NATO STANDARD

AJP-2

ALLIED JOINT DOCTRINE FOR INTELLIGENCE, COUNTER-INTELLIGENCE AND SECURITY

Edition A Version 2
FEBRUARY 2016

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

22 February 2016

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

3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.

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

Dieter Schmaglowski
Deputy Director NSO
Branch Head P&C

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1 PREFACE

1.1 GENERAL

1. Sun Tzu stated that *if ignorant both of your enemy and yourself, you are certain to be in peril.*[1] This situation has remained unchanged throughout history. Indeed, success in military operations is dependent upon the provision of timely intelligence that is of a better quality than that of the adversary. The merging of this intelligence with knowledge of our own capabilities, and that of our allies, provides the foundation for planning and operational execution.

Therefore, today's intelligence is not only about cataloguing an adversary's military forces and assessing their capability. It is also about understanding the adversary's culture, motivation, perspective and objectives. Moreover, recent operations have shown that the intelligence staff should consider not only the adversary, but also assess the population to determine the degree of support that segments of the population will provide to the adversary or to friendly forces. Consequently, modern intelligence is a particularly complex activity that has to consider a myriad of hybrid adversaries and threats.

2. AJP-2(A) considers intelligence, counter-intelligence and security in the modern era where state-versus-state conflict is still possible, but where future NATO operations are likely to be completed in an operational environment that is congested and contested using unconventional tactics and supported by better technical connectivity. AJP-2(A) provides a clear understanding of the critical importance of intelligence and counter-intelligence during operations, particularly those conducted in multinational or coalition environments.

1.2 PURPOSE

1. The aim of AJP-2(A) is to explain intelligence and counter-intelligence in order to optimize their contributions to operations. This general framework should facilitate a common understanding of the intelligence functions throughout all levels of NATO, partner nations and other joint force compositions.

2. Primarily written for commanders and their staff at the operational level, AJP-2(A) is also the principal reference document for intelligence specialists and is the doctrinal baseline to develop effective intelligence, counter-intelligence and security

[1] Sun Tzu, The Art of War, Samuel B. Griffith trans, Oxford University Press 1963

training. Furthermore, it provides an explanation of NATO intelligence functions to those external to NATO. This doctrine expands on NATO Intelligence Policy.[2]

3. The main difference between AJP-2 and AJP-2(A) is the change of focus resulting from the change from state-versus-state conflict to multiple smaller scale intervention and counterinsurgency operations. It considers the more complex operational environment and the increasing number of factors that affect contemporary intelligence operations. It reflects the increasing intelligence capability within NATO and the advent of the comprehensive approach. AJP-2(A) also introduces the Joint Intelligence, Surveillance and Reconnaissance Concept[3] and a revision of NATO intelligence requirement management and collection management (IRM&CM) functions.

4. The application of this doctrine will facilitate a single intelligence environment within which intelligence structures across the Alliance interface and operate in collaboration to support decision-makers at all levels.

1.3 CONTENT

AJP-2(A) is divided into 8 chapters:

a. Chapter 1 outlines the content of AJP-2(A) and explains the purpose of the publication.

b. Chapter 2 explains the context for intelligence in the contemporary environment and considers its pivotal contribution to operations.

c. Chapter 3 considers the fundamentals of intelligence.

d. Chapter 4 outlines the Intelligence Cycle which is the foundation of the intelligence process.

e. Chapter 5 explains the importance of intelligence requirements management and collection management within the intelligence process.

f. Chapter 6 considers joint intelligence planning.

g. Chapter 7 introduces concepts of security.

h. Chapter 8 explains counter-intelligence within NATO.

---

[2] NATO Intelligence Policy is contained in MC 0128/8 dated 13 Jan 12.

[3] MC 0582, 09 July 2009

1.4 TERMINOLOGY

1. AJP-2(A) uses the terminology from AAP-6 whenever possible. Throughout the document, four generic terms are used:

a. **Commander**. The commander is the authority, at any level, who requires the intelligence to make decisions.

b. **Intelligence Staff**. Intelligence staffs are those personnel who are involved in the direction, collection, production and dissemination of intelligence through the conduct of the intelligence process.

c. **Gender**. The term “he” in this document refers to both genders and is used indiscriminately.

d. **Actor**. The term actor is used in this document to refer to *a person or organization, including state and non-state entities, within the international system with the capability or desire to influence others in pursuit of its interest and objectives*.

1.5 RELATED DOCUMENTS

1. AJP-2(A) is intended to be read with NATO Joint Capstone Doctrine, Allied Joint Doctrine (AJP-01) and it complements other doctrinal joint keystone documents (e.g. AJP-3 and AJP-5).

2. It is impossible to capture all complexities of modern intelligence in a single document. Therefore, AJP-2(A) is the keystone doctrine in a series of intelligence documents that expand in detail the themes within this document within a number of specializations. The diagram below illustrates the architecture of doctrinal intelligence documents.

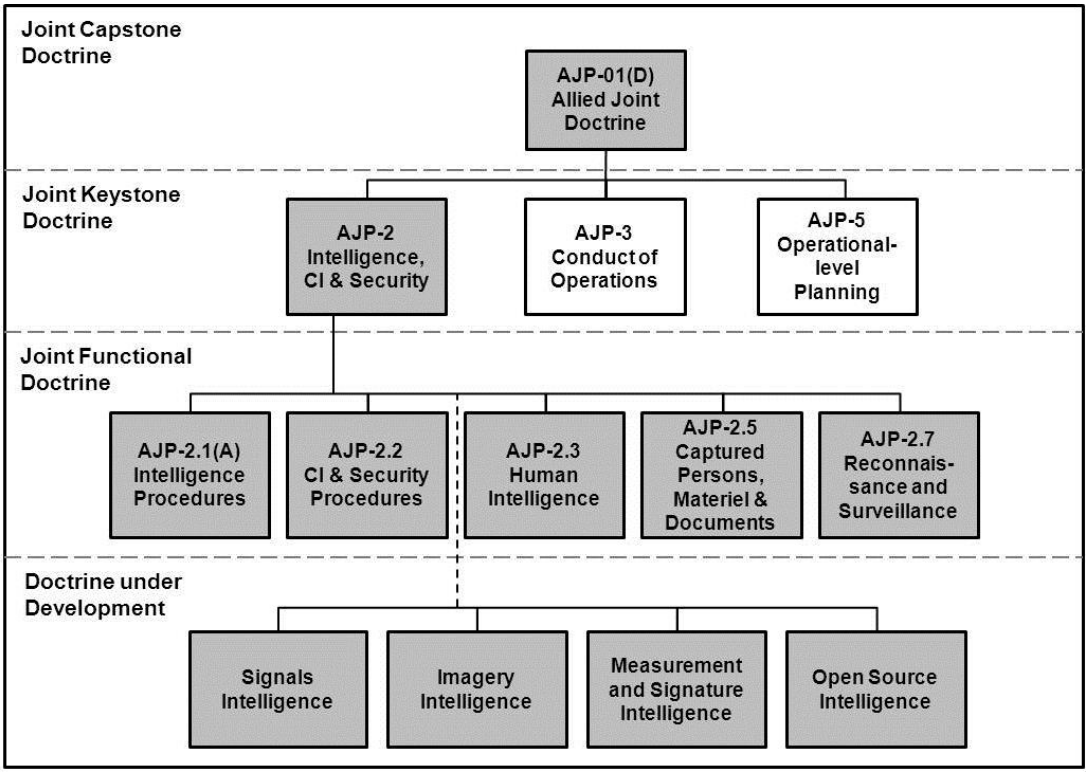

Figure 1: The Place of Intelligence Doctrine within NATO Joint Doctrine Architecture

1.6 CUSTODIANSHIP

1. The custodianship of AJP-2(A) is held by Germany, Strategic Reconnaissance Command, Concepts and Development Branch, kdostrataufklwe@bundeswehr.org (unclassified) or cdint@src.deu.bices.org (classified).

CHAPTER 2 CONTEMPORARY INTELLIGENCE

2.1 INTRODUCTION

1. Intelligence provides more than a tool for counting the forces of adversaries or assessing their preparedness to apply capabilities to create lethal effects. Intelligence is an enabling capability whose value is largely realized when conducting planning and operations. This Chapter will consider the context within which intelligence functions occur and the factors that affect intelligence in the contemporary environment. Finally, it will consider the role of the commander and the intelligence contribution to operations.

2.2 CONTEXT OF THE CONTEMPORARY OPERATIONAL ENVIRONMENT

1. Current operational complexities require commanders to regard intelligence as a critical prerequisite for operations rather than simply a means of determining the obstacles to achieving a mission. At the same time, the intelligence community should consider a greater number of actors, an increasing number of intelligence support systems, a wider range of intelligence requirements and larger numbers of collection capabilities.

2. **Key Actors and Threats**. NATO may be required to face complex and challenging operational environments where defined actors and threats are:

a. **Terrorism**. Terrorism is the unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives.[4]

b. **Hostile States**. Hostile states are those states characterized by enmity or ill will towards the NATO, its allies or the balance of international order. Hostility can be either open (verbal or violent aggression or belligerence) or disguised and can be conducted by proxy.

c. **Fragile and Failing States**. States that cannot adapt to the changing global framework risk failure and collapse accompanied by substantial outbreaks of violence. Poor governance, economic deprivation and inequality that characterizes fragile, failed and failing states is likely to spread to neighboring states.

[4] Allied Administrative Publication (AAP)-06(2015) the *NATO Glossary of Terms and Definitions*

d. **Hybrid Threats**. Hybrid threats occur where conventional, irregular and asymmetric threats are combined in the same time and space.[5] Conflict could involve a range of trans-national, state, group and individual participants operating both globally and locally. Some conflicts may involve concurrent inter-communal violence, terrorism, cyberspace attacks, insurgency, pervasive criminality and widespread disorder.

e. **Globalization**. In certain areas, instability may be created by the need of a nation to acquire or protect food, water and energy supplies. This situation is likely to be exacerbated by the continuing internationalization of markets for goods, capital, services and labor, which integrates geographic dispersed consumers and suppliers.

f. **Environmental and Humanitarian**. Unpredictable natural phenomena can cause major environmental disasters such as, floods, droughts, earthquakes and tsunamis 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.

g. **Proliferation**. The proliferation of ballistic missiles, nuclear weapons and other weapons of mass destruction, 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 UN Security Council Resolutions (e.g., illicit conventional arms). Of particular concern is the likelihood that proliferation will be most acute in some of the world's most volatile regions.

3. **The Requirement for Intelligence**. 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 operational environment. This relies upon geospatial, cultural and linguistic capabilities for information collection and the subsequent processing into intelligence and dissemination. There is an increasing need for contextual intelligence that draws upon a wide range of sources and a comprehensive understanding of the operational environment.

2.3 FACTORS AFFECTING INTELLIGENCE

1. Within the context of the contemporary operational environment, intelligence staffs will be affected by a number of factors that will influence the way they operate.

[5] Asymmetric threats are those 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 (AAP-06(2015)).

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 staff operate. For example, the nature of adversaries may be different in the contemporary operational environment in that they may have no fixed infrastructure, uniforms and tangible military assets or they may operate in cyberspace. In addition, intelligence methods should change to reflect the greater availability of data, the growing sophistication of intelligence capabilities and the impact of network capability on working practices.

b. **Information Abundance**. Information in today's world exists in overabundance and makes it difficult to direct limited resources to focus in the appropriate areas in a timely manner. Therefore, NATO's ability to find and manage relevant information quickly will be critical. This will require 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 timely and reliable intelligence in its correct context will become the defining feature of an intelligence architecture. Consequently, commanders at all levels will need to ensure that they have adequate structures in place providing effective intelligence requirements management in order to mitigate information saturation and overload.

c. **Fading of Traditional Boundaries**. In contemporary operations, the traditional boundaries between the levels of warfare (strategic, operational and tactical) have less relevance in relation to intelligence. Enhanced collection capabilities and better communications have resulted in tactical commanders often having instant access to strategic intelligence, while tactical intelligence often carries strategic ramifications.

2.4 THE COMPREHENSIVE APPROACH

1. Complex crises do not lend themselves to simple definition or analysis. Each instrument of power contributes distinct professional, technical, and cultural disciplines, together with discrete values and perceptions, which offer additional perspectives, depth, and resilience. Sharing respective situational understanding between parties, including the military, can therefore increase the effectiveness of their various capabilities. So contributing to a comprehensive approach requires JFCs to be predisposed to sharing their understanding of a situation and its dynamics. This approach should aid the implementation of any agreed collective goals, leading in turn

to the implementation of mutually supporting activities. Wherever possible, JFCs should exchange respective assessments and liaison with in-theater counterparts.

