AJP-2.3 and AIntP-5

[114] Performance of HUMINT operations require unusual support, such as: access to Intelligence Incentives Funds, non-tactical vehicles (inconspicuous vehicles), rights to upload/download information into/from mission classified equipment and networks or exemptions from general force protection rules. In certain cases, Commanders should ensure the access of HUMINT operators to special categories of individuals of intelligence interest (e.g. Captured Persons).

p. HUMINT coordination, cooperation and deconfliction. HUMINT operations require cooperation with the staff elements at the operational level, Host Nation(s)' Intelligence agencies and other collection assets operating across the JOA. The HOC shall acknowledge the differences in terms of opportunities, methodology, and procedure in order to cope with the responsibilities of coordinating HUMINT Framework Activities conducted by other force elements, perform human source deconfliction and, if warranted, operational deconfliction.

q. HUMINT elements under J2X frequently have interactions with other force elements, such as: Special operations forces, military police and gendarmerie type forces, provost marshal office, drug and law enforcement organizations, PsyOps, CIMIC, country advisers, political advisers, maneuver and combat service support units, liaison & monitoring teams, etc. In this spectrum, debriefing of friendly force elements by HUMINT operators should be regarded as a collection enabler and a building block for enhancing the overall Intelligence effort.

3. Imagery intelligence (IMINT)

a. Imagery intelligence (IMINT) describes intelligence derived from imagery acquired by sensors which can be ground based, sea borne or carried by air or space platforms. IMINT as one of the intelligence collection disciplines in the context of the joint intelligence, surveillance and reconnaissance (JISR) process, and its wider application within the intelligence cycle delivers JISR results. Imagery, in and of itself, is not intelligence. IMINT is produced by imagery analysts who have conducted appropriate exploitation of individual images or image sequences, using specific tools and techniques[115]. Effective IMINT results are the result of a deliberate effort to collect, process, and exploit select imagery, to answer intelligence requirements. IMINT is a valuable part of intelligence providing detailed and precise information on the location and physical characteristics of threats, infrastructure, and the physical environment. It is an important source of information to help determine and monitor physical characteristics of key terrain features and patterns of life, orders of battle, target intelligence, battle damage assessments, and adversary courses of action.

b. IMINT utilises five principles: Requirements focussed; optimised through clear direction, fully coordinated; collaborative in nature and fully compliant (with policy and the law). There are several limiting factors associated with the use of IMINT including: it may be time consuming, its assets requirements, can be affected by weather and its reliance on technology, notably it's use of information systems.

c. Different types of imagery. It is important to understand that imagery is divided in two categories, digital imagery and motion imagery. This section also covers the various collection platforms and the impact of sensor orientation on results. Categories of imagery are: Electro-optical (EO) imagery, radar imagery, light detection and ranging (lidar), commercial imagery. EO imagery refers to the collection of electromagnetic energy from the visual, near infrared and or thermal infrared parts of the electromagnetic spectrum. EO sensors are passive, only collecting electromagnetic energy emitted by or reflected off the

[115] Imagery/IMINT acquired by sensors have usually geolocation data (e.g. corner coordinates), but this data are depending on the platform specifics and are not from high quality regarding accuracy. This data could only be used for joint effects when additionally geospatial support information where to bring this date to highly precise geo-coordinates.

target itself. Radar is an active collection system that, depending on the power and frequency of the transmitter, can penetrate virtually all atmospheric conditions. Radar imagery may look similar to EO imagery, but has particularities that may lead to misunderstanding if not taken into account. Radar imagery generally is limited only by the capability of the platforms conducting the collection mission. Lidar sensors are similar to radar, but transmit laser pulses instead of radio waves, and can be integrated into airborne platforms. Commercial imagery sensors can provide an increased capability to supplement and complement military imagery collection, by providing additional coverage, faster revisit time, larger areas of collection, more image band collection options, unclassified imagery, and tailored imagery products. Using unclassified imagery allows much greater dissemination options, essential for NATO operations.

d. IMINT supports as a JISR result to NATO operations, notably the amount of support required at the strategic, operational and tactical level. IMINT support must be tailored to the needs of the operation in order to support comprehensive joint intelligence preparation of the operating environment (JIPOE). IMINT supports identification of key adversary capabilities. This leads directly to better situational awareness and support to joint effects, collateral damage estimation (CDE), battle damage assessment (BDA) and contingency planning.

e. Developing the imagery capabilities and executing IMINT activities to meet NATO force requirements are challenges that require extensive cooperation and coordination among all members of the intelligence community. Oversight of IMINT at the NATO strategic level is split between the International Military Staff (Intelligence) at NATO headquarters and the strategic commands. This section also includes the responsibilities embedded within a combined joint task force (CJTF). An Important aspect of providing IMINT to a deployed task force is its reachback capability. IMINT reachback support is the ability for deployed units or organizations to refer specific collection and production requirements to higher agencies such as the NATO intelligence fusion center (NIFC), NATO Alliance Ground Surveillance Force (NAGSF), or to national IMINT support agencies. However, the communication and information systems (CIS) requirements needed necessitate advance planning between nations.

f. Working with NATO in a combined/joint service environment is complex and requires participating nations to agree to implement certain standards and agreements related to imagery activities. Interoperability significantly enhances the capabilities of the forces involved and increases flexibility and efficiency to meet mission objectives. There has to be a balance between “responsibility-to-share” and a “need-to-know” basis to protect sources/methods of imagery at national levels. To ensure the ability to retrieve and exchange imagery and IMINT in a network-enabled environment, the use of agreed information exchange requirements and metadata standards is essential.

