

Lt. Col. Győző Csanádi:

## INFORMATION MANAGEMENT IN NATO (PART ONE)

### How NATO Defines and Organizes Information Management, Strategies and its Point of View

*ABSTRACT: As the level of technology is developing, more and more organizations realize that information is a critical resource. The special resource management where information itself is the resource, is called Information Management. Organizational level management systems can be tremendously complex and must be based on massive scientific and leadership pillars. That is why it is useful to have a closer look at what a multinational organization, namely the North Atlantic Treaty Organization (NATO), thinks about its own information management using accessible unclassified information. Thus, this paper aims at providing an overview of the information management system in NATO. The author is currently carrying out broader research and this paper is part of the scientific work titled "Possibilities and technics of the information management in the Hungarian Defence Forces supported by information technologies". This study is a small but important piece that must be put into the puzzle of the aforementioned research. Since information management is a huge and important topic within NATO, one single paper is unable to give a sufficiently detailed description of the subject. Hence, the publication has been divided into two parts. The first part – this paper – concentrates on the theoretical background and the strategic level of thinking. The second part will provide details about how rules and regulations work in practice.*

*KEYWORDS: information management, NATO*

## INTRODUCTION

### Information is a resource

As the level of technology is developing, more and more organizations realize that information is a critical resource. Comparing a classical resource, like money, energy, natural, etc. and information it is obvious that information is different from them. A long list can be made about differences but one thing is clear: a resource needs to be managed<sup>1</sup>.

With the continuous need for information and various ways of delivery, all organizations or individuals have the same issues to face: it is necessary to organize or create some management of information otherwise to fulfil the personal or organizational goals can become provisional or only a matter of luck. The special resource management where

---

<sup>1</sup> Munk, S. *Katonai informatika a XXI. század elején*. Budapest: Zrínyi Kiadó, 2007. 28–29.

information itself is the resource is called Information Management (IM), which is a very simple definition. This paper aims at defining this multi-layered notion of information.

Meanwhile an organization operates with several activities, some of them work with information and all processes have information aspects. It is really difficult to distinguish between information activities and information management activities, since IM itself is also a kind of information activity.

Obviously, several ways and strategies can exist in order to provide appropriate answers to the same question, the system of information management can be different.

When an individual thinks about the “atomic” level of IM or a great multinational organization wants to build up a complex information management, the outcome is definitely different. Organizational level management systems can be really complex and must be based on massive scientific and organizational pillars. That is why it is useful to have a closer look at what a multinational organization – in this case the North Atlantic Treaty Organization – thinks about information management.

## Why this publication was written

This paper aims at providing an overview about information management system in NATO. The author is working on a broader research titled “Possibilities and technics of the information management in the Hungarian Defence Forces supported by information technologies”. This paper is part of the aforementioned research. The same analysis of other organizations will create the basic knowledge how to tailor a good, working information management system.

Studying the subject, it becomes clear immediately that the chosen topic has a huge amount of far-reaching sub-questions with difficult interrelationships. Thus, the publication has been divided into two parts. The first part (this paper) concentrates more on the strategic level of the questions rather than the points of view at high level. The next publication will have a closer look at the practical level examining certain tools and technics advised by NATO-wide conduct of IM activities.

## Some words about NATO

The North Atlantic Treaty Organization (NATO) is a political and military alliance based on the North Atlantic Treaty signed on 4th April 1949. Being a multinational organization based on consensus, it is controlled by multinational committee boards and military commands. Currently 28 member states have an organized political and military representation. In NATO, the principal political decision-making body<sup>2</sup> is the North Atlantic Council (NAC). Concerning specific issues, there is a network of committees responsible for various aspects of the alliance work. All committees have a certain scope of their assigned issues. Since NATO has a political or military point of view about control measures, in NATO phraseology the word “consultation” always refers to political co-operation and the word “command and control” refers to the co-operation of multinational military organizations. The Consultation,

---

<sup>2</sup> The North Atlantic Council (NAC) is the principal political decision-making body of NATO. Each member country has a seat in the NAC. It meets at least once a week or whenever the need arises, at different levels. It is chaired by the Secretary General who helps members reach agreement on key issues. “What is NATO”. 26 December 2016. <http://www.nato.int/nato-welcome/index.html#>, Accessed on 26 December 2016.

Command & Control Board is one of the senior multinational policy bodies advising the NAC and the Defence Planning Committee<sup>3</sup>.

## SOURCES

### Sources are not easy to find

Because of the “need to know<sup>4</sup>” policy, NATO issues are not widely discussed by civilian authors, therefore this research is mainly based on NATO publications.

NATO publications have a certain hierarchy<sup>5</sup> at strategic level but the operational or tactical questions are published by the main headquarters or other organizations. Concerning NATO information management, STANAGs and other written policies and handbooks have been used as the main sources of secondary research. Despite the fact that the only sources available are NATO documents, all of them are unclassified, so the reader should not expect any revelation of secrets in this paper.

### NATO framework of Information Management

NATO has a declared aim to achieve Information Superiority<sup>6</sup>. This effort has brought the information and its management into an even sharper focus. In order to establish a coherent and coordinated way of NATO-wide information management processes, the North Atlantic Council has established a policy on Information Management in NATO, called “NATO Information Management Policy” (NIMP). NIMP highlights the importance of two NATO-wide capabilities in the area of sharing information and services. The two capabilities are the NATO and national Consultation, Command and Control (C3) and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). The framework of NATO IM is manifested in the system of various regulatory documents. A good description can be found about the framework of the information management in the document titled “The Primary Directive on Information Management (PDIM)<sup>7</sup>.”

<sup>3</sup> “NORTH ATLANTIC TREATY ORGANIZATION NATO HQ Consultation, Command & Control Staff”. NATO NC3 Staff. 26 December 2016. <https://nhqc3s.hq.nato.int/Default.aspx>, Accessed on 26 December 2016.

<sup>4</sup> “Need-to-know” is a principle of sharing NATO information in order to deliver information to whom it concerns regardless of the classification. This method of information delivery is a defensive measure.

<sup>5</sup> In this context, the word „hierarchy” means a specific order of creation and reference of documents and a hierarchy among the committees that are responsible for the promulgation of different papers.

<sup>6</sup> “Information Superiority” in this context means a relative advantage concerning possessed information. This is a capability to deliver the right information to the right people at the right time meanwhile decreasing the same capabilities of adversaries.

<sup>7</sup> North Atlantic Council. “C-M(2008)0113(INV): The Primary Directive on Information Management”. 18 December 2008.

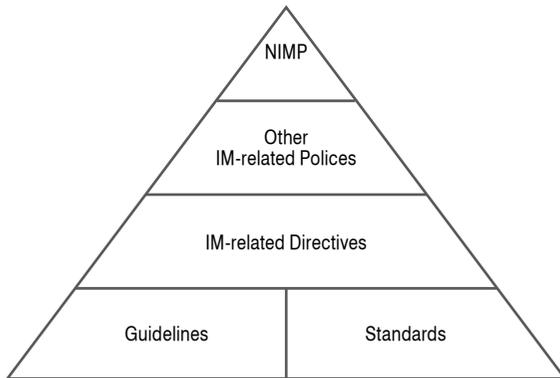


Figure 1: *NATO Framework of Information Management*<sup>8</sup>

## Processed Documents

The **highest level** document about NATO information management is the document of the North Atlantic Council, (C-M(2007)0118), titled “The NATO Information Management Policy (NIMP). The previous version of this document was PO(99)47.