2. To contribute to this comprehensive approach, intelligence staffs should be able to produce intelligence based on a wide range of factors. Intelligence staffs will need to reach-out for expertise (e.g. scientific expertise) to support their analysis or they may need to rely on reach-back to supporting 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.[6]

3. Intelligence Relationship with Knowledge Development (KD)[7]. Within the comprehensive approach, KD is the staff-wide process across all command levels to develop comprehensive situational awareness and understanding of the operational environment and make it available to civilian officials and military leaders to support decision-making throughout the NATO Crisis Management Process. A KD capability is required to support situational awareness, planning, execution and assessment of operations within a comprehensive approach. This is achieved by relevant military and non-military information being acquired, integrated and analyzed across all pertinent inter-related systems. Intelligence will often provide the majority of information used for this process or provide key inputs, which will be combined with information from other parts of the staff and even non-NATO actors in the development and maintenance of comprehensive understanding. Additionally intelligence can be used to validate KD products, as well as to raise further information requirements as gaps are identified. Through continuous review, both intelligence and KD benefit from the maintenance of understanding. Although KD is not an intelligence function, the intelligence staffs make a significant contribution to KD.[8]

2.5 UNDERSTANDING

1. Within a military context, understanding is the perception and interpretation of a particular situation in order to provide the context, insight and foresight required for effective decision-making.[9] This includes answering the main questions of who, what, where, when, why and how, which provides the context and narrative of events. In turn, this informs the application of military power to achieve strategic objectives by enabling commanders to develop and maintain a global view.

---

6 AJP-3(B), Chapter I, Section II, Para 0104.

7 Knowledge Development" is not covered by AAP-06(2015), but is described as a staff-wide process in [e.g. MC 600]

8 Some nations do not use KD as a construct or named concept but refer to it with a different name (e.g. "Sharing Knowledge to Create Shared Understanding").

9 This is a new definition proposal which is awaiting NATO approval.

2. 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. Accessing information and processing it into intelligence is, by its very nature, a multi-agency and multisource activity. The approach should be sufficiently inclusive, flexible and adaptive to accommodate a wide range of experts, both within and external to the formal NATO structure. Such experts may hold the key to understanding within the contemporary operational environment.

3. Situational Awareness. Situational awareness is the general term used when a decision-maker at any level has the right level of understanding and skills required to put new data and information into context to make rational decisions and actions. Basic intelligence provides inputs to the learning process to create understanding and knowledge of the operational environment as well as inputs to realistic training scenario to reach the required level of skills.

2.6 DATA AND INFORMATION

1. Information may consist of a single item of data or a group that has been collected by sensors or other means. Information may or may not be accurate and relevant to the required intelligence picture.[10] In this respect, information is merely an assemblage of collected data, which may or may not be valuable, accurate or even pertinent. Within the intelligence community, information is defined as *unprocessed data of every description, which may be used in the production of intelligence*.[11] In this context, information may or may not become relevant as the end-result after the processing phase of the Intelligence Cycle.

2. Commanders and their staff receive a tremendous amount of information relating to every aspect of their operational environment. Much of this information is factual reporting pertaining to the operational status of friendly forces and elements. However, a considerable amount of this information will be less reliable, fragmented and gleaned from sources where the ability to verify its authenticity and accuracy is either severely limited or impossible. This is particularly the case for information that deals with adversary forces and elements, their intentions and their capabilities.

[10] The term data refers to facts and statistics collected for reference or analysis.
[11] AAP-06(2015)

2.7 THE COMMANDER, INTELLIGENCE AND DECISION-MAKING

'*Creating effective intelligence is an inherent and essential responsibility of command*.' [12]

1. At all levels, the relationship between the commanders and their staff is critically important for effective decision-making. The commander provides the leadership, judgment and energy to focus the staff and the forces under his command towards the goal of achieving the mission.

2. **Commander's Intelligence Responsibilities**. The ultimate responsibility for intelligence rests with the commander. Commanders are the key players in the planning and conduct of intelligence operations. 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 the commander's responsibility to provide direction and guidance, to define priorities, to resource intelligence collection and analysis effectively, to demand the highest standard of products and to review the effects of his chosen actions.

3. **The Commander and Decision-Making**. Intelligence products assist in understanding a specific subject, person or event. This understanding is used by the commander to make intelligence-based decisions. However, effective decision-making is an art that is part nature and part nurture. A good commander knows that:

a. There is both a correlation and a dependency between quality and timeliness, and that some risks are inevitable.

b. Commanders must not delegate their decisions unless there are exceptional circumstances. They should delegate authority to subordinate leaders so that they may exercise initiative and act aggressively and independently to accomplish the mission.

c. Good decisions come with training and experience.

d. The staffs assist the commander to make decisions and this requires mutual trust and confidence in one another.

Effective decision-making combines judgment with information; it requires knowing if to decide, when to decide, and what to decide. Timeliness is the speed required to maintain the initiative over the adversary. Decision-making is both art and science.

[12] Taken from *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Major General M T Flynn, January 2010.

4. **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.

5. **Commander's Intent.** Intent is the commander's clear and concise expression of what the force must do and the conditions the force must establish to accomplish the mission. It is a succinct description of the commander's visualization of the entire operation and what the commander wants to accomplish.

6. **Promoting Access to Intelligence.** A challenge for the commander is to focus the intelligence effort and to achieve timely dissemination. 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. It implies all individuals, groups and agencies are working together collaboratively to achieve a common objective. Therefore, access to intelligence capabilities to support mission requirements should be prioritized by need and not be restricted by organizations or command configurations. If higher priority or competing tasks affect optimization of intelligence activities, the commander should make alternative provision from within his assigned resources or request assistance from other agencies through his chain of command.

7. **The Command Climate**. Commanders should create an atmosphere that allows open-mindedness, critical analysis and creative thinking. Trust is a two-way process and the command climate should enable key staff to tell the commander what he needs to know, even if it contradicts his own view. The relationship and trust developed between commanders and their staff is a critical component of operational success. There are numerous examples throughout history where the breakdown of this relationship has led to operational failure. Failure in this context is generally attributed to either a failure of intelligence or a failure of command, but in reality it is often a combination of both.

2.8 INTELLIGENCE SUPPORT TO COMMANDERS

1. **Support to Strategy Formulation**. Intelligence plays a significant role in the development of military strategy. This role is largely defined within the context of identifying adversarial capability and intent, but includes assisting in the articulation of an end-state, goals, objectives and an appraisal of the resources needed.

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

2.9 INTELLIGENCE CONTRIBUTION TO OPERATIONS

1. The aim of this section is to outline the fundamental intelligence contribution to operations.[13] An effective contribution to operations is based on the production of focused intelligence that supports decision-making related to operational-level planning, preparation and execution.

a. **Contribution to Contingency Planning**. 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 Operational-Level Planning**. The designated operational commanders and planning staffs require intelligence assessment on all aspects of the adversary and the operational environment of the mission area. This intelligence contributes to mission analysis and provides commanders with an understanding of threats and challenges that will be faced during force employment. Further, it assists commanders in determining the optimum composition of forces required to achieve 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 on the adversary and the operational 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 allows the commander to conduct his decision-making based on a comprehensive understanding of the situation. It helps to both frame problems and

[13] AJP-2.1(A) contains detailed guidance on the contribution of intelligence to operations.

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 operational environment within which they operate. In contemporary operations the intelligence staff should provide the commander with:

(1) Intelligence that locates a target and indicates its vulnerability and relative importance.[14] 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 the commander's objectives, including information operations.[15]

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

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

(4) Analysis of acts of deception conducted by an adversary.[16]

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 (for example, information operations and psychological operations).[17] In addition, intelligence makes a significant contribution to counter-improvised explosive

[14] A target is *the object of a particular action, for example a geographic area, a complex, an installation, a force, equipment, an individual, a group or a system, planned for capture, exploitation, neutralisation or destruction by military forces*. (AAP-06(2015))

[15] Targeting is *the process of selecting and prioritising targets and matching the appropriate response to them taking into account operational requirements and capabilities*. (AAP-06(2015))

[16] Deception is those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests (AAP-06(2015)).

[17] Information operations are a military function to provide advice and co-ordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives. (MC 0422/4) and psychological operations (PsyOp) are 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. (TTF 1994-0004, agreed on 2013-01-13; NSA(P&C/TC)MCTC(2012)1262-FINAL)

device (C-IED), Chemical, Biological, Radiological and Nuclear Defense (CBRN Defense), cyberspace operations and civil-military cooperation (CIMIC).[18]

e. **Intelligence Contribution to Targeting**. Intelligence lays the foundation for targeting.[19] Analysis conducted by the intelligence staff will provide the commander and targeting staff with details on how and where an adversary may be vulnerable. Specifically, intelligence provides the basis for the target system analysis, which is the basis of effective target development. Integral to target development is target validation. This process determines whether a target remains a viable element of the target system and whether it is a lawful target under the rules of engagement. 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.

f. **Intelligence Contribution to Counter-Proliferation**. Intelligence is a key enabler in preventing the proliferation of ballistic missiles, weapons of mass destruction, related CBRN threats, and other illicit 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 to produce and disseminate intelligence assessments that include the relevant aspects.[20]

g. **Intelligence Contribution to Operational Assessment**. Intelligence can provide 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 may be required to produce assessments for the commander. The focus for the intelligence staff will be the impact of joint operations on an adversary. It normally consists of an informed narrative assessment by intelligence staff (for example, the success of the air campaign in achieving control of the air could be assessed by the number of effective attacks conducted by an adversary against friendly forces since the commencement of the air campaign). Intelligence provides direct support to evaluation through[21]:

(1) **Measures of Performance.** Measures of Performance can be understood as the criteria used to evaluate the accomplishment of actions. Each level (operational and subordinate levels) will

[18] Intelligence procedures in support of C-IED operations are contained in AJP-3.15 *Counter-IED.*
[19] Details on Joint Targeting are contained in AJP-3.9.
[20] AJP-3.8(A) contains the NATO doctrine for chemical, biological, radiological and nuclear defence.
[21] See AJP-5, 0235.

normally develop measures of performance for the actions they will execute. Each measure of performance must:

a. Align to one or more actions.

b. Describe the element that must be observed to measure the progress or status of the action.

c. Have a known deterministic relationship to the action.

d. Measures of performance answer the question, have the planned activities been carried out successfully as planned?

(2) **Measure of Effectiveness (MOE).**[22] Measure of Effectiveness can be described as a criterion used to evaluate how a system's behavior or capabilities have been affected by actions. In other words, are we doing the right things. MOEs are used to assess progress towards the creation of desired effects and the achievement of objectives and end state. Monitoring an MOE over time will allow the determination of whether or not results are being achieved, as defined in the plan. They can also be used to provide indications that we need to change our actions because they are not achieving our aim. Based on knowledge of the systems involved, the operational planners will determine system elements for which measurable MOEs can be derived, the measurement of which over time will indicate if progress towards the desired objectives and end state is being achieved. Multiple MOEs per intended system state may be required to fully capture desired changes. While an MOE is a metric used to describe a system state, analysts may find it useful to package other information with an MOE such as the desired rate of change and threshold values. This assists in the assessment and analysis process.

(3) **Measurement of Campaign Progress.** Measurement of Campaign Progress is understood to be finding and utilizing criteria for operational success. These provide tests for determining when an objective has been achieved. They establish standards for sustainable self-regulating conditions and system states in the crisis or conflict that must exist as well as the ones that must not exist in order for the objective to be met.

(4) **Measurement of Activity.** Measurement of activity is the assessment of performance of a task and achievement of its

[22] Not defined in NTMS and AAP-06(2015) but listed as abbreviation in AAP-15.

associated purposes. It focuses on answering whether we successfully accomplished the things we planned and if an activity should be repeated or altered. In general, there is a quantitative and qualitative nature to measurement of activity. Commanders may draw on measurement of activity to inform decisions, but it is essentially tactical business.

a. Measurement of activity is reviewed within the daily campaign rhythm, under the activity review cycle.

b. Battle damage assessment is the most common form of measurement of activity and consists of physical damage assessment, functional damage assessment and target systems assessment. It is defined as the assessment of effects resulting from the application of military action, either lethal or non-lethal, against a military objective. Such assessment is primarily an intelligence staff responsibility, but links into the targeting process.

c. 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 battle damage assessment."