g. IMINT-related training goals and objectives and recommends are major topics for inclusion in IMINT and imagery-related training. It does not provide a baseline unit training plan nor does it attempt to describe specific IMINT-related, individual, or unit training standards, operational procedures, or systems training requirements. Training should be performance-oriented and include specialized training focussing on: analysing, sharing, collection and storage of IMINT. Training should also include members of the combined joint planning staff (CJ5) to identify their IMINT requirements.

h. IMINT should be considered in the context of the digital era where modern air, land, maritime, and space platforms may all be imagery collection systems. Current technological changes (e.g. from wet film to digital sensors) have expanded the capabilities of imagery systems, for both collection and exploitation, and how imagery can be used operationally. In the digital era, with increased communication means, still imagery, imaging radar scans, and video can now all be sources of near real-time information.

4. Measurement and signature intelligence (MASINT)

MASINT is described as intelligence derived from the exploitation 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. It produces JISR results for scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, spatial, wavelength, time dependence, modulation, plasma and hydro magnetic) derived from specific technical sensors for the purpose of identifying specific features associated with the source, emitter or sender in order to facilitate subsequent identification and/or measurement of the sender. MASINT is derived from the collection and comparison of a wide range of emissions with a database of known scientific and technical data in order to identify the equipment or source of the emissions. MASINT can provide specific weapon system identifications, chemical compositions and material content and information on a potential adversary's ability to employ these weapons.

a. **MASINT Sub-Disciplines.** As noted, MASINT sensors fall into one of eight sub-disciplines. While NATO defines the sub-disciplines using these eight definitions, many nations use different subsets of these sub-disciplines. While some nations choose to include some capabilities in the MASINT discipline, others exclude some of them in favour of different management of the activity outside the MASINT community. NATO's "super-set" of sub-disciplines incorporates all of the activities of all nations defined as MASINT, allowing each nation to define their own subset definition of MASINT from within this group.

b. Examples of each sub-discipline are included in Table 1, which follows. This list is only exemplary, and not intended to be inclusive of all possible sensor types.

Table 1. Examples of MASINT Sub-Disciplines

Examples of MASINT Sub-Disciplines							
Biometrics	*Radio*	*Geophysical*	*Electro-optical*	*Nuclear*	*Materials*	*Multi/Hyper Spectral*	*Radar*
Identification of Facial features, scars, tattoos Voice Iris Fingerprint DNA	Radio Waves Electro-magnetic Pulse (EMP) Detection Unintentional RF (URF)	Seismic/Acoustic/ Vibrometric Sensing Very Low Freq (VLF) Extremely Low Freq (ELF)	Non-Imaging Infrared (IR) Visible Light Non-Imaging Ultra-Violet (UV) LASER	X-Rays Gamma Ray Detection Neutron Detection Cosmic Ray Detection	Chemical/ Biological Sensing - Liquid - Solid - Aerosol - Gas	High Spectral Resolution Across Multiple Narrow Bands - IR - Visible - UV	Microwave Over-the-Horizon Radar (OTHR) Synthetic Aperture Radar (SAR) Polarimetric

(1) **Biometrics.** Biometrics addresses the detection and analysis of human signatures, which are used to positively identify an individual from a population, and so plays an important role in HUMINT operations. While fingerprints are the most common human trait used for signature analysis, many other attributes of the human body are unique to each individual. NATO Standardization Agreement (STANAG) 4715 defines the biometrics attributes and how to process the signature information to enable biometric data base enrolment, search, and watch list reporting. Within this standard are definitions for appearance characteristics (e.g., face image, scars, tattoos), voice patterns, iris scans, fingerprints, and deoxyribonucleic acid (DNA). Other attributes, such as retinal scans, may be added at a later time. Obtained data, information and JISR results will be used to produce biometrics-enabled intelligence (BEI).

(2) **Radio.** Radio frequency (RF) technical analysis involves measuring electromagnetic radiation across frequencies spanning from nearly zero up to but not including infrared. RF MASINT targets are usually unintentional by-products of an event (e.g., nuclear explosion electromagnetic pulse (EMP)) or unintentional radiation from sources such as engines, power sources, weapon systems, and electronics. Intentional use of RF pulses as a weapon (but not a signal) or nuclear EMP simulation also falls under RF MASINT.

(3) **Geophysical.** This class of sensors focuses on various physical field changes including acoustic, seismic, magnetic, gravity, and electric field collections. Acoustic involves the collection of passive or active emitted or reflected vibrations in the atmosphere (air-acoustic, infrasonic) or in the water (hydroacoustic). Seismic is the passive collection of vibrations in the earth. Magnetic and gravity include detection of perturbations to the earth's magnetic/gravity fields. Geophysics also involves electric and magnetic field measurements and caldera analysis[116].

[116] Caldera analysis is focused on the post-blast assessment of artillery craters or IED contacts with the aim of identifying the weapon system, ammunition nature or the emplacement tactics, techniques and procedures of improvised devices.

(4) **Electro-Optical.** Electro-optical MASINT sensors provide detailed information on the time-changing radiant intensities, dynamic motion, spectral characteristics, and the materials composition of a target. Data may be collected by a variety of optically sensitive devices, such as radiometers, spectrometers, non-imaging systems, lasers, and fibre optics.