After the master policy, several referring documents have been written and in order to create this publication the following relevant documents have been processed:

*“Other IM-related Policies” include the following documents:*

Security Within The North Atlantic Treaty Organisation (NATO) (C-M(2002)49)<sup>9</sup>:

North Atlantic Council publication. Establishes the basic principles of security to be applied by NATO including security programs in order to protect classified information.

The management of Non-classified Information (C-M(2002)60)<sup>10</sup>:

North Atlantic Council publication that establishes principles of protection and handling of non-classified NATO information<sup>11</sup>. This document supported the previous version of NATO Information Management Policy (NIMP) (PO(99)47)

NATO Public Disclosure Policy and Directive (C-M(2008)0116)<sup>12</sup>:

North Atlantic Council publication. Sets principles of the policy on the public disclosure of NATO information and establishes procedures, also roles and responsibilities.<sup>13</sup>

Policy on the retention and disposition of NATO Information (C-M(2009)0021)<sup>14</sup>:

North Atlantic Council publication. Sets policy of the retention and disposition of NATO information.<sup>15</sup>

<sup>8</sup> North Atlantic Council. “C-M(2008)0113(INV)”. ANNEX B: NATO IM Framework.

<sup>9</sup> “NATO UNCLASSIFIED” document, published by North Atlantic Council on 17 June 2002.

<sup>10</sup> “NATO UNCLASSIFIED” document, published by North Atlantic Council on 23 July 2002.

<sup>11</sup> North Atlantic Council. “C-M(2002)60: The Management of Non-classified NATO Information”. 23 July 2002. 1-1.

<sup>12</sup> “NATO UNCLASSIFIED” document, published by North Atlantic Council on 20 November 2008.

<sup>13</sup> North Atlantic Council. “C-M(2008)0116: Public Disclosure of NATO Information”. 20 November 2008. 3. 3.

<sup>14</sup> “NATO UNCLASSIFIED” document, published by North Atlantic Council on 2 March 2009.

<sup>15</sup> North Atlantic Council. “C-M(2009)0021: Policy on the Retention and Disposition of NATO Information”. 2 March 2009. 1. 1-1.

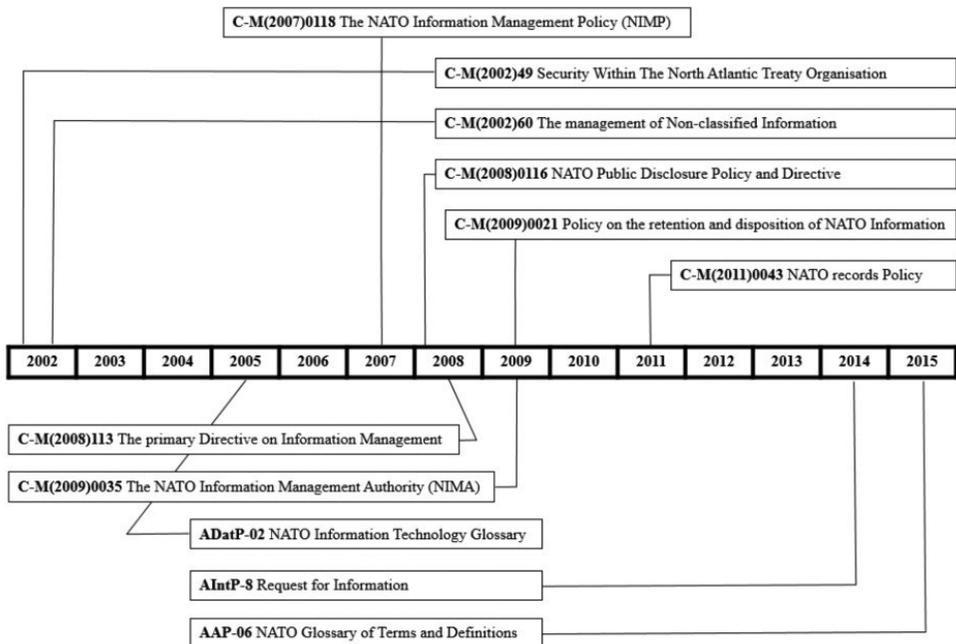


Figure 2: Years of publications processed in this paper.

NATO Records Policy (C-M(2011)0043)<sup>16</sup>:

Publication of North Atlantic Council. This policy “Establishes a framework to ensure that NATO records are handled effectively, efficiently and securely in order to serve the interests of NATO.”<sup>17</sup>

*IM-related Directives include the following:*

The primary Directive on Information Management (C-M(2008)113)

A directive of North Atlantic Council to support implementation of NIMP focusing on Information Superiority, roles and responsibilities and to enable development directives and guidance documents.<sup>18</sup>

The NATO Information Management Authority (NIMA) (C-M(2009)0035)<sup>19</sup>

North Atlantic Council’s organizational arrangements for IM within NATO containing establishment of NATO Information Management Authority and sets specific organization roles and responsibilities and relationship with other actors of IM.

<sup>16</sup> “NATO UNCLASSIFIED” document, published by North Atlantic Council on 28 June 2011.

<sup>17</sup> North Atlantic Council. “C-M(2011)0043: NATO Records Policy”. 28 June 2011. 6. 1-1.

<sup>18</sup> North Atlantic Council. “C-M(2008)0113(INV)”. 18 December 2008. 2. 1.

<sup>19</sup> “NATO UNCLASSIFIED” document, published by North Atlantic Council on 3 March 2009.

*Guidelines will be the subject of the future publication.*

*Standards include the following:*

Standards<sup>20</sup> are represented by Standardization Agreements (STANAG). All STANAGs have to be developed and implemented by NATO bodies and national authorities. The management of standardization is carried out by NATO Standardization Organization (NSO).

The following standards must be quoted and used in both publications:

NATO Information Technology Glossary (ADatP-02)<sup>21</sup>:

A bilingual<sup>22</sup> standard on the terminology of Information Technology.

Request for Information (AIntP-8)<sup>23</sup>:

An allied Intelligence Publication that standardizes the method how and who passes Requests for Information. This standard is connected to intelligence information processes, which differs from the IM principles in process and aim but the subject of the standard is also an information activity.

NATO Glossary of Terms and Definitions (AAP-06)<sup>24</sup>:

Contains NATO-agreed terms and definitions in order to have NATO-wide standardized terminology.

Joint Publications is discussed in an independent chapter of this paper that is why these sources are not in the table.

## DEFINITIONS AND BASICS

In order to understand strategic or any level concept of the Information Management, it is necessary to clarify exactly what is meant by the term “information” and “information management” in NATO.

The term “information” embodies the multitude of concepts, which depend on its role.