2.10 GUIDELINES FOR CONTEMPORARY INTELLIGENCE

In response to the challenges of contemporary operations, intelligence staffs need to operate in a manner that reflects the current environment and the factors that add complexities to their work. To be successful intelligence staffs should apply the following guidelines:

a. Commanders and staff should avoid becoming overly focused on adversaries and the physical terrain. Other aspects of the operational environment are of equal importance in planning and conducting contemporary operations. A more comprehensive view of the dynamics of situations is required. Commanders need to conduct their joint intelligence estimates through physical, cognitive and virtual environments and they should consider all actors within the wider operational environment.

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

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

d. The links between the commander and his intelligence staff must be strong and immediate. A commander cannot afford merely to set his critical information requirements and then leave the intelligence staff to feed them independently. He personally must drive the meeting of those requirements.

e. 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 rather than expecting the intelligence staff to routinely *push* the intelligence to them.

INTENTIONALLY BLANK

CHAPTER 3 FUNDAMENTALS OF INTELLIGENCE

3.1 DEFINITION OF INTELLIGENCE

1. Intelligence is defined as the product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers.

2. Despite the fading boundaries between the levels of warfare, an enduring requirement for intelligence has to be categorized based on its intended use. Consequently, there are three specific definitions of intelligence at these levels:

   a. **Strategic Intelligence**. Strategic intelligence is defined *as intelligence required for the formation of policy, military planning and the provision of indications and warning, at the national and/or international levels.*[23] 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. In NATO-led operations, it is important to develop the appropriate protocols to optimize the effectiveness of strategic intelligence.

   b. **Operational Intelligence**. Operational intelligence is defined *as intelligence required for the planning and conduct of campaigns at the operational level*.[24] It is used in the conduct of a campaign or operation, focusing on detailed reporting regarding the capabilities and intentions of actors and hazards to develop a commander's understanding and to assist in his decision-making.

   c. **Tactical Intelligence**. Tactical intelligence is defined as *intelligence required for the planning and execution of operations at the tactical level*.[25] It focuses on threat and hazard reporting that permits commanders to achieve a particular short-term mission, task or action. In most cases, intelligence assets providing tactical intelligence belong to the sending nation and may be part of the tactical headquarters involved.

[23] AAP-06(2015)
[24] AAP-06(2015)
[25] AAP-06(2015)

3.2 ROLE AND FUNCTIONS OF INTELLIGENCE

1. **Role of Intelligence**. The role of intelligence is to contribute to a continuous and coordinated understanding in a complex global environment, to enable appropriate decisions that permit NATO to take action to maintain security. Intelligence is therefore both an aid to developing understanding and a critical tool for decision-making. Intelligence should drive operations by providing the user with intelligence that supports their particular needs and is tailor-made to those requirements.[26]

2. **The Functions of Intelligence**. The primary functions of intelligence are:

    a. **Developing Knowledge and Enabling Understanding**. Intelligence develops knowledge about the environment and actors, including their intent, capability and motivation. It should strive to put this knowledge into context, thereby enabling the Commander's understanding. This context may encompass additional aspects related to material collected such as tribal or political dynamics that influence why particular groups take particular actions.

    b. **Producing Predictive Assessments**. Intelligence should be forward looking, enabling a commander to maintain the initiative. Nevertheless, reviews of both past and present activities may indicate future intentions and should be utilized accordingly. Intelligence staff should think ahead and establish the relevant structures and technology to feed the decision-maker.

3.3 CATEGORISATION OF INTELLIGENCE

Intelligence may be divided into the following types:

    a. **Basic Intelligence**.[27] Basic intelligence *is intelligence, on any subject, which may be used as reference material for planning and as a basis for processing subsequent information or intelligence*.[28] 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, infrastructural factors, socio-political descriptions, environmental aspects, etc. Basic intelligence, continuously reviewed and updated, is useful reference material on which to develop current

[26] For example, intelligence provided in support of counterinsurgency operations should be designed to meet the specific needs of those operations including C-IED, socio-cultural/human factors and attacking the insurgent network.

[27] Basic Intelligence is also known as *baseline intelligence* in some NATO countries.

[28] AAP-06(2015)

intelligence. Basic intelligence provides the context and backdrop against which current intelligence is reviewed.

b. **Current Intelligence**. Current intelligence *reflects the current situation at either strategic or tactical level*.[29] It should tell the decision-maker why it is relevant (the so what factor) and include 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 to the Common Operational Picture (COP) and predictions for possible developments.

3.4 PRINCIPLES OF INTELLIGENCE[30]

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

2. **Sharing**. Mechanisms are required whereby intelligence can be shared, in a timely manner, within NATO and with non-NATO entities guided by the idea of need to share in accordance with NATO existing security policy. The source of the information might be protected and the information itself might be sanitized to protect the source in order to share information with others.[31] NATO information exchange and classification procedures, must encourage and enable concerted effort, collaboration and cooperation wherever possible.

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

4. **Flexibility**. The intelligence staffs should establish an overall picture that provides timely, relevant, integrated and focused intelligence, suited to evolving security challenges. This requires a robust intelligence structure that can support intelligence driven operations.

5. **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. Intelligence assets should be

[29] AAP-06(2015)

[30] The principles of intelligence are taken from MC 0128/8 - Policy Guidance for NATO Intelligence.

[31] Some information is so critical that information security and force protection require to follow the principle of need-to-know. Need-to-share must be consistent with appropriate security guidelines.

centrally coordinated to avoid duplication of effort, provide mutual support and ensure the efficient, economic use of all resources.

6. **Comprehensive**. Intelligence should be comprehensive in nature and should explain the inter-related elements of a complex operational environment in an unbiased and undistorted manner. It should also consider the situation from the perspective of key actors, thus improving the predicative content of any assessment.

7. To achieve comprehensive intelligence, NATO utilizes the Political, Military, Economic, Social, Infrastructure and Information (PMESII) model. The use of the PMESII model 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 health and legal. Intelligence professionals may need assistance from specialist in some PMESII areas (e.g. the political advisor, engineers and civil military cooperation) to support their analysis or they may need to contact supporting commands and agencies, including non-military and non-governmental organizations. This collaborative process is necessary for intelligence to be successful in most NATO missions. It is also the key to both the KD concept and the comprehensive approach.

3.5 ATTRIBUTES OF INTELLIGENCE

The following attributes complement the principles of intelligence:

a. **Intelligence is 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 intimately understand the commander's intent, they will be unlikely to satisfy his requirements.

b. **Intelligence is Collaborative**. 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.

c. **Intelligence is Timely**. Intelligence should be delivered in time. 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, the commander 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 a commander might wish to take. Quality assessments take time to produce and the commander should always aim to provide intelligence staff with the earliest notification of an intelligence requirement.

d. **Intelligence is fused**. A multiple source approach utilizes the concept of intelligence fusion to optimize the value of various sources of information. 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, multiple source reporting is essential to gain in-depth understanding and avoid deception and misinformation.

e. **Intelligence is Objective**. Intelligence should always be unbiased, requiring staff with open minds. Intelligence staff should not distort their assessments to fit preconceived ideas to provide the answer that they think the commander wants, or conform to fit existing plans. A methodical and determined exploitation of all available information and intelligence will help objectivity.

3.6 LIMITATIONS OF INTELLIGENCE

1. **Management of Expectations**. Even when exploited fully, intelligence will not produce complete certainty. Intelligence staffs should be realistic about what can be achieved through intelligence activities especially when resources are limited. They must manage the expectations of their commanders while doing all they can to optimize available resources.

2. **Incomplete Intelligence**. Intelligence may not meet the commander's requirements exactly and may not be entirely accurate, complete, or easily corroborated. Nevertheless, commanders will have to make judgments and decisions based on it. While there is the risk of misinterpretation or deception, exploiting information is critically important. Intelligence staffs must articulate where there are gaps in knowledge enabling the commander to place appropriate weight on the assessments.

3. **Collection Assets**. All collection, exploitation and processing assets have limitations. Intelligence staff must provide the commander and all staff branches with a realistic appraisal of collection, exploitation and processing 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 should be provided with the strengths and weaknesses of adversary

collection assets. Additionally, commanders need to understand that the requirement for intelligence is likely to exceed the availability of collection or exploitation assets and that there will be a need to prioritize their requirements in order to make the best use of available intelligence resources.

4. **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 operational environments, where the size of an opponent's military capability may be less relevant due to unconventional or hybrid tactics, intelligence staff should ensure that commanders understand the increased difficulty of determining adversaries' capabilities, center of gravity, networks and intentions.

5. **National Constraints**. Some nations place national constraints upon the use of their intelligence capability. This is often due to restrictions placed upon their activities under their national laws. In addition, many European nations are legally required to operate within the requirements of the European Convention on Human Rights. Under no circumstances should commanders or their staffs task contributing nations to conduct intelligence activities that are contrary to their national law.

6. **International Law**. In most operations of an international nature, the legal mandate will be founded in international law and involve the application of elements of the Law of Armed Conflict. All intelligence activity should be conducted within this overarching legal framework.

3.7 AGENCIES, SOURCES AND SENSORS

1. **Sources.** In intelligence use, a source is a person from whom or a thing from which information can be obtained.[32] Sources can be divided into controlled, uncontrolled and causal:

a. **Controlled.** Controlled sources are under control of an intelligence agency or organization, or specifically nominated intelligence staff. They can be tasked directly.

b. **Uncontrolled.** Uncontrolled sources are those not under formal control of an intelligence agency or organization, or specifically nominated intelligence staff. Therefore, they cannot be tasked directly.

c. **Casual Sources.** Casual sources provide unsolicited information. Information provided by a casual source should be treated with caution, as the collector has no reporting history to utilize in order to verify a source's reliability.

[32] AAP-06(2015)

2. **Source Protection.** Source protection is critical where covert collection capabilities are involved.[33] However, source protection should not be a reason for withholding intelligence from those who need to know because the release of intelligence is often crucial for force protection and in gaining operational success. 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 in the information no longer being available, the source being used to pass deceptive information or the source being physically harmed or removed.

3. **Agencies.** In intelligence usages, an agency is *an organization engaged in collecting or processing information*.[34] An agency may be capable of collecting and processing information or may simply have the capability to collect information and should 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.

4. **Sensors.** Sensors are entities or items of *equipment which detects, and may indicate, and/or record objects and activities by means of energy or particles emitted, reflected, or modified by objects*.[35] A mix of sensors provides flexibility and enables the cross-cueing of sensors; using data from one sensor to direct another sensor to obtain additional data or to refine or clarify details.[36]

5. **Single and Multiple-Source Intelligence**. Most intelligence is derived from a single source. However, there are significant advantages to be derived from the use of Multiple Source Intelligence (MULTI-INT). MULTI-INT is the deliberate application of 2 or more discrete but supporting intelligence disciplines (e.g. Human Intelligence and Signals Intelligence) seeking to improve the quality of the intelligence product. Devoting time and effort to corroboration during intelligence collection activities increases certainty and reduces risk. Corroboration is achieved by comparing intelligence derived from one source with that derived from at least one other source so that common features or contradictions can be identified.

6. **National Intelligence Cell**. As nations often provide only limited intelligence capabilities to NATO and frequently retain national command and control of those assets they have provided, 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 a means for direct and timely exchange of national and theatre intelligence at the operational level.

---

[33] For example source protection is a vital issue during SIGINT, CI and HUMINT activities.
[34] This revised definition is awaiting NATO approval.
[35] AAP-06(2015)
[36] Cross-cueing is the passing of detection, geo-location and targeting information to another sensor.

3.8 INFORMATION MANAGEMENT

1. **Information Management**. Information management is the supervision, administration, regulation and timely dissemination of information. All personnel within the management process must understand the context of the information that they are handling in order to manage it effectively. Simply processing it is insufficient. While software applications allow the staff to receive, store, manipulate and disseminate information, human interaction provides the ability to identify opportunities to exploit it. Information management should not be regarded as a separate process in its own right, but part of an overall approach that includes exploitation and assurance, providing the highest possible quality of information efficiently and on time.

2. **Effect of Technology**. Modern technology has revolutionized the flow of information. This provides the commander with significant new capabilities that can deliver operational advantage enhancing the range, speed and volume of the bearers, providing new formats for information and increasing the ability to manipulate information. However, modern technology does not necessarily enhance either the understanding of the information or the ability to exploit it. The volume of information, the requirement to integrate numerous information sources and the speed of the reaction can result in information overload and can lead to decision paralysis. It can also lead to dependency on specific technology, applications or bearers to deliver mission critical information; leading to overreliance on potential single points of failure. To optimize operational efficiency, commanders should maintain a coherent, overarching staff-wide information management system within their command.