(5) **Nuclear.** These sensors focus on detection, identification, and characterization of nuclear sources and events. Space-based nuclear radiation MASINT sensors monitor X-rays, gamma rays, and neutrons. Ground-based nuclear radiation sensors are able to monitor the movement of nuclear materials by tracking the radiation emitted by nuclear material.

(6) **Materials.** Material sampling systems involve analysis of chemical, biological, explosive, armour splash patterns[117], and other materials. Materials data may be acquired by air, ship-borne, or ground-based sensors, as well as by human-enabled physical collection.

(7) **Multispectral/Hyperspectral.** Multispectral and hyperspectral imaging sensors are typically imaging sensors that split the detected spectrum into many small bands. The usual distinction between multispectral and hyperspectral is that the multispectral sensors have between 4 and 99 bands, while hyperspectral sensors have between 100 and 999 bands. (Another term, ultraspectral, has been coined to define sensors with 1000 bands or more, but no practical sensor has yet been developed with that capability. Note also that normal three-band images are considered “colour” sensors since the bands are normally chosen to provide an image with colour representation similar to natural colour or pseudocoloured camouflage detection films.) The utilization of spectral information allows for more detailed analysis of the objects. In some cases, the material composition of the object can be identified. Detection of camouflage, concealment, or deception techniques is enhanced. The spectral information can also be used for crop analysis, both in terms of crop yield prediction and in detection of illicit crops. This type of foliage analysis can also be used for trafficability analyses by determining the type and extent of ground cover and the effects the foliage would have on wheeled or tracked vehicles.

(8) **Radar.** The radar sub-discipline involves active or passive collection of electromagnetic energy reflected from a target by line-of-sight, bistatic, or over-the-horizon radar systems. Radar data collection provides information on radar cross sections, tracking, precise measurements of components, size, shape, motion, radar reflectance, and absorption characteristics for targets or objects.

c. **MASINT in Operations.** Tasking for the MASINT sensors is based at the JTF level. Within J2, the Collection Manager is responsible for overseeing all MASINT sensor tasking. In some cases, the collection manager may delegate tasking authority to component command collection managers when the sensor is dedicated to support a component command requirement. In general, however, the tasking is issued from the joint level to

[117] The analysis of splash and fragmentation patterns on armour is used to determine the weapon system and ammunition nature used, the TTPs employed and the effectiveness of defensive measures.

ensure that all component commands have equal access to the capabilities. The collection manager is supported by a MASINT cell at the joint level to identify the best sensor to be given a specific task.

d. At the tactical level, available detectors will be battle enablers, allowing the unit to manoeuvre out of contact, launching operations at the most salient point and time. The commander will have full targeting and force protection sensor suites available to provide early indications and warning (I&W), and advanced tactical picture recognition. Tactical commanders and staffs will see the results of this MASINT system in a fully processed format on the systems displays. These results can be made available, as well as relevant products of national and theatre MASINT systems, to the fighting forces on the ground at the lowest echelon as possible.

e. At the operational level, MASINT will help in the timely delivery of intelligence support to improve situational awareness and further support JIPOE. The MASINT Desk analyst is tasked to provide inputs to the operations planning process and assist in managing the operating environment. Specific request for information can be provided or more general tasking can be assigned on a continuing basis.

f. At the strategic level, MASINT provides intelligence to policy makers to plan the overall operational objectives and strategy. In some cases different sensors are required than those used at the tactical level, but the requirement for integration still exists. In fact, many of the questions posed by policy makers will require the integrated deployment of multiple sensors to properly answer. For strategic analysis, the MASINT integration can be performed with a MASINT desk dedicated to supporting the Strategic planners. This can be accomplished by dedicating a NATO billet in the planning staff to a MASINT subject matter expert, or by temporary assignment of a national subject matter expert for the purpose of specific support to strategic planning.

5. Open-source intelligence (OSINT)

a. Open-source intelligence describes intelligence that is derived from publicly available information, as well as other unclassified information that has limited public distribution or access. It is derived from the systematic collection, processing, and exploitation of open source information, of any form, in response to intelligence requirements. Publicly available information includes any freely available information or material posted on Internet, published, broadcast (radio and television), or provided for general public consumption. Information of limited public distribution implies material that is commercially available to the public for a fee.

b. OSINT is a primary intelligence collection discipline, which utilizes publicly available information. It provides access to information useful for the production of all types of intelligence and much of the thus acquired information feeds PMESII methodology or ASCOPE/PMESII matrix for commanders to understand their operating environment (OE). Systematic collection, processing and analysis of publicly available information support answering IRs and the cross-cuing of other collection disciplines.

c. OSINT is a significant contributor to the joint intelligence preparation of the operating environment (JIPOE) process. OSINT is the predominant source of sociological and

cultural basic intelligence for JIPOE. It provides information and intelligence regarding the sociological and cultural environment, such as social and cultural perspectives, demographics, politics, and economics. It can also provide information on adversary leadership, capabilities, locations, and intentions. Additionally, OSINT is especially supportive in the following activities:

(1) Evaluation of operational effectiveness;

(2) Indications and warning of threats to the transition environment and to end-state security through exploitation of social media monitoring and other sources; and

(3) Enhance the cooperation with the non-NATO coalition forces and international or non-governmental organizations through the provision of releasable unclassified intelligence.

d. OSINT is a valuable discipline supporting and answering the commander's IRs. For example:

(1) In support of basic intelligence, OSINT can provide encyclopedic data and information on leadership, security, military, terrorism, international relations, economy, media, infrastructure, health, demographics, climate and geography. Information on international organizations, governmental agencies, and cultural and anthropological studies on potential operational areas can support the commanders understanding of the complex environments in which they will be operating. OSINT is also a useful tool for horizon scanning, early warning, and general information on all areas affecting and being influenced by cyberspace.