In the official NATO Glossary of terms and definitions (AAP-06), the definition of the term “information” is the same<sup>25</sup> as AJP-2<sup>26</sup> formulates. In accordance with this approach, information should be “any unprocessed data”. However, NIMP gives another definition<sup>27</sup> that states that information is “any communication or representation of knowledge”. Furthermore, to give illustration to the accurate quotations are as follows:

<sup>20</sup> To lay down and elaborate principles to guide actions of military forces. In support of objectives, NATO has a top-down standardization process. This process is to enhance interoperability of organizations.

<sup>21</sup> “NATO UNCLASSIFIED” document, published by NATO Standardization Agency on March 2005.

<sup>22</sup> English and French are the official languages of NATO. The text appears on two sides of the page in different languages: in English on the left hand side and in French on the right.

<sup>23</sup> “NATO UNCLASSIFIED” document, published by NATO Standardization Office (NSO) on 28 August 2014.

<sup>24</sup> “NATO UNCLASSIFIED” document, published by NATO Standardization Office (NSO) on 17 November 2015.

<sup>25</sup> Unprocessed data of every description, which may be used in the production of intelligence.

<sup>26</sup> “AJP-2: Allied Joint Doctrine for Intelligence, Counterintelligence and Security”. NATO Standardization Office (NSO). 22 February 2016. All important strategic level doctrines will be introduced later in the text.

<sup>27</sup> Any communications or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual forms.

## Definitions of information from the point of view of intelligence:

“information is merely an assemblage of collected data”<sup>28</sup>

information is defined as “Unprocessed data of every description, which may be used in the production of intelligence.”<sup>29</sup>

## Definition of information in the NIMP:

“Any communications or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual forms”<sup>30</sup>.

### *Analysis*

The first case is the “intelligence style” definition. Here the noun “information” means a kind of “special fuel” of a specific system described in the intelligence doctrine. From this point of view, the focus is on the content and the purport of the information. In other words, what the information contains or carries. Both these definitions emphasize how important resource the information is.

In the second case, when the management of information is the subject of the inquiry, information as a phenomenon becomes the subject. This approach concentrates on the role of information without regard to the accurate content or meanings that information carries or conveys.

However, the two points of view are different but one identical moment is shared in both definitions. Namely, information is something important that builds some kind of knowledge. The first approach deals with the certain knowledge, while the second one is more general and does not concentrate on what the purpose of the information is, but tries to define how to deal with any kind of information.

### *Definitions of IM*

Hence, these different points of view impact on the notion of Information Management. The intelligence gives a long definition and description of IM:

“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.”<sup>31</sup>

This definition considers IM as a process. The most characteristic words in the text are nouns and verbs expressing activities. A process is a serial of basic activities. That is

<sup>28</sup> “AJP-2”. 2.6/1. 2-5.

<sup>29</sup> “AJP-2”. B-4.

<sup>30</sup> North Atlantic Council. “C-M(2007)0118: The NATO Information Management Policy (NIMP)”. 11 December 2007. 1-4.

<sup>31</sup> “AJP-2”.

why the text sets sequences that are made up of activities like “supervision; administration; regulation; dissemination” or “receive; store; manipulate; disseminate”. These sequences of activities are the steps of the information process.

It is also important to note that the publication highlights the fact that information management is not an “art of art” separate process<sup>32</sup> but is a part of an effort to provide proper information in time.

On the other hand, the concept of NIMP defines the term IM as follows:

**“A discipline that directs and supports the handling of information thorough its life-cycle ensuring it becomes the right information in the right form and adequate quality to satisfy the demands of an organization”<sup>33</sup>**

The main statement of this definition is that IM is a discipline. Moreover, information has a life-cycle like a living creature. Meanwhile verbs ergo activities appear in the definition like “direct”; “support”; “ensure”; “satisfy”. However, these activities refer to the role of the “discipline”, as IM is defined. The second part puts the emphasis on the results that a good working IM must achieve: the information must be the “right information” in the “right form” and in the “adequate quality”. The definition does not explicitly mention specific series of activities but it does not mean the definition does not care about information processes. The process appears in the notion of “life-cycle of information”.

### *Differences are superficial*

Along with the fact that both definitions refer somehow to series of activities either with explicit listing or referring to a cyclic process, later in the text it will be important to put information processes under the objective lens of science.

In conclusion of the comparison of IM definitions, I must say that the main goals of the two definitions are identical, that is to provide the right information according to the demands of an organization.

Hence, in the two definitions there is no significant difference between the aims but in the “NIMP version” activities about information are organized in a cyclic way meanwhile the other approach does not make any effort to systemize activities. The reason is the same as mentioned above relating to the notion of information. The main purposes are different; NIMP concentrates on the generalization of IM while the intelligence-style thinking considers IM as a tool to serve intelligence process. In other words, NIMP has a resource-management point of view where information itself is a resource meanwhile “intelligence” definition is part of a specific information process, where the “protagonist” is not the information but the intelligence and the information is just one of the important factors. This difference is a good example illustrating how Information Management differs from other information processes.

## Flows and cycles, sunrise-sunset

Nowadays the modern – rather post-modern – person considers the flow of time as linear progress, starts with a forgotten enigmatic point and keeps going into the far, unthinkable future. But this was not the same in the past and we still have remains of cyclic time vision. In the natural environment of the Earth, life has a repetition of events: continuous cycles

<sup>32</sup> In the text expressed as follows „Information management should not be regarded as a separate process in its own right”.

<sup>33</sup> North Atlantic Council. “C-M(2007)0118”. 1-4.

of days and nights, cycles of seasons and the repeating life stages from childhood through maturity until hoariness.

This was the most fundamental experience of mankind for thousands of years, from generation to generation. That is the reason why repetitive acts are worth describing in a cyclic way. When the order and time are important factors of the arrangement of activities, we can distinguish two basic types:

- serial arrangement – flow
- repetitive arrangement – cycle

All other difficult structures of order of activities derive from these two basic elements<sup>34</sup>.

Moreover, the examination of information processes and their repetitive or serial nature can provide significant takeaway concerning the understanding of IM strategies.

## The information life-cycle

As it was shown in the definition of IM, in NIMP the concept of information life-cycle was introduced:

“The life-cycle of information encompasses the stages of planning, collection, creation or generation of information; its organization, retrieval, use, accessibility and transmission; its storage and protection; and, finally, its disposition.”<sup>35</sup>

Later, in the document PDIM the life-cycle has further elaboration as well as a graphical interpretation.

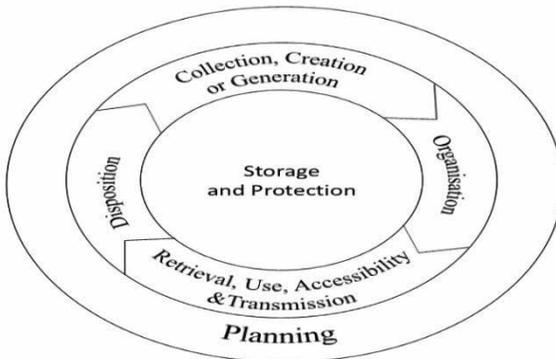


Figure 3: *the information life-cycle*<sup>36</sup>

Analysing the graphical abstraction it becomes clear that not all the activities are part of the repetitive serial only “Collection, Creation or Generation”; “Organization”; “Retrieval, Use, Accessibility and Transmission”; and “Disposition”. The two others, namely: “Planning”; and “Storage and Protection” are necessary to embrace all cycles. That means that all other four have their own connection or phase of “Planning”, and “Storage and Protection”. In other words, storage and protection are continuously necessary pillars of the cycle while all repetitive phases must have their own phases in planning.