3.9 JOINT INTELLIGENCE SURVEILLANCE AND RECONNAISSANCE

1. **The Joint Intelligence, Surveillance and Reconnaissance (JISR).** JISR is an integrated intelligence and operations set of capabilities, which synchronises and integrates the planning and operations of all collection capabilities with processing, exploitation, and dissemination of the resulting information in direct support of planning, preparation, and execution of operations.

2. **Joint Intelligence Surveillance and Reconnaissance (JISR) Architecture.** The 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 Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) including the conduct of the Intelligence Requirements Management (IRM) and Collection Management (CM) processes, and optimizes intelligence and operations functions at all levels. The Intelligence System Support Architecture (ISSA) is an essential, integral part of the JISR Architecture.

3. **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 military operations to other operations that may include peace support, humanitarian, and non-combatant evacuation, as well as stabilization, reconstruction operations, crisis management missions, and other missions.

4. 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 shooter link) and to provide immediate threat warning to friendly forces. The JISR process helps develop situational awareness by contributing to the common operating picture.

5. **JISR Planning.** 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.

d. Coordinate between Intelligence, Operations, Plans, Communication Information Systems (CIS) staff divisions and other relevant staff divisions.

e. Manage time critical events.

3.10 INTELLIGENCE COLLECTION DISCIPLINES AND PRODUCTS

1. **Collection Disciplines**. Intelligence collection disciplines are the means or systems used to observe, sense, and record or convey information of conditions, situations, threats and events. The primary collection disciplines are:

a. **Acoustic Intelligence**. Acoustic Intelligence (ACINT) is *intelligence derived from signals or emissions*.[37] This is intelligence derived from sound. Examples of ACINT sources are hydrophones, geophones, SONAR, Integrated Underwater Surveillance System and artillery sound ranging systems. Due to the nature of the origin of sound, ACINT is primarily concerned with movement and the intelligence that can be derived from its detection.

b. **Human Intelligence**. Human Intelligence (HUMINT) is a *category of intelligence collected and provided by human sources*.[38] It includes the systematic and controlled exploitation, by interaction with human sources, objects, or individuals. It has the ability to provide information regarding an actor's intentions, morale, and relationships among individuals and organizations. HUMINT activities involve collection, reporting and analysis integrated within the overall 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*.[39] The information conveyed by an image or full motion video is clear and concise. It will often serve to support or confirm intelligence derived from other sources.

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 for the purpose of identifying any distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification*.[40] 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.

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.*[41] OSINT is collected from sources such as radio, television, newspapers, state propaganda, journals and technical papers, the Internet, technical manuals and books and other media. There is considerable archival evidence to confirm that the intelligence community has always used open sources in the production of intelligence. Freedom of Information

[37] AAP-06(2015)
[38] AAP-06(2015)
[39] AAP-06(2015)
[40] AAP-06(2015)
[41] AAP-06(2015)

legislation around the world has unlocked all but the most valuable of nations' secrets. There is also the growing ability to reach this information by systems such as the Internet. OSINT is most likely to be the source of basic intelligence. However, with the capabilities of modern news gathering equipment, there will be occasions when television reporting will be used to produce current intelligence.

f. **Signals Intelligence**. SIGINT is intelligence *derived from the collection and exploitation of foreign electromagnetic signals or emissions*.[42] 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 defined as:

(1) **COMINT**. COMINT is intelligence *derived from electromagnetic communications and communications systems by other than intended recipients or users*.[43] 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 down links.

(2) **ELINT**. ELINT is intelligence *derived from electromagnetic, non-communication transmissions*.[44] 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 about the equipment and its operator can be derived.

2. **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. Specialist intelligence products include, but are not limited to:

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

---

[42] NACSI approved revised definition dated 19th November 2010
[43] AAP-06(2015)
[44] AAP-06(2015)

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. **Forensic and Biometric Intelligence**. Forensics Enabled Intelligence (FEI) is a product regarding data and information derived from the application of multi-disciplinary scientific or technical processes and can often, although not exclusively, be collected to an evidential standard.

Biometric Enabled Intelligence (BEI) refers to forensic intelligence related to a specific individual. Examples include fingerprints and Deoxyribonucleic Acid (DNA).[45] [46]

d. **Geospatial Intelligence**. The geospatial community provides information that contributes towards the production of all source intelligence. Geospatial Intelligence combines quality-assured geospatial information with verified feature data and intelligence for compliance with a requirement.

e. **Medical Intelligence**. Medical intelligence is *derived from the processing of medical, bio-scientific, epidemiological, environmental and other information related to human or animal health*.[47] This intelligence, being of a specific technical nature, requires informed medical expertise throughout its direction and processing within the intelligence cycle. In the contemporary environment, medical intelligence can also be used as a collection discipline to obtain and analyze information relating to disease, biological warfare threats or health concerns.

f. **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, and weapons systems and their capabilities.

g. **Technical Intelligence**. Technical Intelligence (TECHINT) is *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*.[48] There are intelligence products derived from the scientific examination and testing of materiel including computer hardware and operating

[45] Some nations consider FEI and BEI to be part of MASINT or TECHINT
[46] MCM 0050-2012
[47] Details of Medical Intelligence are contained in AJMedP-3.
[48] AAP-06(2015)

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. TECHINT is a subset of Scientific and Technical Intelligence.

h. **Security Intelligence**. Security Intelligence (SI) is defined as *intelligence on the identity, capabilities and intentions of hostile organizations or individuals who are or may be engaged in espionage, sabotage, subversion or terrorism*.[49] 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. It is especially related to CI activity.

i. **Targeting Intelligence**. Targeting intelligence *portrays and locates the components of target or target complex and indicates its vulnerability and relative importance*.[50] It is intelligence produced for the targeting process.

3. **Geospatial Information**. Geospatial Information is about facts about the earth referenced by geographic position and arranged in a coherent structure. This includes topographic, aeronautic, hydrographic, planimetric, relief, thematic, geodetic, geo-referenced imagery, geophysical products, data, information, publications and materials. These will be available in either analogue or digital formats. [51]

4. **Sociological and Cultural Information**. Sociological and cultural information concerns human geography, social and cultural factors. These factors include population, political, economic, ethnicity, social stratification, stability, public opinion, education, religion, health, history, language, values, perceptions and behavior.

[49] AAP-06(2015)
[50] AAP-06(2015)
[51] MC 296/1 to be reviewed by MCJSB

INTENTIONALLY BLANK

CHAPTER 4 THE INTELLIGENCE CYCLE

4.1 INTRODUCTION

1. The Intelligence Cycle[52] is *the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available for users*.[53] These activities are focused through the four intelligence core stages of direction, collection, processing and dissemination shown in Figure 2. While the Intelligence Cycle outwardly appears to be a simple process, in reality it is a complex set of activities comprised of many cycles operating at different levels and speeds. Some tasks overlap and coincide so that they are often conducted concurrently, rather than sequentially.

2. The Intelligence Cycle consists of 4 stages:

   a. **Direction**. Direction is defined as the determination of collection 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.[54] Direction is the key to the intelligence process. There are two distinct types of direction required to make the process work: external and internal. 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.

   b. **Collection**. Collection is defined 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*.[55] ISR assets conduct the bulk of all collection activities, but non-dedicated ISR assets can also contribute.[56] Collection activity requires close collaboration with both intelligence and command staff to optimize the use of collection assets.

   c. **Processing**. Processing is defined as *the conversion of information into intelligence through collation, evaluation, analysis, integration and*

[52] Some nations use different national intelligence processes in accordance with their national doctrines.
[53] Allied Administrative Publication (AAP)-06(2015)
[54] AAP-06(2015)
[55] AAP-06(2015)
[56] Non-traditional ISR (NTISR) assets are assets that were not assigned for specific ISR tasks, but contribute to the intelligence picture as part of their routine operations (for example the use of a Military Police patrol to obtain HUMINT during their routine activities).

interpretation.[57] Processing is iterative and may generate further requirements for collection before dissemination of the intelligence.

d. **Dissemination**. Dissemination is defined as *the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it*.[58] It also requires security, conformity to the customer's requirement and a mechanism for feedback.

As depicted in the diagram below, the effective monitoring of the Intelligence Cycle and the coordination of the four core stages is undertaken through the Intelligence Requirement Management and Collection Management (IRM&CM) process.

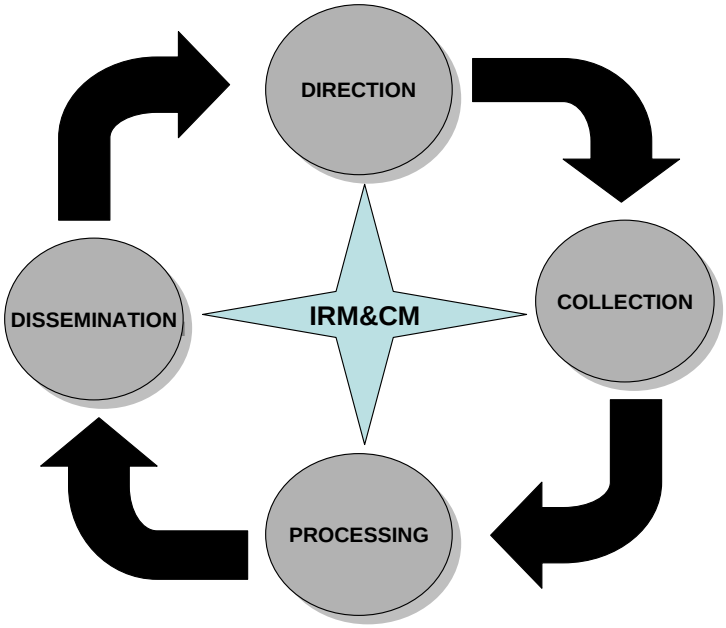

Figure 2: The Intelligence Cycle

4.2 DIRECTION

1. The Commander should prioritize his intelligence requirements and direct his intelligence staff by giving clear instructions concerning the intelligence he needs and the time limits on its provision.[59] This direction should be specific and, wherever feasible, should highlight those factors that are critical to the planning process.

[57] AAP-06(2015)
[58] AAP-06(2015)
[59] Details of intelligence requirements management are contained in Chapter 4.

2. In accordance with the Commander's direction the intelligence staff, in conjunction with operations and plans 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.

b. Tasking sources 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 the re-tasking or reprioritizing as required.

4.3 COLLECTION

1. Collection is the second phase of the Intelligence Cycle and is when information is obtained to meet the commander's intelligence requirements. During the collection phase, the appropriate JISR assets, sources and agencies are tasked to collect information. Those agencies with a processing capability may respond with intelligence rather than information.

2. There are two parts to the collection process. Primarily, intelligence staff will use JISR assets, sources and collection agencies to obtain the information required. Secondly, they will ensure the timely delivery of the collected information into the processing step in the Intelligence Cycle. It is important that intelligence staff ensure the commander and his staff understand the capabilities, limitations, vulnerabilities and response times of JISR assets, sources and agencies likely to be available to them, along with their susceptibility to deception.

3. There are several types of collection capability:

a. **Intelligence**. Intelligence assets have the ability to collect and analyze information. For example the collation and analysis of HUMINT collected by human intelligence units or SIGINT collected by signals intelligence units.

b. **Surveillance**. Surveillance is defined as *the systematic observation of aerospace, surface or subsurface areas, places, persons or things, by visual, aural, electronic, photographic or other means*.[60] Surveillance is conducted against known and potential adversaries and threat as well as in support of operations in current and potential future crisis areas. It can

[60] AAP-06(2015)

be passive or active, covert or overt. It can be *coarse grained* to provide early warning of 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 behavior.

c. **Reconnaissance**. Reconnaissance is defined as *a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area*.[61] It is a focused method of collecting information about specific locations, facilities or people. Reconnaissance tasks are not confined by specific reconnaissance units, but may be undertaken by other force elements in the course of their duties.

4.4 PROCESSING

Processing is the third phase in the Intelligence Cycle and entails a structured series of activities which, although set out sequentially, may also occur concurrently. Processing is conducted at a number of points within the intelligence function. The processing is a multi-faceted phase of the Intelligence Cycle consisting of collation, evaluation, analysis, integration and interpretation.

4.4.1 Collation

1. Collation is the first step in the processing phase in which the grouping together of related items of information or intelligence provides a record of events, which facilitates further processing.[62] 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 information and intelligence.

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

2. 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 information and intelligence will be placed during collation must be related to the commander's intelligence requirements and his area of responsibility.