(2) In support of current intelligence, social media (SM) and live news feeds can be invaluable, allowing analysts to see or hear first-hand the evolving situation during a crisis.

(3) In support of psychological operations, OSINT provides cultural information as well as valuable insights concerning perceptions, intentions and capabilities that may influence decisions/actions of the target audiences and those in the local area.

(4) In support of trend analysis and assessing measures of effectiveness, social media networks provide a unique opportunity to learn how actors in the battle space are reacting to operations in the area; in particular, friendly operations.

(5) In support of the development of alternate scenarios, e.g. red teaming and alternative analysis[118], OSINT can provide access to authoritative thinking and opinions from academia, think tanks and strategic studies institutes.

(6) In support of Strategic Communications, OSINT provides valuable insight regarding the characteristics and nature of the Information environment.

e. **Advantages.** Availability, access, diverse information, language, ease of use, and widespread practice of the internet are some of the significant advantages of OSINT. It

[118] Red teaming and alternative analysis are techniques designed to help de-bias thinking, enhance decision making, and avoid surprise.

becomes the foundation when used in conjunction with other intelligence disciplines to provide a more complete answer to an intelligence problem. OSINT supports a broad-based understanding of the OE allowing for rapid orientation of the ongoing situation. It also allows the intelligence analyst to add context to higher classified material that may result in new assessments, or other avenues of inquiry for the intelligence problem. Data and information obtained by the OSINT specialist can be the only source of information or can pose a trigger for further requirements. Other advantages to OSINT exploitation are that it is generally less expensive than other collection disciplines, and can reduce demands on classified collection capabilities. OSINT may also generally be shared with a wider audience, including non-NATO elements.

f. **Disadvantages.** Open source information may contain inaccuracies, biased perspectives, irrelevant information and disinformation. Source verification helps to mitigate these issues, although it does not eliminate them completely. While it is easier not to follow proper operational security when “surfing the net”, this behaviour may result in unintentional exposure of friendly intelligence interests to adversaries and potential adversaries. OSINT searches can also result in a vast volume of information. Even with enough properly trained personnel, open source collection and processing therefore can be very labour-intensive and time-consuming. Finally, rapidly evolving internet and information technologies can quickly make existing collection technologies redundant. This issue can be mitigated with proper management of paid and free sources, although it may result in an increase in cost.

g. Intelligence units may have OSINT capabilities imbedded. IRM&CM staff should have an adequate understanding of specifics of OSINT activity. When the IRM&CM staff does not have the resources to collect the OSINT required they can request support from higher levels of command or dedicated agencies, or nations. Such reach-back support may be especially advantageous when in-depth collection and analysis are required.

h. Like any other intelligence collection, OSINT collection is determined by time, topic, scope and capabilities, i.e. available human resources and equipment. Upon receipt of collection tasks from the combined joint intelligence staff (CJ2), the OSINT collection team plans how to collect the required information, as the tools, procedures and time required to complete the collection will vary with the sources.

i. Factors that affect the OSINT collection plan include:

(1) Planning and allocation of resources for acquisition of printed publications or commercial subscriptions. This is a long-term and deliberate collection activity. Selection of material should be done in collaboration with analysts expected to use the sources. Renewal of contracts and subscriptions should likewise be a deliberate process.

(2) Analysis of the risks of bias, disinformation, and the likelihood that hostile intelligence services will track and identify our own open source collection efforts. The results of these risk assessments may drive the collection effort to use Internet services that are not attributable to NATO.

(3) Consideration of the time available and the type of information required to determine the breadth, depth, strategies and techniques of Internet searches.

(4) OSINT collection which targets a specific individual and risks the collection of private information is likely to require explicit authorization in accordance with national laws and policies.

6. Signals intelligence (SIGINT)

a. **SIGINT description and purpose.** Signals intelligence (SIGINT) is described as intelligence derived from electromagnetic signals or emissions. It is the generic term used to describe communications intelligence (COMINT) and electronic intelligence (ELINT) when there is no requirement to differentiate between these two types of intelligence, or to represent a fusion of the two. NATO SIGINT is comprised of COMINT and ELINT.

(1) COMINT is described as intelligence derived from electromagnetic communications and communication systems by other than intended recipients or users.