<sup>34</sup> For example a “spiral”, which is a combination of cyclic but continuously developing processes.

<sup>35</sup> North Atlantic Council. “C-M(2007)0118”. 1-5.

<sup>36</sup> North Atlantic Council. “C-M(2008)0113(INV)”. ANNEX-A 1-A-1.

Later, in the document titled “NATO Information Management Manual”<sup>37</sup> the model has a short description where it is highlighted that stages in the model can overlap and may occur in increments and in different order.

According to this notice, a lifecycle owns a great flexibility. Although the cyclic approach is a good general description but it is not compulsory to insist on the order of all elements.

The summary of the aforementioned phases of the information lifecycle is as follows:

The **storage and protection** ensures the persistence of the information regardless of the medium or format. It may be classical paper, or other electronic ways of storing. On the other hand, the protection of the information handler ensures confidentiality.

The **collection, creation or generation** are ways how information is born. All individuals or organizations within NATO can conduct this activity as part of normal business processes in accordance with IM framework.

**Organization** is a stage for the preparation of information to be accessible, exploitable and capable of disposition. The organization must find a standardized way to ease discoverability and accessibility of the information parallel with the application of the necessary protection.

**Retrieval, use, accessibility and transmission** comprise the phase when the information is used. It ensures the discoverability and provides the exploitation of information.

**Disposition** means transfer the information to archives or destroy it.

**Planning** is the activity to prepare efficient plans about all phases of the information lifecycle considering the mission requirements.

## OBJECTIVES, PRINCIPLES, AND IMPLEMENTATIONS

### Establishment of leading

As it was shown, the NATO Information Management Policy is the top of the NATO IM framework pyramid. In the background of this document is the main initiator, the Riga Summit<sup>38</sup> at the end of 2006. The Heads of State and Government agreed among others on the support Information Superiority. The North Atlantic Council (NAC) approved the NIMP in 2007 and assigned the NATO Consultation Command and Control Board (NC3B) as the lead Council Committee in NATO for IM.

Furthermore, it is important to notice that the NC3B is not the only committee related to IM. The NAC named the following other committees to be coordinated:

- NATO Military Committee
- Political Committee
- NATO Security Committee
- NATO Archives Committee

<sup>37</sup> North Atlantic Council Archives Committee. “AC/324-D(2013)0001: NATO Information Management Manual”. 7 March 2013.

<sup>38</sup> “Riga Summit Declaration”. 29 November 2006. 1. <http://www.nato.int/docu/pr/2006/p06-150e.htm>, Accessed on 29 November 2006.

## Three key objectives

The NIMP lays down the three key objectives of Information Management to support:

- 1.) the achievement of Information Superiority primarily within an information sharing networked environment;
- 2.) effective and efficient use of information resources;
- 3.) identification and preservation of information of permanent value to NATO.

## Seven principles

The document sets out principles<sup>39</sup>. These principles are explained in one or two sentences.

**Information is a Corporate Resource:** Information shall be managed as a corporate (NATO) resource in all processes, regardless of the medium or format in which the information is held.

**Information Ownership and Custodianship:** Means, that all information shall have an originator and clearly defined ownership and custodianship.

**Leadership and Organizational Structure:** This principle regards IM as a fundamental responsibility, which requires executive leadership and organizational structure.

**Information Sharing** is one of the most important principles and indicates a significant turn in the thinking about information sharing. On the contrary of earlier stranglehold of restrictions, “information sharing” means moving emphasis to the “responsibility to share” balanced by the old preference “need-to-know”

**Information Standardization:** in order to promote interoperability and co-operation, information shall have standardized structures.

**Information Assurance** is a principle of protection as the set of measures of Defence with respect to confidentiality, integrity, availability, non- repudiation and authentication.

**Information Needs** is a principle about planning and architecture processes through information needs shall be determined.

To sum up the principles, we can state:

Information is a corporate resource that needs to have a defined owner, a custodian, tasks assigned to the leaders as well an organized structure responsible for the management of information.

Information shall be handled in standardized structures to enhance interoperability by the aforementioned personnel in the structure through its lifecycle in a protected way but all information shall be shared according to responsibility to share. In order to know the requirements, leaders must plan their information needs.

## How to implement

The PDIM defines IM implementation in three big groups according to the NIMP key objectives of NATO IM.

<sup>39</sup> Principles are the following: Information is a Corporate Resource; Information Ownership and Custodianship; Leadership and Organizational Structure; Information Sharing; Information Standardization; Information Assurance; Information Needs.

## Support of information superiority

In this section, PDIM highlights the importance of planning and follow-on plans, and gives guidance how to identify key elements of planning such as when, what format and to whom the information must be provided.

In order to keep operations continuous, NATO bodies must identify and develop procedures to ensure mission-critical IM activities.

## Effective and efficient use of information resources

The use of information resources must be organized in a standardized way. In accordance with the PDIM, using metadata is titled as a key enabler for effective and efficient information sharing. Metadata describe and categorize information. They contain data about ownership and custodianship, protection and access control, retention and disposition, re-usability and comprehensibility, discoverability, and permissible values. Permissible values refer to the content of the information with controlled vocabularies, taxonomies, ontologies and topic maps. This bunch of categories helps users to categorize and find information. All in all, metadata give information about information, help to find and use information. Since metadata must have a collective value, all bodies have to co-ordinate with the IM authority.

Networking and Information Infrastructure (NII) is considered as a key enabler of sharing and re-using information. In order to have an appropriate system, the PDIM emphasizes the importance of NATO standards.

As for systems and services in general, the PDIM gives some overall advice on the easy access of information, e.g. timing, availability etc.

The organizational culture is also considered a key enabler of efficient IM. The importance of training is highlighted as well. In order to build greater organizational culture, individuals must be trained, and awareness of IM must be built.

## Identification and preservation of information of permanent value

This expression contains the obligation of classification of information in the aspect of preservation. All information must be classified as permanent or temporary value and must assign a proper retention period. Information classified as having permanent value must be archived.

## ROLES AND RESPONSIBILITIES

The most important message in the documentation about IM is that information management is not a specific issue for specific IM organizations, but all individuals in NATO working with information must consider information as a corporate resource and recognize that IM is an integral element of work.

The North Atlantic Committee (NAC) is the body that shoulders the responsibility for setting the policy of NATO-wide information management. As it was mentioned before, the NATO C3 board is accountable to the NAC for the coherent implementation of IM. Nations are to agree about policies (NIMP) and encouraged to adopt and execute related policies.

**Individuals and information Originators**<sup>40</sup> and national authorities are addressed to follow the aforementioned principles and must apply and follow relevant rules and standards.

**Information owners** are responsible for setting rules of handling data and possible transferring of ownership.

**The North Atlantic Council** is addressed to monitor and ensure coordinated implementation of the policy and must coordinate among all NAC Policy bodies<sup>41</sup>.