[61] AAP-06(2015)
[62] AAP-06(2015)

4.4.2 Evaluation

1. There are many reasons, including deception and subjectivity, why information may not be reliable or accurate. 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 and the credibility of the information.[63]

Evaluation allocates an alphanumeric rating to each piece of information or intelligence indicating the degree of assurance, which may be placed upon it.[64] This rating is based partly on the subjective judgment 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 3 provides an example of the values used for allocating ratings for the reliability of the source and the credibility of the information.

	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 3: Evaluation and Rating

2. 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 the analyst should also consider, which affects his assessment of both reliability and credibility, is the source's access to the information involved.[65] This method of

[63] Amendment to definition in AAP-06(2015).

[64] 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 it is not formally used analysts should continue the mental process of evaluation.

[65] 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.

evaluation provides an indication over time of the capabilities of various sources and agencies and aiding the selection of those best suited for particular tasks.

4.4.3 Analysis and Integration

Analysis is the third step in the processing phase where information is subjected to review in order to identify significant facts for subsequent interpretation.[66] Integration is the fourth step in the processing phase whereby analyzed information and/or intelligence is selected and combined into a pattern in the course of the production of further intelligence.[67] In practice, integration follows on from analysis without a break and the two processes are treated as one.

During analysis, collated and evaluated information is scanned for significant facts. These are then related 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 the profile of an individual. This aspect of processing, as with evaluation, is almost totally based on human judgment, 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 judgment of the analyst.

4.4.4 Interpretation

1. Interpretation is the final step in the processing phase and is where the significance of information or intelligence is judged in relation to the current body of knowledge.[68] 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 information or intelligence is compared with, or added to, that which is already known, giving rise to new or updated intelligence. This mental process can be broken down into a sequence of four principal elements, which should be addressed 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, in order to discover whether there is any change in the pattern of activity.

[66] AAP-06(2015)
[67] AAP-06(2015)
[68] AAP-06(2015)

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.[69] The intelligence community is a primary target for hostile deception and the analyst should always be cautious of the information in front of him. In short, the analyst should seek confirmation of even the most credible information.

2. **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.

4.5 DISSEMINATION

1. The final phase of the Intelligence Cycle is dissemination. It is important for 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 affecting 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.

2. **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 higher formations to push information to satisfy intelligence requirements at lower levels of command. The ‘pull’ concept involves direct electronic access to databases, intelligence files, or other repositories by intelligence organizations at all levels of command. Web-based technologies and standards are now commonly used to organize and present intelligence products. 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.

[69] AAP-06(2015)

Intelligence can be disseminated in 5 formats. The format selected should be appropriate to the requirement and the recipient:

a. **Verbal**. Verbal briefing is useful for establishing trust, providing an opportunity to emphasize significant issues and limitations, as well as providing the briefer with immediate feedback and the potential for further direction. The process may be quick and can be delivered to a wider audience. It has a concomitant difficulty in controlling the understanding, a limited accessibility and a chance of misinterpretation when repeated.

b. **Written**. Written dissemination encompasses Intelligence Reports and Intelligence Summaries. Intelligence summaries should be disseminated at regular intervals, while urgent material is disseminated using intelligence reports. Presentation is important to written products that, although slower to prepare than some other forms of dissemination, may be tailored to recipients and provide a permanent record that can support databases. All originators should be aware of possible misunderstandings of written reports or summaries and therefore use clear wording.

c. **Multimedia**. Multimedia dissemination, encompassing pictorial, audio and video formats, may increase understanding and as a permanent record will support databases. This material requires careful editorial control of content to avoid distortion or over-simplification and appropriate training of intelligence staffs.

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

e. **Web-based**. Intelligence published on an internet and/or intranet-hosted website can store easily handled information and which may allow demanders to conduct their own intelligence requirement management. The effectiveness of a web-based database is dependent on its management and the quality of the inputs.

3. **Principles of Verbal and Written Dissemination**. Both verbal and written briefs should be governed by the following principles:

a. **Clarity**. The briefer has to ensure that he has marshaled his thoughts before briefing. The briefing should follow a standard format. The use of visual aids, maps, drawings and diagrams will enhance the briefing and clarify the information being discussed.

b. **Relevance**. The briefer has to ensure the information that he is discussing is relevant to the level of operations in which his audience is involved. It must also be current and not have been previously briefed.

c. **Brevity**. To be brief and succinct is the key to the successful dissemination of verbal information and intelligence. The good briefer is the one who imparts the most information in the fewest words.

4. **NATO Reporting Formats**. NATO uses standard report formats and message sets to guarantee multinational interoperability.[70] Wherever possible, written and web-based intelligence reports should follow NATO formats. Examples of these formats include:

a. **Intelligence Report (INTREP)**.[71] 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 commander or his staff. The INTREP should include any relevant deductions made in the time available. 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 flanking command echelons, but depending on content, a wider distribution will sometimes be necessary. The format of an INTREP must accord with agreed NATO reporting procedures.

b. **Intelligence Summaries (INTSUM)**.[72] 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, which 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 accord with agreed NATO reporting procedures.

[70] Further details on NATO intelligence report formats are contained in STANAG 7149/APP-11(C).
[71] The short title, INTREP, is always used in reports.
[72] The short title, INTSUM, is always used in reports.

c. **Supplementary Intelligence Reports (SUPINTREP)**. 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 CI-INTREPs, CI-INTSUMs and 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 operational environment, such as a region or town, a political or religious movement or a particular adversary organization, sometimes covering longer time-scales.

CHAPTER 5 INTELLIGENCE REQUIREMENTS MANAGEMENT AND COLLECTION MANAGEMENT

5.1 AIM AND PURPOSE

1. Conducted at all levels in NATO, Intelligence Requirements Management and Collection Management (IRM&CM) is at the center of the Intelligence Cycle. It ensures intelligence requirements (IR) are answered and the intelligence assets available are focused and prioritized. A common understanding of the IRM&CM process allows higher and lower headquarters within NATO and nations to share intelligence information and to make best use of collection capabilities.

2. Specific personnel from within the intelligence staff conduct IRM&CM. These personnel work closely with the commander's operational, intelligence and planning staff to satisfy intelligence requirements. They provide a vital link between the commander and the myriad of agencies and collection assets who are available to contribute to building the knowledge base on which to make decisions.

3. For IRM&CM to support any particular operation it must be able to coordinate the intelligence capabilities 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 also requires visibility of activity within all flanking and lower commands.

4. Within some staffs and nations IRM&CM could be carried out by designated Collection Co-ordination and Intelligence Requirements Management (CCIRM) sections.

5.2 INTELLIGENCE REQUIREMENTS MANAGEMENT

1. In any operation or planning situation, the commander will determine the type of information required to allow him to plan and conduct his 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.

2. 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.

3. 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 by collection management, which is the production and coordination of the plans for the subsequent collection, processing and dissemination of intelligence.

4. **Intelligence Requirements**. Intelligence requirements provide the rationale and priority for any intelligence activity as well as providing the detail to allow the intelligence staff to answer the requirement in the most effective manner. Intelligence requirements should cover the broad scope of information on the PMESII spectrum (as described in chapter 3). The military spectrum will be covered by the commander's critical information requiremens (CCIRs). Military types of intelligence requirements are:

a. **Commander's Critical Information Requirements (CCIR)** [73]. Information concerning areas that are either critical to the success of the mission or represent a critical threat are expressed as Commander's Critical Information Requirements (CCIR). CCIR cover all aspects of the commander's concern including Friendly Force Information Requirement (FFIR), Essential Elements of Friendly Information (EEFI)[74] and the Priority Intelligence Requirements (PIR). The two key elements of CCIRs are Priority Intelligence Requirements (PIR) and Friendly Force Information Requirements (FFIR). PIRs are derived from the CCIRs and their identification and drafting initiates and drives the intelligence process.

b. **Priority Intelligence Requirements (PIR)**. The Commander's Priority Intelligence Requirements (PIRs) are a vital part of the CCIRs and are normally formulated by the intelligence staffs in close cooperation with the commander. The PIRs encompass those intelligence requirements for which a commander has an anticipated and stated priority in his tasking of planning and decision-making and normally encompass 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 should provide comprehensive and coherent groupings of key issues. They may be enduring or limited to a particular phase or situation.

[73] FFIR and EEFI are not in the responsibility of intelligence staffs.
[74] Some nations do not recognize EEFI as a component of CCIR in their doctrine any longer.

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 the commander 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.[75]

c. **Specific Intelligence Requirements (SIR)**. Specific intelligence *requirements support and complement each PIR and provide a more detailed description of the requirement*.[76] Specific intelligence requirements 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 the support of the appropriate assets. The specific intelligence requirements allow collection and analysis agencies to develop their response or collection toward that best suited to the stated requirement. Specific intelligence requirements are divided in the same manner as PIRs. Some collection requirements may be submitted by other organizations within the intelligence community.

d. **Essential Elements of Information (EEI)**. SIRs are broken down into more detailed questions known as Essential Elements of Information (EEI). The EEIs add the details to the specific intelligence requirements and allow the production of a collection task list based on an intelligence collection plan. EEIs could be related to several SIRs and should provide enough guidance to allow analysts to give a complete and satisfying answer to each requirement. EEIs are the basis to create collection requirements and to establish relevant tasking and coordination with organic sources, sources or relevant agencies.

5. **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 staff's responsibility to determine if the request is valid. The IRM 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.

[75] The Joint Intelligence Estimate is considered in Chapter 5.
[76] New definition awaiting NATO approval

The methods pursued to answer these questions form the basis of the intelligence collection plan (ICP).

6. **Requests for Information**. The term Request for Information (RFI) is used to describe an intelligence requirement that is passed to the intelligence requirements manager at higher, lower or adjacent levels. A RFI is used when a commander does not have sufficient allocated collection capabilities or the intelligence staff is unable to answer a question through research or other means, and thus the commander requires assistance from a superior or adjacent 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 assets or subordinate headquarters.

7. **Intelligence Indicators**. Before beginning the collection process the intelligence staff should identify the indicators that are 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*.[77] Indicators are normally categorized 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 priority intelligence requirements. For example, tactical indicators 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.

[77] Allied Administrative Publication (AAP)-6 *NATO Glossary of Terms and Definitions*.

Selection of indicators appropriate to the operational situation is the responsibility of the intelligence staff. The nature of the indicators that they select will inform the intelligence collection plan.

5.3 COLLECTION MANAGEMENT AND PLANNING

1. Collection Management is the activity of matching the validated and structured intelligence requirements to the available collection assets. This process must take into consideration the availability of assets, sensor coverage and communications capabilities etc. The result is an Intelligence Collection Plan (ICP).

2. **The Intelligence Collection Plan**. The ICP is a detailed breakdown of how each intelligence requirement is to be satisfied. Normally in matrix or table form, it indicates by which means an intelligence requirement can be best satisfied, the frequency of coverage required and the type of product expected. It will indicate the general level of detail required and will list the organizations, agencies or assets best suited to the task.

3. **Collection Coordination**. The coordination of the collection effort is achieved through the implementation and control of the ICP. The intelligence requirements are converted into specific tasks that are put to assigned sources and agencies. Where a commander has no assigned collection capability to answer the intelligence requirement it is passed to higher or adjacent formations as a RFI. It is important that IRM&CM staffs develop a procedure for time-sensitive, unexpected or urgent requirements that need to be fast-tracked.

4. **Dissemination Planning**. Dissemination planning enables the right information to be distributed to the right people in the right format and within the right timescale. Staff elements responsible for IRM&CM will determine the means of dissemination, storage and retrieval of product. That can be a single system or currently relying on a myriad of ways and means which have to be coordinated with the wide variety of entities within the IRM&CM process.

5. **Allocation of ISR Tasks**. Staff elements responsible for IRM&CM will produce an intelligence collection plan. However, they do not have the authority to issue and execute orders in the operational area. That task is undertaken as a collaborative effort between the intelligence and operations staff. This requires the allocation of ISR tasks to assigned or subordinate ISR assets.

6. **Selection of Collection Assets**. ISR assets must be assigned according to their suitability and availability rather than ownership. For tasks involving complex targets, or the possibility for camouflage, concealment and deception techniques, multi-collection capabilities may be necessary to answer a single intelligence requirement. In some instances, it may be preferable to modify the constraints of the intelligence requirement to match an available asset than to pass an unachievable intelligence requirement to another organization as a Request for Information. In

addition to knowledge of dedicated ISR assets, and non-dedicated ISR assets organic to their organization, intelligence staffs should be familiar with assets of higher or national organizations, their strengths and weaknesses, and the process for tasking them.

7. **Allocation of Collection Assets**. Coordination is required to prioritise competing demands on the same collection capability. This includes re-allocating assets and the direction to assets. This coordination also ensures coherence between the collection and alternative functions of dual-role or multirole assets.