(2) ELINT is described as intelligence derived from electromagnetic non-communications transmissions by other than intended recipients or users.

b. SIGINT represents a prime source contributing to the intelligence requested in support of all NATO Crisis Management Process (NCMP) phases (Indications and warning (I&W), assessment of the crisis situation, developing response options, planning and execution) as well as for situational awareness, threat warning and cyberspace defence. Commanders at all levels in NATO should ensure that SIGINT contributions are taken into account during the planning and execution of operations, as well as during exercises.

c. **NATO SIGINT policy.** The Military Committee has established the NATO Advisory Committee on Signals Intelligence (NACSI) to develop SIGINT policy and doctrine. NACSI is composed of representatives from National SIGINT Authorities of member nations. “NACSI Nations” refer to the NATO Nations and Partner Nations that have agreed to contribute SIGINT to NATO and are member states or associated nations of NACSI. The aim of NATO SIGINT Policy is to provide NATO agreed, ratified and standardized guidance and a general framework for SIGINT. NATO SIGINT Policy does not supplant national constraints and is only applicable to the extent that it does not contradict or overrule national policy or individual national legislation.

d. **Role of SIGINT.** SIGINT supports military and strategic decision-making. The support to military operations continues to be a primary goal of NATO SIGINT. SIGINT provides intelligence on threat capabilities, disposition, composition, and intentions. In addition, SIGINT can improve the safety and effectiveness of NATO and allied forces in military operations.

e. **SIGINT fundamentals.** It is imperative that the commander and intelligence staff understand how joint SIGINT assets are organised and their capabilities. SIGINT assets as a rule are located at the JTF level and above. NATO assigned SIGINT assets combined with national SIGINT assets, work together to support commanders from the tactical to the strategic level. Only by understanding the SIGINT structure that transcends component command’s boundaries the commander and intelligence staff will know how to use SIGINT effectively.

f. **SIGINT planning.** SIGINT collection can be employed independently. However, when feasible SIGINT should be employed in conjunction with another intelligence collection discipline.

g. **SIGINT support to intelligence cycle.** SIGINT follows what is referred to as the SIGINT process which complements the overarching intelligence cycle. The requirement for its completion is dictated by the time criticality of the information and the required level of detail:

(1) Direction and Requirements. SIGINT supports the direction phase of the intelligence cycle through intelligence requirements to be filled by SIGINT results and the respective SIGINT requests for information (RFIs);

(2) Collection. NATO has no organic SIGINT collection capabilities and thus is dependent on the support of NACSI Nations (or other cooperating nations). NATO has no authority to directly task a nation to collect SIGINT. SIGINT collection will be conducted by individual NACSI Nations in accordance with their respective national laws;

(3) Processing. NACSI Nations, as well as their personnel assigned to NATO SIGINT positions, provide analytic and reporting efforts on behalf of NATO;

(4) Dissemination. Timely dissemination of the SIGINT results is critical to its relevance. Transmission of SIGINT reports will only be via systems accredited for the appropriate classification level.

h. **Security of NATO SIGINT.** The highest standards of personnel, physical and information security must be applied when dealing with SIGINT. The NATO Office of Security (NOS) is responsible for all security directives dealing with classified information up to and including COSMIC Top Secret (CTS); NACSI is responsible for any additional security guidance in accordance with policy set in MC 0101. To protect the sensitivity of CTS-B information an additional indoctrination process has been set forth in MC 0101. With regard to the NATO Emitter Database (NEDB) which contains parametric and related information on electromagnetic emitters, the security regulations are laid out in NEDB manual 1, Section 7 and STANAG 6009. Any release of data from NEDB is strictly controlled by the submitting nation.

i. **SIGINT support to NATO operations**. SIGINT contributes to gaining information superiority through the provision of actionable intelligence on validated targets of interest. This empowers decision makers and military leaders at all levels with situational awareness and understanding for the decision making process and to determine appropriate actions. This can be achieved through SIGINT contribution to:

- Situational awareness and understanding;
- Indicators and Warning;
- Cyberspace defence;
- Force protection;
- Joint intelligence preparation of the operating environment;
- Battle damage assessment;

- Operations assessment.

j. While the SIGINT support to operations as listed above are used in the full spectrum of NATO operations, the focus is set to the mission profile and can shift during the different phases of the operation.

ANNEX B - SOURCES AND SENSORS, DATA AND INFORMATION, JISR RESULTS AND ALL-SOURCE-INTELLIGENCE, INFORMATION THEORY

Different levels of information refinement are described as being part of an information hierarchy, an information theory. This is commonly described as the progression from data through information to knowledge and wisdom.

Data are the smallest components of the information hierarchy. They are commonly presented as discrete facts or simple products of observation. A single piece of data, datum, often has little meaning in isolation. Examples of data are the speed, altitude and or emitter values of an object moving through the air that is detected, calculated and presented by a radar system.

Information is data arranged to convey meaning. It might be thought of as “data + meaning”. Information is often constructed by combining different data points into a meaningful picture, given certain context. Information is a continuum of progressively developing and clustered data; it answers questions such as “who”, “what”, “where”, and “when”. An example of information would be the data above combined into a whole and provided with additional meaning through comparison of the emitter values to emitter libraries.

JISR results in information theory normally fall into the categories data and or information. JISR results are results of directed collection and consist of data and information, that is exploited by certain specialists (mostly inside one intelligence collection discipline).

Intelligence is the fused product used to satisfy Intelligence requirements (IR) of the commander. In information theory intelligence falls into the category of knowledge. It is information that has been synthesized so that relations and interactions are defined and formalized; it is built of JISR results and meaningful information constructed of discrete data points. It is derived by discovering patterns of relationships and confirmations between independent results of different intelligence collection disciplines as well as different clusters of information and data. Intelligence is based on all available data, information and JISR results that are relevant to satisfy an IR and answers also the questions of “why” or “how”. The fusion of all available data, information and JISR results into all-source intelligence will increase the commander’s understanding of the operating environment and improve his decision-making. An example would be bringing the information above into context through comparing it to known actors and their capabilities, tactics, intentions and standard behaviour, the reasons behind this behaviour, an estimate or prediction to the future behaviour and an advice or recommendation to the user of intelligence.