**The NC3 Board and subordinates' tasks.**

The NC3B has three layers<sup>42</sup>

- decider;
- adviser;
- provider.

The decider is the NC3B itself.

The adviser layer consists of four so-called Capability Packages (CaP). A specific capability, like “network and security” or “data management” is a Capability Target (CaT). In other words, a CaT is a specific issue that builds a capability for NATO. CaT-s are grouped according to their characteristic values. The name of this group is Capability Package.

Providers are Capability Targets (CaT) themselves. Although there are some CaTs not put into Packages, they remain under the direct control of the Board.

Information Management has an independent organization within the NC3B as it will be elaborated below.

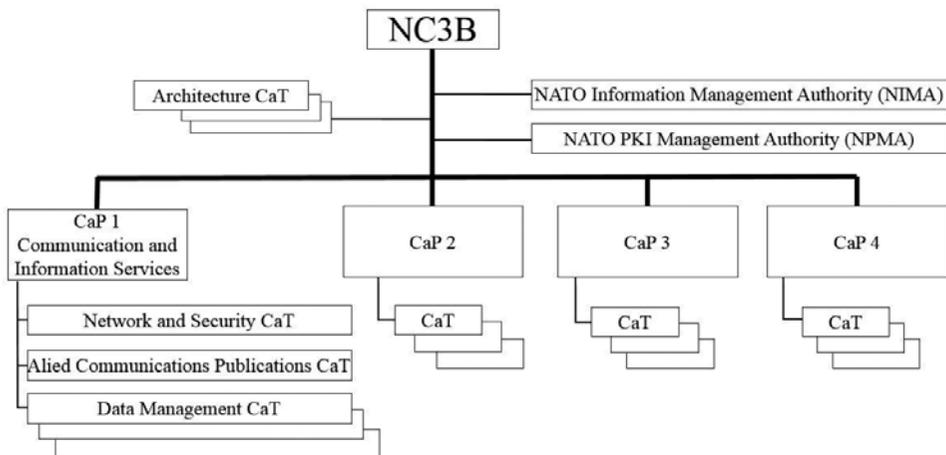


Figure 4: Overall structure of NATO's C3 Board<sup>43</sup>

<sup>40</sup> Originator is the nation or international organisation under whose authority the information has been produced or introduced into NATO. Information Owner in the NATO context means same entity to Originator.

<sup>41</sup> NAC policy bodies: NATO Military Committee; Political Committee; NATO Security Committee; NATO C3 Board; NATO Archives Committee.

<sup>42</sup> NATO NC3 Staff.

<sup>43</sup> Extraction and simplification of NC3 Board published figure. NATO NC3 Staff.

In 2009, to foster the Primary Directive (2008) and based on the principle of “**Leadership and Organizational Structure**”, a coordinated and synchronized approach was introduced. The IM lead council committee, the NC3B proposed a decentralized system of responsibilities with the establishment of NATO Information Management Authority (NIMA). The organizational arrangement for IM within NATO was published by the North Atlantic Council in document C-M(2009)0035(INV) – The NATO Information Management Authority (NIMA).

The Authority was created in a similar pattern to NATO Public Key Infrastructure Management Authority (NPMA) and the Cyber Defence Management Authority (CDMA). The NC3B retains the primary responsibility for assessing the IM capabilities of the Alliance. Consequently, NIMA has become the authority implementing NIMP and PDIM within NATO.

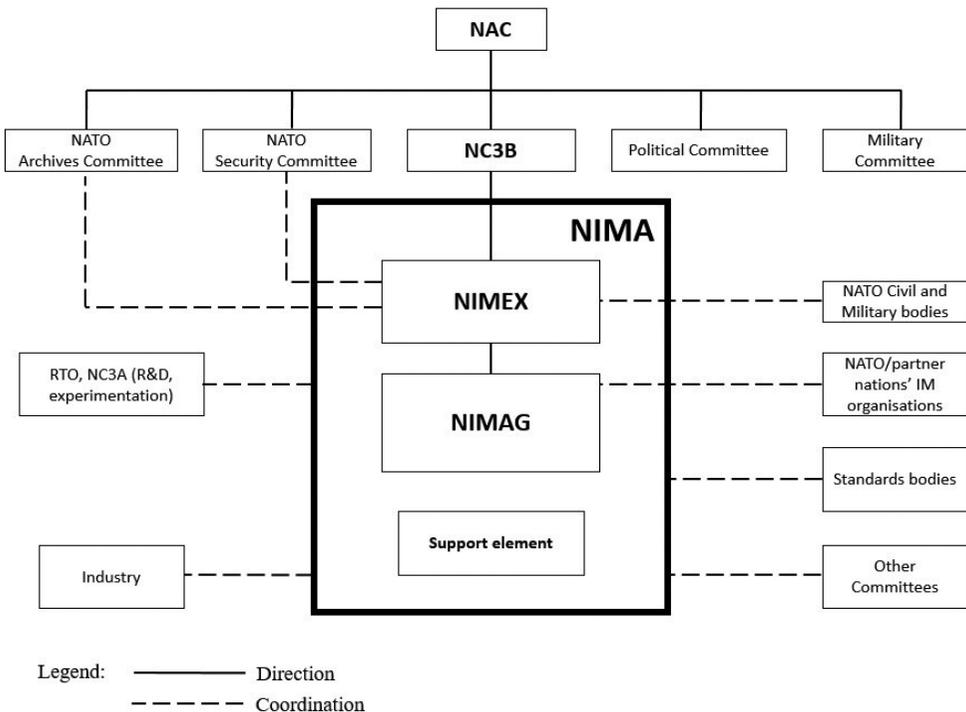


Figure 5: The structure of NATO Information Management Authority<sup>44</sup>

As shown above in Figure 4, NIMA is comprised of the following components:

**NATO IM Executive body (NIMEX)** This body is constituted for consultation at strategic and political levels. NIMEX is chaired by Director NHQC3S<sup>45</sup> and the members are the Senior IM officials of NATO bodies and representatives of relevant Committees.

<sup>44</sup> North Atlantic Council. “C-M(2009)0035 (INV): The NATO Information Management Authority (NIMA)”. 03 March 2009. ANNEX 1 ENCLOSURE. 1-1-3.

<sup>45</sup> NHQC3S: NATO HQ Consultation, Command & Control Staff. NATO staff organization for analysis, advice and actionable recommendations to Nations and NATO Bodies that will lead to the delivery of C4ISR capabilities needed to support Alliance operations and missions and enable Alliance transformation. NATO NC3 Staff.

**NATO IM Advisory Group (NIMAG)** This body is established for co-ordination at technical and operational levels. NIMAG is chaired by the Branch Chief of NATO HQ Information Services Branch, and the participants are Information Managers and other SME<sup>46</sup>-s from the NAC Council Committees. This body provides advice and support to NIMEX and is not a decision-making organization.

**NHQ3S Support Element** NHQ Information Services Branch that existed before NIMA created to support the new organization. Figure 5 describes the co-operation and direction of IM-relevant organizations and subsequent bodies.