5.4 MANAGEMENT AND EXCHANGE OF INFORMATION

1. The IRM&CM process is a complex management function involving the administration of IRs, the channeling of RFI and the tasking of collection, and the delivery of intelligence products and answers to demanders; this data flow must cross quickly between nations and command chains. Therefore, the IRM&CM process is a significant data management and interoperability challenge involving a number of discrete activities, but based around a generally similar set of criteria. The IRM&CM process therefore requires a seamless method of linking the various requesting, managing, tasking, production and distribution activities.

2. IRM&CM must employ standardized formats and interoperable systems to allow automated, seamless communication and sharing of IRs, plans and products. This includes standardized metadata. Nations and headquarters within the operational structure are responsible for complying with these standards to enable participation in the process. In addition to current NATO intelligence tools that can store and process intelligence, IRM&CM requires tools that are also able to pass and manage information requests and final intelligence products.

CHAPTER 6 JOINT INTELLIGENCE PLANNING

6.1 JOINT INTELLIGENCE AREAS

1. To enable the commander and his intelligence staff to focus their intelligence effort, the joint operational area is divided into two areas:

a. **Area of Operations (AOO).** An area defined by the joint force commander within a joint operations area for the conduct of specific military activities.[78]

b. **Area of Intelligence Responsibility:** An area allocated to a commander, in which he is responsible for the provision of intelligence, within the means at his disposal.[79]

2. **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. Therefore, commanders should consider cyberspace to be an area in its own right.

6.2 OPERATIONAL-LEVEL PLANNING PROCESS

NATO's Operational-Level Planning Process is described in AJP-5 and in the Allied Command Operations Comprehensive Operations Planning Directive. The Operational-Level Planning Process is applicable to any strategic, operational or tactical headquarters. The intelligence staffs provide a major input to operational-level planning throughout the conduct of the process.

6.3 JOINT INTELLIGENCE ESTIMATE

1. The Joint Intelligence Estimate describes the operational environment in relation to meteorological and oceanographic (METOC) conditions, adversary, cyberspace and terrain. The intelligence estimate results in a forecast based on degrees of probability. It is a series of logical deductions drawn from the information available and influenced by the knowledge and experience of the author. The Joint Intelligence Estimate informs the Operational Estimate by contributing to the commander's understanding and informing campaign planning. The Joint Operational

[78] AAP-06(2015)
[79] AAP-06(2015)

Estimate enables the commander to decide how to achieve his mission. It should encompass situational understanding, what is to be achieved and by when, the courses of action available and the desired end-state.

2. As intelligence is gathered, the Joint Intelligence Estimate increases in detail and provides significant input to the operational-level planning process.[80] The principal outputs of the Joint Intelligence Estimate are:

a. Providing the commander with the intelligence required for the Operational Estimate.[81]

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

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

3. **Production of the Estimate**. The creation of the Joint Intelligence Estimate is a process that comprises an analysis of the situation and an assessment.[82] It requires analytical and logical thought processes. The Joint Intelligence Estimate should include:

a. An assessment of the adversary's capabilities and likely intentions based on the available intelligence:

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

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

a. The commander's mission.

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.

---

[80] The Intelligence Estimate can be done using the Joint Intelligence Preparation of the Operational Environment as a method, or as a straight text document.

[81] The Intelligence produced by the Intelligence Estimate should include basic intelligence on the adversary's Centre of Gravity, his potential courses of action and his high value targets etc.

[82] The Joint Intelligence Estimate is produced in the standard NATO format contained within AJP-2.1 *Intelligence Procedures*.

e. The options and the adversary's doctrine of operations

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

g. Socio-cultural factors of the hostile and non-hostile population in the JOA.

5. **Assumptions**. Assumptions may be used when there are gaps in the intelligence staff's knowledge. 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. 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 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.

6. **The Joint Intelligence Estimate and the Joint Intelligence Preparation of the Operational Environment**. In general, the formal intelligence estimate process will be conducted at the higher levels of command where there are greater resources to carry out the process. A Joint Intelligence Estimate is likely, for example, to form part of a campaign plan. Joint Intelligence Preparation of the Operational Environment is more likely to be conducted at lower levels of command where time is of the essence and priorities are more urgent.

6.4 JOINT INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

1. Joint Intelligence Preparation of the Operational Environment (JIPOE) provides an understanding of the operational environment and is a basis for planning.[83] 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.

2. JIPOE should be constructed in a manner that allows:

a. Easy and speedy updating.

[83] The JIPOE Process has replaced the former IPB (Intelligence preparation of the battlespace) process at the operational-level planning

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.

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

a. Define the operational environment.

b. Describe the environment's effects.

c. Analyze the actors or intended targets.

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

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

f. Identify when the commander must act to influence the outcome of the operation.

4. 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, weather METOC conditions, the adversary's tactical doctrine or preferred Scheme of Maneuver and any other actors impacting on the operation, all of which can be prepared well in advance. Just before and during operations, current updates can be included to reflect changes in key factors that may affect force activity across the spectrum of conflict.

5. **The JIPOE Process**. The NATO JIPOE process consists of 3 basic steps that are described below:[84]

a. **Step 1 – Area Evaluation**. The first step assesses the effects of relevant factors concerning the operational environment on the activities conducted by both friendly and opposing forces. In relation to counter-terrorism and force protection, this will include the threats to military and

[84] Some individual member nations use different JIPOE / IPB processes with a different number of steps.

non-military operations, (e.g. the ethnic distribution of the population and its loyalties). Some of the principal factors affecting the operational environment are terrain, infrastructure, information environment, protected areas, weather METOC conditions and medical factors.

b. **Step 2 – Actor Evaluation**. The aim of Step 2 is to identify an actor's doctrinal courses of action independent of terrain and weather constraints, (i.e. how the actor fights according to his 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 his doctrinal course of action.

c. **Step 3 – Threat Integration**. In Step 3 of the JIPOE process, the results of the Area Evaluation are combined with the doctrinal course of action and other overlays developed in the Threat Evaluation. The aim of Threat Integration is to identify how the operational environment will shape doctrine and turn it into practice.

6. **PMESII**. The Political, Military, Economic, Social, Infrastructure and Information (PMESII) model[85] consists of factors that should be considered when conducting JIPOE. Additional factors can be added to PMESII if required by the specific operations (for example, health matters). PMESII describes the foundation and features of an adversary and can help determine their strengths and weaknesses, as well as help estimate the effects various actions will have on actors across these areas.

7. **Validation**. Validation involves setting up a team or teams 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 we would 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.

8. **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 combat.

[85] The operational environment can be initially viewed through several conceptual models. The most common in NATO are the six listed PMESII domains. But other models are admitted

9. **JIPOE and the Joint Targeting Process**. The joint targeting process closely parallels JIPOE. Initial targeting data is refined through the JIPOE process. Additional intelligence requirements arise during the targeting process and these are integrated into the Intelligence Collection Plan. 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.

CHAPTER 7 THE THREAT TO SECURITY

7.1 INTRODUCTION

Security is the condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure.[86] It includes the measures implemented to protect against the threat to security. The sharing of security information among NATO partners improves security of multi-national operations.

7.2 THE THREAT TO SECURITY

1. Threats to security can originate from both external and internal sources. 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.[87]

2. The threats to security can be categorized as:

   a. **Terrorism**. Terrorism is the *unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, ethnic, religious or ideological objectives*.[88]

   b. **Espionage**. Espionage is defined *as intelligence activity directed towards the acquisition of information through clandestine means and proscribed by the law of the country 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 a nation by undermining the morale, loyalty or reliability of its citizens*.[89] An attack on individual or collective loyalty is

[86] AAP-06(2015)

[87] 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.

[88] AAP-06(2015)

[89] AAP-06(2015)

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.[90]

f. **Computer Network Attack**. Actions taken using computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

7.3 COUNTERACTING THE THREAT TO SECURITY

1. **Responsibility for Counteracting the Threat**. Counter Intelligence (CI organizations, military or civilian, of the member nations (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. 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.

2. **Responsibilities of Security Staff**. The principal responsibilities of the security staffs at all levels of command are:

a. Advising the commander on all security threats.

[90] This is a new definition awaiting NATO approval.

b. Managing and supporting operations to counteract the security threats.

c. Collecting, processing and disseminating information relative to CI requirements and producing and disseminating current threat assessments.

d. Contributing to the operational security process, including the planning, coordination and application of protective security measures throughout the formation.

e. Establishing and maintaining liaison with civil law enforcement and CI authorities.

3. **Need-to-Know**. The fundamental security principle is that knowledge or possession of classified information should be strictly limited to those, security personnel cleared to the appropriate level, who clearly have a need-to-know in order 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.[91]

4. **Principles 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.

e. Threat information should be produced by 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.

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

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

5. **Security Education**. 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.

7.4 PROTECTIVE SECURITY

1. Protective Security is defined as *the organized system of defensive measures instituted and maintained at all levels of command with the aim of achieving and maintaining security.*[92] It is the protection of assets including personnel from an unwanted event or from compromise. There are four categories of protective security measures:

a. Personnel security, which includes *those measures taken to exclude or restrict access to protectively, marked information or material by persons whose loyalty, reliability or trustworthiness may be in doubt*.[93]

b. Physical security, which is *that part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, and documents and to safeguard them against espionage, sabotage, damage and theft*.[94]

c. Operations Security, which is *the process that gives a military operation or exercise appropriate security using passive or active means to deny an enemy knowledge of the dispositions, capabilities or intentions of friendly forces*.[95]

d. Information security (INFOSEC) is defined as *the measures required for the preservation of confidentiality, integrity and availability of information, in documentary, audible or digital formats from compromise*.[96]

2. The aims of protective security measures are to:

a. Expose any attempt by unauthorized persons to penetrate controls.

b. Prevent hostile intelligence services or subversive/criminal/terrorist organizations, groups or individuals, from acquiring information, causing disruption or subverting military or civilian personnel.

---

92 AAP-06(2015)
93 This term and definition are only applicable in this publication.
94 AAP-06(2015)
95 AAP-06(2015)
96 This is a new definition proposal awaiting NATO approval.

c. Provide common minimum standards of security that can be applied in all formations and units.

d. Prevent the possibility of unauthorized access to digital information and the destruction or alteration of information in communications information systems or on personal computers.

e. Assist security personnel conducting investigations into security breaches.

3. No single security measure will be effective in isolation; therefore, protective security must consist of a number of interrelated, mutually supporting measures that together achieve an acceptable degree of security.

4. The application of protective security measures is mainly a national responsibility. Forces deployed in countries other than their own apply security measures within their area of responsibility and they should co-ordinate these measures in conjunction with the host nation. Security of the rear areas remains a national responsibility of the respective host nation. Exchange of security intelligence and co-ordination in the application of protective security measures is a precondition for the achievement of adequate security. However, the application of protective security measures is a national responsibility.

7.5 PROTECTIVE SECURITY PROCEDURES

1. **Development of a Threat Assessment**. A threat assessment is vital to countering the threat and it should be prepared thoroughly by:

a. Studying the strengths, capabilities, methods and probable intentions of all organizations, groups, individuals and respective assets as mentioned above.[97]

b. Defining the possible targets most likely to be attacked.

c. Considering the threat to and the vulnerability of critical targets.

2. **Personnel Security Measures**. The principal personnel security measures are:

a. Careful selection of reliable personnel for sensitive posts.

b. Authorization for selected personnel to have access to classified information on the principle of “need to know”.

[97] See Chapter 5, Section IV; The Joint Intelligence Preparation of the Operational Environment

c. Vetting the character and background of personnel selected for sensitive posts as permitted under national legislation. The object is to prevent persons of doubtful reliability from having access to classified information. However, vetting does no more than indicate that on a given date a particular individual was, or was not, reliable.

d. Maintaining within the context of general supervision a constant watch on the reliability of persons having access to classified information.

e. Good personnel-management, supervision and education.

3. **Physical Security Measures**. Physical security measures include:

a. The employment of guards and necessary reaction forces as well as structural and technical measures, such as physical obstacles, deployed in depth to frustrate attempts to penetrate security defenses.

b. Measures taken to prevent penetration by eavesdropping devices, whether electronic or acoustic.

Since one of the prerequisites of successful espionage is that the holders of secrets should not be alerted to the fact that these secrets have become known to the belligerent, it follows that physical security must be supported by other measures. However, the best locks, alarm systems and perimeter fences can do little more than impose delays because a determined and skillful intruder will always succeed in gaining access. The advantage of physical security is that it makes penetration of the security defenses more difficult and thus provides time for other security measures to be taken.