Within a military context, understanding is the perception and interpretation of a particular situation to provide the context, insight and foresight required for effective decision-making. Intelligence contributes to a continuous and coordinated understanding of the operating environment, supports commanders by identifying conditions required to achieve desired objectives; contributes to avoiding undesired effects; and assessing the impact of adversary, friendly and neutral actors on the commanders’ concept of operations. Understanding (of the OE) is based on a large variety of intelligence products, JISR results, information and data.

Wisdom is, in information theory context, regarded as being the appropriate use of described levels in Figure 7 below to manage situations effectively and in accordance with the goals and ethics set up by the organization. An example of applied wisdom would be the ability of a commander on how to handle the unfolding situation, taking into account likely future actions from the relevant actors involved as well as their likely reactions to our actions.

The boundaries between the information theory levels are not strict; rather, they are interrelated and there is a “constant flux” between them. Simply put, data is used to generate information and knowledge while the derived new knowledge coupled with wisdom, might trigger assessment or reassessment of existing data or information.

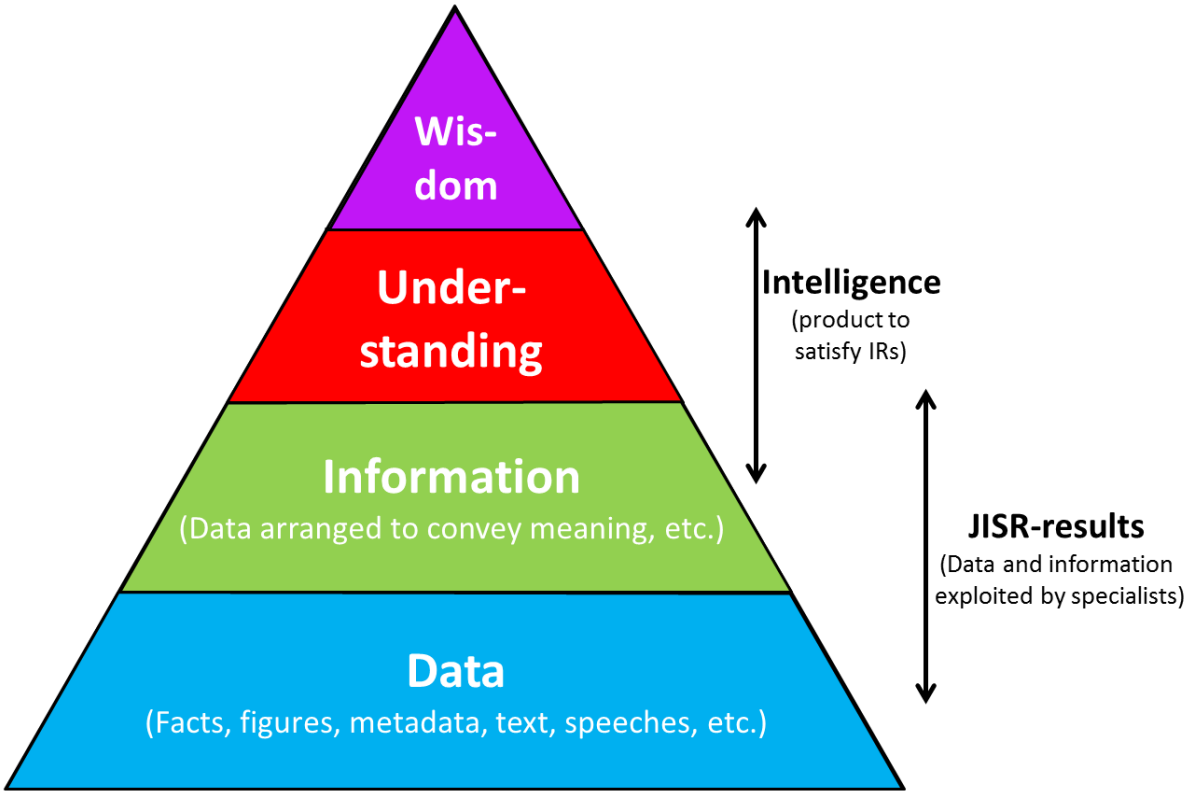

Figure 7. Data, information, JISR results, intelligence and understanding in information theory

LEXICON

Part I – LIST OF ACRONYMS

AAP	Allied administrative publication
ACINT	acoustic intelligence
ACO	Allied Command Operations
AIntP	Allied intelligence publication
AII	area of intelligence interest
AIR	area of intelligence responsibility
AJP	Allied joint publication
AOO	area of operation
ASCOPE	areas, structures, capabilities, organizations, people and events
ASG-I&S	Assistant Secretary General for Intelligence and Security
ASIC	all-source intelligence cell
BDA	battle damage assessment
BEI	biometrics-enabled intelligence
C-IED	countering improvised explosive devices
CBRN	chemical, biological, radiological and nuclear
CCIR	commander's critical information requirement
CI	counter-intelligence
CICA	counter-intelligence coordinating authority
CIMIC	civil-military cooperation
CIS	communication and information systems
CJSOR	combined joint statement of requirements
CM	collection management
COMINT	communications intelligence
DOTMLPFI	doctrine, organisation, training, materiel, leadership development, personnel, facilities, and interoperability
EEI	essential elements of information
EEFI	essential elements of friendly information
ELINT	electronic intelligence