**The NATO Archivist:** Appointed by the Secretary General and reports to the Archives Committee. The Archivist coordinates, develops, and ensures long-term preservation and accessibility of information with permanent value.

**The heads of NATO bodies** as leaders must ensure that the relevant policies should be effective. They support the processes with training and appointment of IM senior officials. Also, it is their responsibility to identify and protect essential information.

**Tasks of IM Senior Officials:** Appointed by and responsible to the head of NATO military or civilian body to ensure the implementation of IM and are supported by appropriate staff, IM Senior Officials will:

- establish IM Plan;
- ensure coordinated IM improvements;
- evaluate and report;
- provide proper environment of information across different management and security domains;
- ensure implementation of IM framework;
- implement and maintain IM education;
- liaise in order to define and develop IM;
- agree on service levels with information service providers.

The IM Senior Officials should minimum be supported by the following services to ensure that they could meet the specific obligations of PDIM:

- Security services in the area of information assurance;
- Archives services in the area of preservation of information;
- Registry services in the area of cataloguing and control and dissemination of information;
- Library services in the area of acquisition and availability of external information;
- Training services in the area of IM education;
- Communication and Information Systems (CIS) in the area of effective and interoperable working of CIS infrastructure.

**Tasks of information managers:** Information managers support the IM Senior Official in the execution of the IM Plan and help the staff in the execution of IM related tasks.

The information managers' tasks cover all tasks assigned to the IM Senior Official but Information managers directly contribute to tasks directed by the IM Senior official.

<sup>46</sup> SME: Subject Matter Expert.

## HOW IM IS REFLECTED IN DOCTRINES

### Stones rolling

In order to lay down top level principles of NATO military operations, high-level conceptual papers called Allied Joint Doctrines (AJP) have been introduced. Among Allied Joint Doctrines, it is possible to recognize a certain hierarchy. On the top of the hierarchy a so-called "capstone" document can be found. The AJP-01(D) Allied Joint Doctrine contains the main principles of allied working and all other doctrines are derivatives of this capstone document. To cover a specific area, subordinated "keystone" documents have been created like AJP-3 Allied Joint Doctrine for the conduct of operations. The numbering of these documents more or less follows the logic of J-G-S structure of NATO-command HQs.

identifier	title	latest version	level
AJP-01	Allied Joint Doctrine	2017	capstone
AJP-2	Allied Joint Doctrine for Intelligence, Counter Intelligence and Security	2016	keystone
AJP-3	Allied Joint Doctrine for the Conduct of Operations	2011	
AJP-4	Allied Joint Logistic Doctrine	2003	
AJP-5	Allied Joint Doctrine for Operational-level Planning	2013	
AJP-6	Allied Joint Doctrine for Communication and Information Systems	2011	

Figure 6: table of the most important AJPs processed in this paper

The current structure of Allied Joint Doctrines including subordinated and derived publications is well described in a chart named Allied Joint Doctrine Architecture (AJDA). The AJDA including all NATO unclassified STANAGs can be reached for registered<sup>47</sup> users on the webpage of NATO Standardization Office<sup>48</sup>.

NATO High level STANAGs are not to deal with information management directly but contain important factors and requirements.

### Allied Joint Doctrine

The capstone document, **Allied Joint Doctrine AJP-01(D)**<sup>49</sup> denominates information as the "fourth corner<sup>50</sup> of the instruments of national power"<sup>51</sup>. This so-called "corner" receives

<sup>47</sup> Registration is available for any NATO members' official organizational e-mail address after a short period of authorization process. <https://nso.nato.int/nso/sosite/requestmember.html>, Accessed on 28 May 2018.

<sup>48</sup> NATO Standardization Office (NSO) webpage. <https://nso.nato.int/protected/index.htm>, Accessed on 28 May 2018.

<sup>49</sup> "NATO UNCLASSIFIED" document, published by NATO Standardization Agency on 21 December 2010.

<sup>50</sup> According to the AJP-1 the three corner of countries power are the diplomacy, economic power, and the military power.

<sup>51</sup> "AJP-01(D): Allied Joint Doctrine". NATO Standardization Agency (NSA). 21 December 2010. 0106. 1-2.

the name of “information instrument”<sup>52</sup>. The word “information” in the context of AJP-01 is mainly to express the importance and a key factor of interoperability. This point of view refers to and enforces the NIMP principles of “Corporate Resource” and “Information needs”. Another aspect of the usage of information is mentioned in the publication named Information Operations<sup>53</sup>. AJP-01(D) does not explicitly mention or regulate IM.

As the summary of AJP-01(D), it can be stated that this doctrine highlights the importance of information and its essential role in interoperability but directly does not interfere in the matters of IM.

## Allied Joint Doctrine for Intelligence, Counter Intelligence and Security (AJP-2)<sup>54</sup>

This doctrine is deeply involved in the topic of information and information management.

In Chapter 2.1 of AJP-2 as part of the “Contemporary Intelligence engages relationship of data and information”, the document gives a special definition of the information that slightly differs from the definition given in NIMP as it was explained in Chapter “DEFINITIONS AND BASICS” of this paper. This point of view is based on a process named Intelligence Cycle.



Figure 7: *The Intelligence Cycle*<sup>55</sup>

The Intelligence Cycle is “the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available for users”,<sup>56</sup> and it has four stages:

- 1.) **Direction** – the determination of collection;
- 2.) **Collection** - the exploitation of (information) sources;

<sup>52</sup> The information instrument is „adjacent to, and supporting the three instruments of national power” (diplomacy, economic, military) “focused on countering adversarial information and information systems, while defending the Alliance’s own, and is therefore largely coordinated by Information Operations (Info Ops)”. “AJP-01(D)”. 0110. 1-3.

<sup>53</sup> Information Operation is “a staff function to analyse, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC approved audiences in support of Alliance mission objectives.” “AJP-3.10: Allied Joint Doctrine for Information Operations”. November 2009. 0108. 1-5.

<sup>54</sup> “NATO UNCLASSIFIED” document, published by NATO Standardization Office (NSO) on 22 February 2016.

<sup>55</sup> Based on “AJP-2”. Figure 2 (4-2), reprocessed by author in order to be similar to the information life-cycle.

<sup>56</sup> “AJP-2”. B-5.

**3.) Processing** - the conversion of information meaningful for intelligence;

**4.) Dissemination** - the timely conveyance of intelligence to those who need it.

The Intelligence Requirement Management and Collection Management (IRM&CM) process monitors and coordinates the four stages of the Intelligence Cycle.

Altogether, this cycle is an information process where information is the object and aim of a specific (intelligence) activity. In this way this approach and definition derived is not a competitive or alternative definition of IM but as a specific process, it is a particular part of the IM as a whole.

Also, an important and frequently used notion concerning IM is the “Request for Information (RFI)”. The RFI is part of a bigger category called Intelligence Requirements Management (IRM), which is similar to IM as both control processes and the information is in the centre of processes.

The commander’s task is to determine the type of required information in the Intelligence Requirements Management. The IRM should contain details of the nature of information required, with priority. IRM considers availability of information and whether it is necessary to collect.

The RFI is a term that describes an intelligence requirement. It is used when the commander wants to use intelligence resources that are not available. In practice it means that the answer will be provided by a superior or adjacent organization.