4. **Operations Security Measures**. Operations security measures depend largely on the application of certain procedures which are laid down in NATO, national, command or unit laws, orders, instructions or standing operating procedures. They can be personnel or physical security measures or a combination of both. These include:

a. Designation of zones as being of high or low sensitivity.

b. Collocation of zones of high or low sensitivity.

c. Control of access to restricted or prohibited areas.

d. Provision of guards and a reaction force to support them.

e. Provision of a system of security passes.

f. Development of security contingency plans to cover security, riot control and control of keys, including the establishment of an adequate Alert States System.

g. The inclusion in local standing orders of all security plans, including regular inspections, surveys and checks to ensure that protective security measures are kept up to date and remain effective.

h. Security investigations to remedy and identify faults.

i. Appropriate classification of documents, material and equipment.

j. Planning and providing equipment for the destruction of classified material generally and in an emergency.

k. Security training, in the form of security briefings, security training and security exercises which put into effect contingency plans for dealing with emergencies.

l. Implementation of censorship (determined by national legislation/freedom of information).

m. Area security procedures for providing Restricted Areas for military assets (e.g. Airfield security for military aircraft).

5. **INFOSEC Measures**. In order to prevent unauthorized access to digital information the following measures should be taken, unless national authorities direct otherwise:

a. Information Technology (IT) systems should only be operated and equipment should only be stored in restricted areas with limited access.

b. Access to IT systems should only be permitted to personnel, who are cleared to the highest level of available classified information/data in the system.

c. Access to IT systems by electronic devices (CD-ROM, Disc etc.) should be limited and controlled.

d. Approved equipment should be used wherever the available facilities do not meet given standards, especially when systems are deployed in the field.

e. Regular change of passwords should be compulsory.

f. Military networks should not be connected to public networks like the Internet unless secure technical means can prevent unauthorised access.

7.6 FORCE PROTECTION

Force protection (FP) is measures and means to minimize the vulnerability of personnel, facilities, materiel, operations, and activities from threats and hazards in

order to preserve freedom of action and operational effectiveness thereby contributing to mission success.[98]

[98] For more information on Force Protection see AJP-3.1.4 „Allied Joint Doctrine for Force Protection“

CHAPTER 8 COUNTER-INTELLIGENCE

8.1 INTRODUCTION

1. Counter-intelligence (CI) includes 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.*[99] This chapter provides an overview of CI including role, responsibilities, the CI process and countermeasures. Additional, details on CI are contained in the Allied Joint Doctrine for Counter-Intelligence and Security Procedures (AJP-2.2).

2. The main thrust of the CI effort is to protect personnel, information, plans and resources, both at home and when deployed. It 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.

3. 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-educated decisions on security measures. In reality, there are likely to be compromises between what is needed and what is feasible.

8.2 THE ROLE OF COUNTER-INTELLIGENCE

2. To ensure successful military operations the commander should deny the adversary the opportunity to conduct terrorism, espionage, subversion, sabotage, organized crime or computer network attacks against friendly force. To achieve this requires identification of 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.

8.3 CI RESPONSIBILITIES

1. **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 defense (MODs) with superior, lateral and subordinate headquarters to ensure familiarity with neighboring CI structures.

[99] AAP-06(2015)

2. **National Responsibilities**. Each nation should designate one organization as the single point of contact for CI matters. Within each national organization, a National CI Adviser (NCIA) will be nominated. As some of these NCIAs are unlikely to be permanently available, nations will nominate National CI 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 in order 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.

3. **CI Coordinating Authority**. When NATO forces are deployed on operations, the designated CI Coordinating Authority (CICA) will supervise all aspects of CI and will be the commander's principal advisor in CI matters. The CICA is responsible for coordinating and de-conflicting national and NATO CI operations and investigations in the joint operations area.

4. **J2X**. 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 the register of sources and de-conflict both HUMINT and CI activity. In addition, they will provide advice to commanders on HUMINT and CI operations. Within J2X, the CI Cell is responsible for the co-ordination of CI activities including overseeing the operational activities, briefings and debriefings. The J2X is also responsible to ensure that information sharing agreements and methods are in place in order to increase situational awareness and the efficiency of the entire CI and HUMINT effort.

5. **HUMINT and CI**. HUMINT activities often occur alongside those involving CI and many of the skills and capabilities are common. HUMINT and CI should be regarded as being complementary and must not become competitive. It is essential that commanders encourage co-operation between respective intelligence specialists and that J2X co-ordinates all HUMINT and CI activity.

8.4 CI IN MULTINATIONAL OPERATIONS

1. **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.

2. **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 contemporary operations the need to counter the existing and constantly changing threat will require timely exchange of all available CI information.

3. **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.

4. **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.[100] Liaison is conducted to obtain and corroborate information, develop sources of information and foster both goodwill and understanding. 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.[101] CI operations require a high degree of integration with intelligence and HUMINT staffs.

8.5 THE CI ESTIMATE

1. The CI Estimate is produced in parallel with the production of the Joint Intelligence Estimate.[102] A CI Estimate focuses on the hostile intelligence services

[100] 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.

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

[102] More details on the Joint Intelligence Estimate are contained in Chapter 5.

capabilities, the threat posed by subversive, terrorist, criminal organizations and friendly force vulnerabilities.

2. The CI Estimate supports and complements the Joint Intelligence Estimate by:

   a. Providing an estimate of friendly force vulnerabilities to an adversary's ISR operations; thereby informing counter surveillance, OPSEC and deception planning.

   b. Giving 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.

8.6 THE CI PROCESS

In order to ensure that CI is always conducted in the most efficient way in a manner that is common within and across the nations of the Alliance, guidelines for a standard methodology have been developed. This methodology is known as the CI Process. The CI Process, in common with other intelligence processes, is based on the Intelligence Cycle. The relationship between the CI Process and the Intelligence Cycle is shown diagrammatically below:

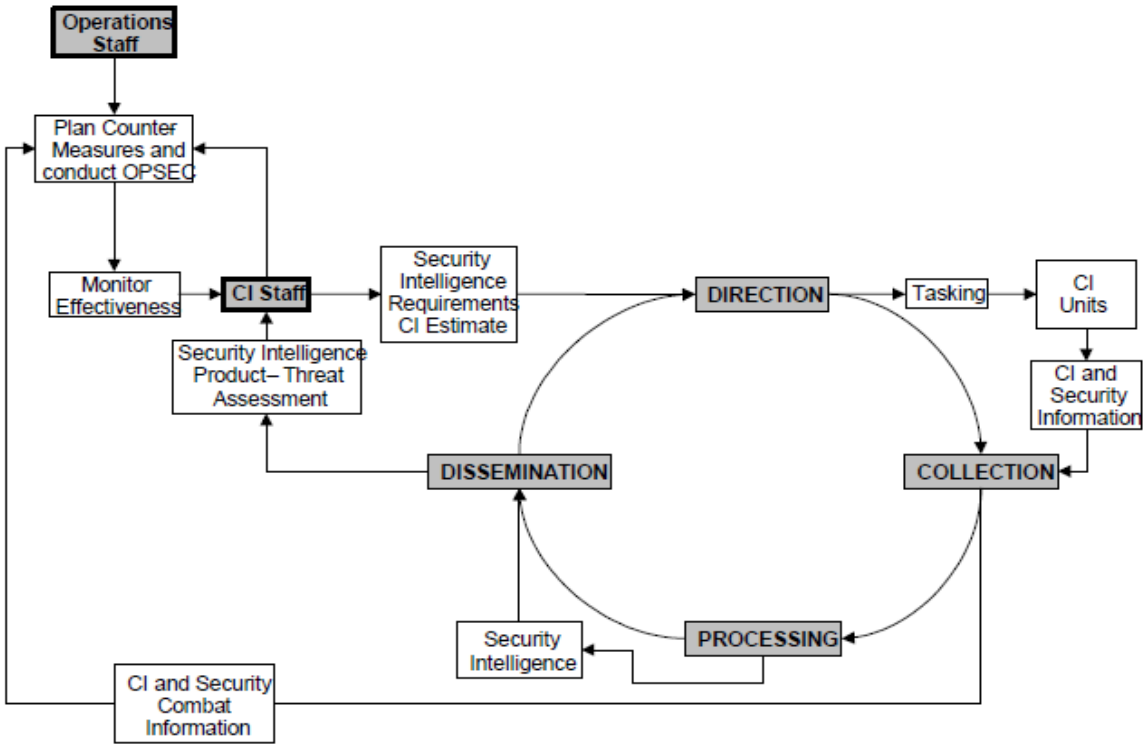

Figure 3: The CI Process

8.6.1 Stage 1 - Direction

1. Successful CI operations require the formulation of a detailed and coordinated CI Plan. The CI Plan prioritizes threats to indicate the degree of security risk they represent and thus the degree of urgency with which they are required to be neutralized or exploited. The CI Plan also contains details of the appropriate countermeasure.

2. Commanders with CI responsibilities need CI information and support to accomplish their mission. These needs shall be categorized as:

a. Basic CI Requirements. Information on non-NATO intelligence services and subversive organizations, terrorist and criminal groups directed against NATO, NATO member nations, partners or allied forces.

b. Current CI Requirements. Timely information which might give additional clarification and broaden knowledge of non-NATO intelligence services and subversive organizations, terrorist and criminal groups and their activities such as espionage, sabotage, subversion, terrorism and organized crime.

c. Urgent CI requirements. Timely information on activities requiring immediate countermeasures by NATO, NATO member nations, partners or allied forces

8.6.2 Stage 2 - Collection

1. CI collection is primarily conducted through debriefings, liaison with law enforcement, intelligence organizations and source directed operations. CI collections can also be conducted through RFIs via the IRM &CM processes for non-assigned resources. Best practice is for CI requirements to be contained within the intelligence collection plan. Inevitably, there will be conflicting demands for the use of scarce collection assets and commanders should be prepared to change priorities for use of the assets as the operational situation develops.

8.6.3 Stage 3 - CI Processing

1. Information of CI value is subjected to CI analysis, which equates to the processing stage of the intelligence cycle and the procedures used are the same.[103] This analysis is the first step taken in countering the threat and is the catalyst for all other security measures. Therefore, each national CI organization, and level of command must make an assessment which should be kept under constant review and amended in the light of new knowledge or of changes in the operational situation. The analysis process and CI reports produced from it are disseminated as an intelligence product.
2. Whenever possible, CI assessments should be based on accurate and timely intelligence, directed by the CI Estimate to include reports from all relevant

[103] More detail on processing is contained in Chapter 3.

organizations and assets. All information collected should be processed and disseminated as a CI product in accordance with the intelligence cycle. CI products will be the major contributor to the assessment of the threat.

8.6.4 Stage 4 - CI Dissemination

1. Dissemination is the timely conveyance of information or intelligence, in an appropriate form and by suitable means, to those who need it.[104] The time factor is a critical aspect of dissemination of all kinds of intelligence, but the value of CI assessments can be seriously degraded or even useless if it arrives late. As most aspects of security are a national responsibility, the establishment of an international intelligence dissemination system is of vital importance. Dissemination can be oral, written, graphic or through data-exchange. All forms of dissemination must meet the extant security regulations.

2. CI and security staffs are responsible for ensuring that all information and all intelligence is disseminated to the responsible commander and others who need it, including CI and Security staffs in flanking or neighboring formations. CI assessments that provide warnings of threats to security should be disseminated widely to warn every unit that could be affected.

3. CI information will be reported as follows:

   a. **Counter-Intelligence Report (CI-INTREP).** This report should be used to report CI information immediately without regard to a specific time schedule. It details significant changes in threat intentions, capabilities, status, imminent threat attacks, or other events and indications of threat activity based upon the mission, situation, and needs of the commander. CI-INTREPs are always event-driven.

   b. **Counter Intelligence Summary (CI-INTSUM).** This should be a summary of CI information on a periodic basis as required. CI-INTSUMs contain both summaries of events and an analysis of what these events indicate, especially in terms of identifying threat intentions and capabilities. Furthermore, the inclusion of human factors, intentions, capabilities and perceptions of key threat leaders/cadre distinguish CI-INTSUMs from generic intelligence summaries. Thus, the content of CI-INTSUMs should identify and analyze the motivation, ideology, level of sophistication, extent and levels of leadership (narrow or wide based), level of education, direction of movement/organization (growing or shrinking, becoming more or less violent, etc.) of threat entities and factions. Also of critical importance is the relationship between individuals and organizations, sources of external support, structural descriptions of organizations, vulnerabilities, leadership power struggles

[104] CI disseminations procedures are the same as those given in Chapter 3.

and shifts, etc. Predictive analysis remains inherent and essential. The following information should be included:

(1) Espionage activities.