EMP	electromagnetic pulse
EO	electro-optical
FFIR	friendly forces information requirement
FHT	field human intelligence team
GEOINT	geospatial intelligence
HOC	human intelligence operations cell
HQ	headquarters
HUMINT	human intelligence
I&W	indications and warning
ICP	intelligence collection plan
IFC	intelligence fusion center
IMINT	imagery intelligence
INTREP	intelligence report
INTSUM	intelligence summary
IR	intelligence requirement
IRM	intelligence requirements management
IRM&CM	intelligence requirements management and collection management
ISB	Intelligence Steering Board
ISR	intelligence, surveillance and reconnaissance
JIPOE	joint intelligence preparation of the operating environment
JISD	Joint Intelligence and Security Division
JISR	joint intelligence, surveillance and reconnaissance
JOA	joint operations area
MASINT	measurement and signature intelligence
MC	Military Committee
METOC	meteorological and oceanographic
MOE	measure of effectiveness
MOP	measure of performance
MP	military police
NAC	North Atlantic Council
NACSI	NATO advisory committee on signals intelligence
NATO	North Atlantic Treaty Organization
NCIA	national counter-intelligence adviser
NCIR	national counter-intelligence representative
NEDB	NATO Emitter Database

NGO	non-governmental organization
NIC	national intelligence cell
NIFC	NATO intelligence fusion center
OE	operating environment
OPSEC	operations security
OPP	operations planning process
OSINT	open-source intelligence
PED	processing, exploitation and dissemination
PIR	priority intelligence requirement
PMESII	political, military, economic, social, infrastructural and informational
PsyOp	psychological operation
RF	radio frequency
RFI	request for information
SIGINT	signals intelligence
STANAG	NATO standardization agreement
SUPINTREP	supplementary intelligence report
TCPED	task, collect, process, exploit, disseminate
TECHINT	technical intelligence
TESSOC	terrorism, espionage, subversion, sabotage, organized crime
WMD	weapon of mass destruction

Part II – Terms and Definitions

acoustic intelligence (ACINT)
Intelligence derived from the collection and processing of acoustic phenomena.
(NATO Agreed)

Actor
In intelligence usage, 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 has been 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 interest (AII)
A geographical area for which a commander requires intelligence on the factors and developments that may affect the outcome of operations.
(NATO Agreed)

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

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

Note: As a matter of principle basic intelligence is fused from all available data, information, JISR results, single-source intelligence and all-source-intelligence and is fundamental to current intelligence.

battle damage assessment (BDA)
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 requirement (CR)
A validated information requirement, for which the requested information is not already available in a repository and therefore requires collection through joint intelligence, surveillance and reconnaissance asset tasking or will be forwarded as a request to higher or adjacent commands.
(This term is a new term and definition and has been processed for NATO Agreed status.)

communications intelligence (COMINT)
Intelligence derived from electromagnetic communications and communications systems.
(NATO Agreed)

computer network attack (CNA)
Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself.
Note: A computer network attack is a type of cyberspace attack.
(NATO Agreed)

counter-intelligence (CI)
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.
(NATO Agreed)

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

cyberspace ISR
Intelligence, surveillance and reconnaissance conducted within cyberspace to collect data and information in order to achieve results that contribute to or can be processed to intelligence.
Note: These data and information may be collected within computer network operations (CNO) by computer network exploiters from sources that are not publicly available. In this case the methods of computer network operations are used to obtain data and information. CNO-specialists collect and exploit these data and information to establish respective results.
(This term and definition only applies to this publication.)

deception
Deliberate measures to mislead targeted decision-makers into behaving in a manner advantageous to the commander's objectives.
(This term and definition modifies an existing NATO Agreed status.)

electronic intelligence (ELINT)
Intelligence derived from electromagnetic non-communications transmissions.
(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)

geospatial intelligence (GEOINT)
Intelligence derived from the combination of layered geospatial information with other intelligence data, products and layers.
Note: The layered geospatial information is quality assured.
(This term and definition modifies an existing NATO Agreed status.)

hostile
In identification, the designation given to a track, object or entity whose characteristics, behaviour or origin indicate that it is threat to friendly forces. Designation as hostile does not necessarily imply clearance to engage.
(NATO Agreed)

human intelligence (HUMINT)
Intelligence derived from information collected by human operators and primarily provided by human sources.
(NATO Agreed)

hybrid threat
A type of threat that combines conventional, irregular and asymmetric activities in time and space.
(NATO Agreed)
imagery intelligence (IMINT)

Imagery intelligence is intelligence derived from imagery acquired from sensors which can be ground-based, sea borne or carried by air or space platforms.
(NATO Agreed)

Indicator
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.
(NATO Agreed)

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

information activities (IA)
Actions designed to affect information or information systems. Note: Information activities can be performed by any actor and include protection measures.
(NATO Agreed)

integration
In intelligence usage, a step in 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)
Note: The term is also applied to the activity which results in the product and to the organizations engaged in such activity.

intelligence collection disciplines
Means or systems used to observe, sense, and record or convey information of conditions, situations, threats and events.
(This term and definition only applies to this publication.)

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

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

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

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

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

(NATO Agreed)

intelligence requirement
A requirement for assessed information about any aspect of a situation needed to develop a commander's understanding.
(This term is a new term and definition and has been processed for NATO Agreed status.)