As a summary of AJP-2, information and data have been treated as coherent notions IM is a process that serves the information process cycle of intelligence.

### Allied Joint Doctrine for the Conduct of Operations, AJP-3(B)<sup>57</sup>

AJP-3 is to describe fundamental principles of joint operations at operation level. In the chapter where this doctrine deals with execution, transition and termination<sup>58</sup>, two IM related notions are introduced: the Commander’s Critical Information Requirements and the Information Management itself as a technique to organize the Battle Rhythm.

### Commander’s Critical Information Requirements (CCIR):

“Properly developed information requirements ensure that subordinate and staff effort is focused, scarce resources are employed efficiently, and decisions can be made in a timely manner. Information requirements focus on friendly forces, the operational environment or the adversary. The commander will identify only those information requirements, which are particularly important to him. Therefore CCIRs are limited since they must be linked to the critical decisions the commander anticipates making. This focuses the commander’s subordinate commanders’ and staff’s planning and collection efforts”<sup>59</sup>

According to the doctrine, in the centre of the effort of an effective IM are the CCIRs, and IM directs the processing, flow and use of information.

The notion of Battle Rhythm is introduced as a 24-hour repetitive routine of meetings, briefings and miscellaneous gatherings. This time-controlled work intends to reach

<sup>57</sup> “NATO UNCLASSIFIED” document, published by NATO Standardization Agency (NSA) on 16 March 2011.

<sup>58</sup> “Chapter 4 – Execution, Transition and Termination”. In NATO Standardization Agency (NSA). “AJP-3(B): Allied Joint Doctrine for the Conduct of Operations”. 16 March 2011. 1-23.

<sup>59</sup> “AJP-3(B)”. 0415. 4-5.

an optimal performance of the staff. At the meetings several tools are used to present and make a common understanding of the information collected. One of them, the Situational Awareness is to understand operating environment in the context of the ongoing mission. This geospatial representation of force and other supporting information is essential to a common understanding of the situation and decision-making.

Information Management is introduced as a technique used to aid shared Situational Awareness among Synchronization Matrix<sup>60</sup>, Mission Rehearsal<sup>61</sup>, Mission Essential Checklists<sup>62</sup> and War-gaming<sup>63</sup>.

**“Information Management (IM).** JFCs make decisions based on their understanding of the operational environment. The role of IM, then, is to provide a timely flow of relevant information that supports all aspects of planning, decision-making, and execution; to include all activities involved in the identification, collection, filtering, fusing, processing, focusing, disseminating, and using information. Information management officers (IMOs) assemble information that promotes understanding of the information environment and enable the JFC to better formulate and analyse COAs<sup>64</sup>, make decisions, execute those decisions, and understand results from previous decisions.”<sup>65</sup>

As the summary of AJP-3, the main factor of the various aspects of the information is the critical importance (CCIR), and IM has a supporting role as a technique to facilitate information activities. In this doctrine, Information Management Officers (IMOs) are named explicitly and specific tasks are assigned to them. It is important that IM is considered as an activity that provides timely delivery of information and IMOs are responsible for supporting this activity.

**Allied Joint Logistic Doctrine, AJP-4(A)**<sup>66</sup> does not really deal with information and its management.

Information as an important entity appears among principles as part of the principle “simplicity”: “simple reporting mechanisms ensure the accurate and efficient dissemination of information to all those who require it”<sup>67</sup>. In this manner, the text harmonizes with NIMP principle of “Information Sharing” and “Information Standardization”.

In AJP-4(A), the word “information” later appears mainly in the context of Information and Logistic Information Systems.

**Allied Joint Doctrine for Operational-level Planning (AJP-5).**<sup>68</sup> To the contrary of AJP-3B, this doctrine concentrates on planning joint operations instead of principles of conduct of operations.

<sup>60</sup> Synchronization Matrix is a matrix showing broad order activities. “AJP-3(B)”. 0441/b. 4-15.

<sup>61</sup> Mission Rehearsal is a technique to conduct walk-through activities in the mission. “AJP-3(B)”. 0441/c. 4-15.

<sup>62</sup> Mission Essential Checklists are matrixes containing actions and sequences including anticipated outcome concerning the mission success. “AJP-3(B)”. 0441/d. 4-16.

<sup>63</sup> War-gaming is an activity when the planned activities are modelled in a mathematically abstracted way in order to estimate success of plans. “AJP-3(B)”. 0441/e. 4-16.

<sup>64</sup> COA: Course of Action, an important element of planning process.

<sup>65</sup> “AJP-3(B)”. 0441/a. 4-15.

<sup>66</sup> “NATO UNCLASSIFIED” document, published by NATO Standardization Agency on December 2003.

<sup>67</sup> “AJP-4(A): Allied Joint Logistic Doctrine”. NATO Standardization Agency (NSA). December 2003. 0105/h. 1-4.

<sup>68</sup> “NATO UNCLASSIFIED” document, published by NATO Standardization Agency (NSA) on 26 June 2013.

In this doctrine information is considered as one of the operational level factors among time, space and forces.<sup>69</sup> Information as an operational factor must be considered through the whole planning process. Time, space and forces as traditional operational factors are linked with the fourth factor: the sphere of information. An interesting notification can be found about the importance of information that says that in today's operation instead of the quantity the orientation of information is important. That aspect of "orientation" reflects the basic role of information management.

Meanwhile, the doctrine does not explicitly defines or cares about IM as defined in PDIM but the emphasis on the importance of the correct information process and flow of information is a repetitive part of the document. The notion of information appears in the text in the connotation of critical information, information operations, and information systems and Strategic Communication<sup>70</sup> as well.

As a summary, AJP-5 introduces a new expression about information, the "information sphere" and although it expresses the importance of managed information flows, IM as defined in PDIM does not explicitly appear in the text.

**Allied Joint Doctrine for Communication and Information Systems (AJP-6).**<sup>71</sup> The declared purpose of this Doctrine is to provide guidance of integration, Communication and Information Systems (CIS) for allied joint operations including a set of roles and responsibilities and desirable characteristics of CIS in order to support operational commander's command and control (C2).

This doctrine approaches the information and its management from the point of view of CIS. AJP-6 clearly defines the term "communication system"<sup>72</sup> and "information system"<sup>73</sup>

According to its text, "an information system is an assembly of equipment, methods, and procedures and, if necessary, personnel, organized to accomplish information processing functions"<sup>74</sup>

Among the terms, information is called a "vital corporate resource" and with the direct quotation of NIMP, six key principles of IM are included in the text. NIMP contains seven principles (see: Chapter 3).

Information management as a notion appears as Communication and Information Systems Principle in the company of "Communication and Information Systems Structure" Economy of CIS Employment, Interoperability, Flexibility, Information Assurance, Spectrum Management, Data Security, Timeliness, Information Sharing, Prioritization, Resilience, and Capacity.

According to AJP-6, the Communication and Information Systems Information Management is defined as a discipline referring to the flow of information. Activities named in connection with IM are the following:

- gathering;
- storing;
- processing;
- directing;
- reporting.