(2) Sabotage activities.

(3) Subversive activities.

(4) Terrorist activities.

(5) Organized crime activities.

(6) Computer network attack.

(7) General assessment.

c. **Counter Intelligence Supplementary Report (CI-SUPINTREP)**. The purpose of a CI-SUPINTREP is to provide information on all CI data collected over an extended period including an assessment of trends in the development of the CI situation. The CI-SUPINTREP is also used to provide a comprehensive review of one or several specific CI projects and thus is often subject dependent.

d. **Counter Intelligence Warning Messages**. Although hostile intelligence service activities remain the focal point of interest in NATO operations, terrorism also poses a severe threat to military forces. Therefore, commanders are to be informed of available terrorist information that may require subsequent security action(s) to ensure continuous operational readiness.

4. All forms of CI reports should be classified based on their content, but the classification should be kept as low as possible. The methods of disseminating reports and data are determined by the classification of the information itself.

8.7 CI COUNTERMEASURES

1. **CI Targets**. Once the CI assessment has been completed and the implications for security identified, CI targets can be identified. CI targets are installations, organizations, information networks and personnel of either intelligence or CI interest that must be seized, destroyed, exploited or protected.

2. **Security Implications**. The intelligence and security staffs can deduce from the CI assessment the effects that the various threats identified within the assessment may have on the friendly force's activity. These can be categorized as:

a. Threats to be resolved by the enforcement of effective security and OPSEC measures.

b. Threats (which could be turned into opportunities) to be exploited by both the meeting of intelligence requirements and the conduct of information operations.

3. **Countermeasures**. Countermeasures fulfill tasks across the whole spectrum of CI and Security and have four basic aims. These are:

a. **Deter**. Robust overt measures will constitute an effective deterrent to a potential attacker. However, even the knowledge that less overt measures designed to deny access and detect intrusion have been introduced can also deter adversary intelligence attack or physical operations.

b. **Deny**. Activities applied to prevent an adversary gaining access to protected and sensitive information, preventing the influencing and subversion of personnel and the penetration of the friendly force's physical security barriers.

c. **Detect**. The exposure and neutralization of the efforts of adversary information collection operations.

d. **Deceive**. Activities primarily used to mislead or otherwise confuse the adversary about the friendly force's capabilities and intentions.

ANNEX A - REFERENCES

a.	MCM-0077-2000	Military Committee Guidance on the Relationship between NATO Policy and Military Doctrine
b.	MC 64	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 on Information Operations
l.	MC 0472	NATO Military Concept for Defence Against 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 0600	NATO Policy on Knowledge Development
q.	Bi-MNC	Reporting Directive Volume II – Intelligence Reports
r.	AJP-01(D)	Allied Joint Doctrine
s.	AJP-2.1(A)	Allied Doctrine for Intelligence Procedures (TBP)
t.	AJP-2.2	Counter-Intelligence and Security Procedures
u.	AJP-2.3	Allied Joint Doctrine for Human Intelligence (HUMINT)
v.	AJP-2.5(A)	Captured Persons, Materiel and Documents
w.	AJP-2.7	Allied Joint Doctrine for Reconnaissance and Surveillance
x.	AJP-3(B)	Allied Joint Doctrine for the Conduct of Operations
y.	AJP-3.4(A)	Allied Joint Doctrine for non-Article 5 Crisis Response Operations
z.	AJP-3.4.1	Peace Support Operations

aa.	AJP-3.8(A)	Allied Joint Doctrine for Chemical, Biological, Radiological and Nuclear Defence
bb.	AJP-3.9	Allied Joint Doctrine for Joint Targeting
cc.	AJP-3.10	Allied Joint Doctrine for Information Operations
dd.	AJP-3.10.1(B)	Allied Joint Doctrine for Psychological Operations
ee.	AJP-3.14	Allied Joint Doctrine for Force Protection
ff.	AJP 3.15(B)	Allied Joint Doctrine for Counter Improvised Explosive Devices (C-IED)
gg.	AJP-5	Allied Joint Doctrine for Operational-level Planning
hh.	AAP-06(2015)	NATO Glossary of Terms and Definitions
ii.	AAP-03(J)(2)	Production, Maintenance and Management of NATOs Standardization Documents
jj.	AAP-47(A)	Allied Joint Doctrine Development
kk.	AAP-32(B)	Publishing Standards for Allied Publications

ANNEX B - LEXICON

Part I – LIST OF ABBREVIATIONS

AAP	Allied administrative publication
ACINT	acoustic intelligence
AJP	Allied joint publication
CBRN	chemical, biological, radiological and nuclear
CCIR	commander's critical information requirement
CCIRM	collection co-ordination and intelligence requirements management
CI	counter-intelligence
CICA	counter-intelligence coordinating authority
C-IED	counter-improvised explosive device
COMINT	communications intelligence
EEI	essential elements of information
EEFI	essential elements of friendly information
ELINT	electronic intelligence
FFIR	friendly force information requirement
HUMINT	human intelligence
ICP	intelligence collection plan
IMINT	imagery intelligence
INTREP	intelligence report
INTSUM	intelligence summary
IR	information requirement
IRM&CM	intelligence requirement management and collection management.
ISR	intelligence, surveillance and reconnaissance
JIPOE	joint intelligence preparation of the operational environment
JISR	joint intelligence, surveillance and reconnaissance
KD	knowledge development
MASINT	measurements and signatures intelligence
NATO	North Atlantic Treaty Organization

NCIA	national counter-intelligence adviser
NCIR	national counter-intelligence representative
NIC	national intelligence cell
OPSEC	operations security
OSINT	open source intelligence
PIR	priority intelligence requirements
PMESII	political, military, economic, social, infrastructural and informational
RFI	request for information
SIGINT	signals intelligence
SUPINTREP	supplementary intelligence report
TECHINT	technical intelligence

Part II – Terms and Definitions

acoustic intelligence (ACINT): Intelligence derived from acoustic signals or emissions (AAP-06(2015)).

agency: In intelligence usage, an organization or individual engaged in collecting and/or processing information (AAP-06(2015)).

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. (AAP-06(2015)).

area of intelligence responsibility (AIR): An area allocated to a commander, in which he is responsible for the provision of intelligence, within the means at his disposal. (AAP-06(2015)).

area of operations (AOO): An area defined by the joint force commander within a joint operations area for the conduct of specific military activities. (AAP-06(2015)).

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 (AAP-06(2015)).

basic intelligence: Intelligence, on any subject, which may be used as reference material for planning and as a basis for processing subsequent information or intelligence. (AAP-06(2015)).

battle damage assessment (BDA): The assessment of effects resulting from the application of military action, either lethal or non-lethal, against a military objective. (AAP-06(2015)).

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.

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. (AAP-06(2015)).

communications intelligence (COMINT): Intelligence derived from electromagnetic communications and communications systems by other than intended recipients or users (AAP-06(2015)).

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. (AAP-6 (2015)).

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. (AAP-06(2015)).

current intelligence: Intelligence which reflects the current situation at either strategic or tactical level. (AAP-06(2015)).

deception: Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (AAP-06(2015)).

electronic intelligence (ELINT): Intelligence derived from electromagnetic non-communications transmissions (AAP-06(2015)).

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. (AAP-06(2015)).

forensic and biometric intelligence: Intelligence derived from the application of multi-disciplinary scientific or technical processes. (This term and definition are only applicable in this publication).

geospatial: Of or related to any entity whose position is referenced to the Earth (AAP-06(2015)).

geospatial information: Facts about the earth referenced by geographic position and arranged in a coherent structure. This includes topographic, aeronautical, hydrographic, planimetric, relief, thematic, geodetic, geo-referenced imagery, geophysical products, data, information, publications and materials. These will be available in either analogue or digital formats. [MC 296/1 (Not NATO Agreed)].

human intelligence (HUMINT): A category of intelligence derived from information collected and provided by human sources. (AAP-06(2015)).

indicator: In Intelligence usage, an item of information, which reflects the intention, or capability of a potential enemy to adopt or reject a course of action. (AAP-06(2015)).

information: Unprocessed data of every description, which may be used in the production of intelligence. (AAP-06(2015)).

information security: The measures required for the preservation of confidentiality, integrity and availability of information, in documentary, audible or digital formats from compromise. (This term and definition are only applicable in this publication).

integration: In intelligence usage, a step in the processing phase of the intelligence cycle whereby analyzed information and/or Intelligence is selected and combined into a pattern in the course of the production of further intelligence. (AAP-06(2015)).

intelligence (INTEL): 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. (AAP-06(2015)).

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. (AAP-06(2015)).

intelligence staff: Those personnel who are involved in the direction, collection, production and dissemination of intelligence through the conduct of the intelligence process. (This term and definition are only applicable in this publication).

interpretation: In intelligence usage, the final step in the processing phase of the intelligence cycle in which the significance of information and/or intelligence is judged in relation to the current body of knowledge. (AAP-06(2015)).

joint intelligence, surveillance and reconnaissance (JISR): JISR is an integrated intelligence and operations set of capabilities, which synchronises and integrates the planning and operations of all collection capabilities with processing, exploitation, and dissemination of the resulting information in direct support of planning, preparation, and execution of operations. (This term and definition modifies an existing NATO Agreed term and/or definition and will be processed for NATO Agreed status).

knowledge development (KD): The staff-wide process across all command levels to develop comprehensive situational awareness and understanding of the engagement space and make it available to civilian officials and military leaders to support decision-making throughout the NATO Crisis Management Process (MC 0600).

measurement and signature intelligence (MASINT): Intelligence derived from 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. (AAP-06(2015)).

medical intelligence: 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. (AAP-06(2015)).

open source intelligence (OSINT): Intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access. (AAP-06(2015)).

operational intelligence (OPINTEL): Intelligence required for the planning and conducting of campaigns at the operational level. (AAP-06(2015)).

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 are only applicable in this publication).

operations security: The process that gives a military operation or exercise appropriate security using passive or active means to deny an enemy knowledge of the dispositions, capabilities or intentions of friendly forces. (This term and definition are only applicable in this publication).

psychological operation (PsyOp): Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behavior affecting the achievement of political and military objectives (AAP-06(2015)).

protective security: The organized system of defensive measures instituted and maintained at all levels of command with the aim of achieving and maintaining security. (AAP-06(2015)).

physical security: That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, and documents and to safeguard them against espionage, sabotage, damage and theft (AAP-06(2015)).

reconnaissance (RECCE): A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy; or to secure data concerning the meteorological, hydrographical or geographic characteristics of a particular area. (AAP-06(2015)).

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 and definition are only applicable in this publication).

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 and definition are only applicable in this publication).

security (Sy): The measures necessary to ensure designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure. (AAP-06(2015)).

security intelligence: Intelligence on the identity, capabilities and intentions of hostile organizations or individuals who are or may be engaged in espionage, sabotage, subversion or terrorism. (AAP-06(2015)).

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. (AAP-06(2015)).

sociological and cultural intelligence: Concerns human geography, social and cultural factors including population parameters, ethnicity, social stratification and stability, public opinion, education, religion, health, history, language, values, perceptions and behavior. (This term and definition are only applicable in this publication).

signals intelligence (SIGINT): The generic term used to describe communications intelligence and electronic intelligence when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two. (AAP-06(2015)).

source: In intelligence usage, a person from whom or thing from which information can be obtained (AAP-06(2015)).

strategic intelligence: Intelligence required for the formation of policy, military planning and the provision of indications and warning, at the national and/or international levels (AAP-06(2015)).

subversion: Action or a coordinated set of actions of any nature intended to weaken the military, economic or political strength of a nation by undermining the morale, loyalty or reliability of its citizens. (AAP-06(2015)).

surveillance: The systematic observation of aerospace, surface on subsurface areas, places, persons or things by visual, aural, electronic, photographic or other means. (AAP-06(2015)).

tactical intelligence: Intelligence required for the planning and execution of operations at the tactical level. (AAP-06(2015)).

target (Tgt): The object of a particular action, for example a geographic area, a complex, an installation, a force, equipment, an individual, a group or a system, planned for capture, exploitation, neutralization or destruction by military forces. (AAP-06(2015)).

targeting: The process of selecting and prioritizing targets and matching the appropriate response to them taking into account operational requirements and capabilities. (AAP-06(2015)).

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 (AAP-06(2015)).

terrorism: The unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives (AAP-06(2015)).

INTENTIONALLY BLANK

AJP-2(A)(1)