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)

intelligence requirements management and collection management (IRM&CM)
A set of integrated management processes and services to satisfy the intelligence requirements by making best use of the available collection, processing, exploitation, dissemination (PED) and processing capabilities.
(This term is a new term and definition and has been processed for NATO Agreed status.)

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

joint intelligence, surveillance and reconnaissance (JISR) asset
A detachment, unit, sensor, or platform, which can be tasked by respective authorities to achieve joint intelligence, surveillance and reconnaissance results.
(This term is a new term and definition and has been processed for NATO Agreed status.)

joint intelligence, surveillance and reconnaissance (JISR) capability
An asset supported by organizations, personnel, collectors systems, supporting infrastructure, processing, exploitation and dissemination (PED) processes and procedures to achieve a designated joint intelligence, surveillance and reconnaissance JISR result.
(This term is a new term and definition and has been processed for NATO Agreed status.)

joint intelligence, surveillance and reconnaissance (JISR) process
A coordination process through which intelligence collection disciplines, collection capabilities and exploitation activities provide data, information and single source intelligence to address an information or intelligence requirement, in a deliberate, ad hoc or dynamic time frame in support of operations planning and execution. The joint intelligence, surveillance and reconnaissance (JISR) process consists of five steps: Task, Collect, Process, Exploit and Disseminate, referred to as task, collect, process, exploit and disseminate (TCPED).
(This term is a new term and definition and has been processed for NATO Agreed status.)

joint intelligence, surveillance and reconnaissance result (JISR result)
The outcome of the intelligence, surveillance and reconnaissance process disseminated to the requester in the requested format.
(This term is a new term and definition and has been processed for NATO Agreed status.)

measure of effectiveness (MOE)
A criterion used to assess changes in system behaviour, capability, or operational environment, tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.
(NATO Agreed)

measure of performance (MOP)
A criterion to assess friendly actions that is tied to measuring task accomplishment.
(NATO Agreed)

measurement and signature intelligence (MASINT)
Intelligence derived from the scientific and technical 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.
(NATO Agreed)

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

open-source intelligence (OSINT)
Intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access.
(NATO Agreed)

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

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

operational level
The level at which campaigns and major operations are planned, conducted and sustained to accomplish strategic objectives within theatres or areas of operations.
(NATO Agreed)

operations security (OPSEC)
The process that gives a military operation or exercise appropriate security, using passive or active means, to deny an adversary knowledge of the essential elements of friendly information (EEFI), or indicators of EEFI.
(This term and definition modifies an existing NATO Agreed status.)

organized crime
Any enterprise, or group of persons, engaged in continuing illegal activities which has as its primary purpose the generation of profits, irrespective of national boundaries.
(This term and definition only applies to this publication.)

protective security
The organized system of defensive measures instituted and maintained at all levels of command with the aim of achieving and maintaining security.
(NATO Agreed)

psychological operation (PsyOp)
Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour affecting the achievement of political and military objectives.
(NATO Agreed)

reach-back
Reach-back provides products, services, applications, capabilities or material from commands, agencies and facilities that are not deployed and available in the area of operation.
(This term and definition only applies to this publication.)

reconnaissance (RECCE)
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, hydrographic or geographic characteristics of a particular area.
(NATO Agreed)

sabotage
Acts falling short of a military operation, or any omission, intended to cause physical damage in order to assist an adversary or to further a subversive political objective.
(This term is a new term and definition and has been processed for NATO Agreed status.)

scientific and technical intelligence
Intelligence concerning foreign developments in basic and applied scientific and technical research and development including engineering and production techniques, new technology, and weapons systems and their capabilities.
(This term is a new term and definition and has been processed for NATO Agreed status.)

security
The condition achieved when designated information, materiel, personnel, activities and installations are protected against terrorism, espionage, subversion, sabotage, organized crime or computer network attacks and damage, as well as against loss or unauthorized disclosure.
(NATO Agreed)

security intelligence (SI)
Intelligence on the identity, capabilities and intentions of hostile organizations or individuals who are or may be engaged in terrorism, espionage, subversion, sabotage, organized crime.
(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)

signals intelligence (SIGINT)
Intelligence derived from electromagnetic signals or emissions. Note: The main subcategories of signals intelligence are communications intelligence and electronic intelligence.
(NATO Agreed)

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

strategic communications (StratCom)
In the NATO military context, the integration of communication capabilities and information staff function with other military activities, in order to understand and shape the information environment, in support of NATO strategic aims and objectives.
(NATO Agreed)

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

strategic level
The level at which a nation or group of nations determines national or multinational security objectives and deploys national, including military, resources to achieve them.
(NATO Agreed)

subversion
Action or a coordinated set of actions of any nature intended to weaken the military, economic or political strength of an established authority by undermining the morale, loyalty or reliability of its members.
(NATO Agreed)

surveillance
The systematic observation of aerospace, surface or 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)

tactical level
The level at which activities, battles and engagements are planned and executed to accomplish military objectives assigned to tactical formations and units.
(NATO Agreed)

target (Tgt)
An area, structure, object, person or group of people against which lethal or non-lethal capability can be employed to create specific psychological or physical effects. Note: The term 'person' also covers their mindset, thought processes, attitudes and behaviours.
(NATO Agreed)

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

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

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

terrorism
The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives.
(NATO Agreed)

understanding
Interpretation and comprehension of a particular situation in order to provide the context, insight and foresight required for effective decision-making.
(This term is a new term and definition and has been processed for NATO Agreed status.)

AJP-2(B)(1)