<sup>69</sup> "AJP-5: Allied Joint Doctrine for Operational-level Planning". NATO Standardization Agency (NSA). 26 June 2013. 0225. 2-21.

<sup>70</sup> Strategic Communication: "Militarily it is the coordination of communications and information activities and products to support the creation of desired effects and the achievement of the commander's objectives". "AJP-5: Allied Joint Doctrine for Operational-level Planning". 26 June 2013. 0107/1. 1-7.

<sup>71</sup> "NATO UNCLASSIFIED" document, published by NATO Standardization Agency (NSA) on 6 April 2011.

<sup>72</sup> Communication system is "an assembly of equipment, methods, and procedures and, if necessary, personnel, organized to accomplish information transfer functions." "AJP-6: Allied Joint Doctrine for Communication and Information Systems". NATO Standardization Agency (NSA). 6 April 2011. 0102/a. 1-1.

<sup>73</sup> "AJP-6". 0102/b. 1-1.

<sup>74</sup> "AJP-6". 0102/b. 1-1.

The list of these five information activities does not match fully either the stages of information life-cycle defined in PDIM or the phases of the intelligence-cycle.

Here is the combination of categories of both cycles

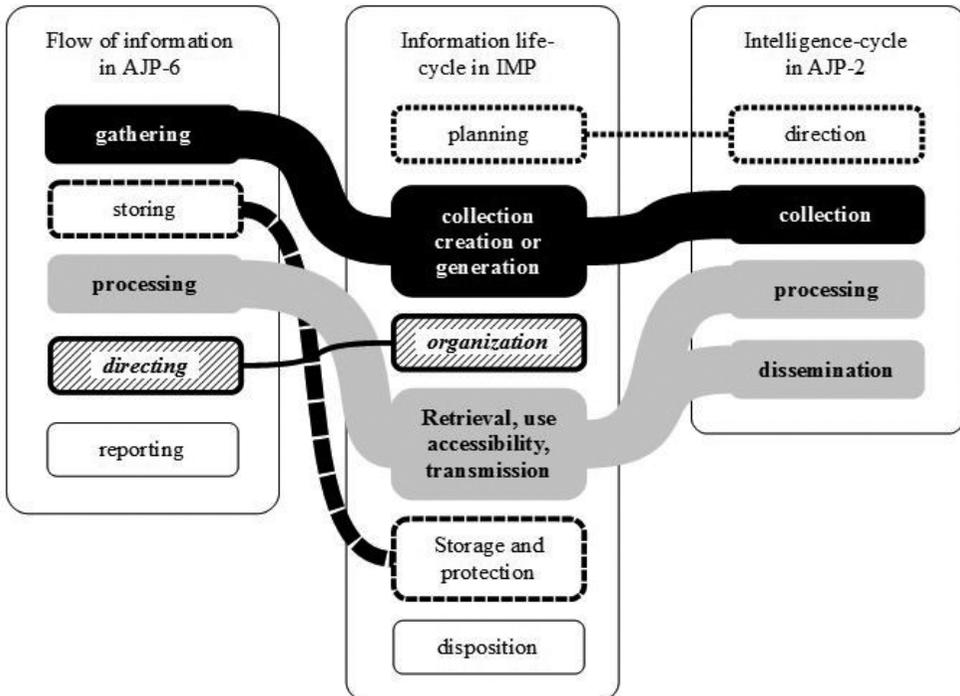


Figure 8: *relations between elements of information processing in various sources*<sup>75</sup>

After analysing logical connections between notions, it can be said, that AJP-6 and AJP-2 do not regulate the disposition of information by definition. That is a consequence of the aforementioned CIS and intelligence technological point of view. Reporting is a unique activity in AJP-6, which approaches information from the technical aspects of its processing. The basic AJP-6 point of view about information flow is linear contrary to NIMP and AJP-2 cyclic approach.

## SUMMARY

According to NATO, information is a critical resource. It has a specific life-cycle. In order to treat information well, a defined discipline, named Information Management is necessary.

Information management, as defined in the NATO policy and subordinated directives, has three key objectives: achievement of Information Superiority, effectiveness, and preservation of valued information. To reach the aforementioned aims, well-defined principles have been identified. In order to achieve the desirable requirements, IM has a specific organizational structure consisting of a Management Authority (NC3B) and various systems of responsibilities in NATO bodies at national level.

<sup>75</sup> Author's drawing.

All heads and members of NATO bodies have extra responsibilities to support IM among other tasks connected to their positions.

In order to treat information as a set in the alliance policies, new roles have been defined referring to the information and IM, such as originator, owner and custodian. New organizational positions are named in order to support IM with specific tasks, namely IM senior Official and Information Manager. The IM Senior Officer must be supported by existing services dealing with information, such as Security, Archives, Registry, Library, Training and CIS services.

In conclusion, this approach of NATO builds a solid fundament of effective work, since information is treated as organic and part of a system, with no regard to the different formats of information, such as traditional paper, audio-visual, or electronic ways of information representation.

In this paper, it was possible to recognize the difference between IM and other information processes. IM supports the treatment of information generally through its lifecycle while in other information processes, like intelligence process the objective is to support a specific area of military work having information as only one of the important tools.

#### BIBLIOGRAPHY

- “AAP-06: NATO Glossary of Terms and Definitions”. NATO Standardization Office (NSO). 17 November 2015.
- “AIntP-8: NATO Standard, Request for Information”. NATO Standardization Office (NSO). 28 August 2014.
- “AJP-01(D): Allied Joint Doctrine”. NATO Standardization Agency (NSA). 21 December 2010.
- “AJP-2: Allied Joint Doctrine for Intelligence, Counterintelligence and Security”. NATO Standardization Office (NSO). 22 February 2016.
- “AJP-3.10: Allied Joint Doctrine for Information Operations”. NATO Standardization Agency (NSA). November 2009.
- “AJP-3(B): Allied Joint Doctrine for the Conduct of Operations”. NATO Standardization Agency (NSA). 16 March 2011.
- “AJP-4(A): Allied Joint Logistic Doctrine”. NATO Standardization Agency (NSA). December 2003.
- “AJP-5: Allied Joint Doctrine for Operational-level Planning”. NATO Standardization Agency (NSA). 26 June 2013.
- “AJP-6: Allied Joint Doctrine for Communication and Information Systems”. NATO Standardization Agency (NSA). 6 April 2011.
- Munk, S. *Katonai informatika a XXI. század elején*. Budapest: Zrínyi Kiadó, 2007.
- NATO Standardization Office (NSO) webpage. (<https://nso.nato.int/protected/index.htm>), Accessed on 28 May 2018. NATO Standardization Agency (NSA). “ADatP-02: NATO Standard, NATO Information Technology Glossary”. March 2005.
- North Atlantic Council Archives Committee. “AC/324-D(2013)0001: NATO Information Management Manual”. 7 March 2013.
- North Atlantic Council. “C-M(2002)49: Security Within the North Atlantic Treaty Organization (NATO)”. 17 June 2002.
- North Atlantic Council. “C-M(2002)60: The Management of Non-classified NATO Information”. 23 July 2002.

- North Atlantic Council. "C-M(2007)0118: The NATO Information Management Policy (NIMP)". 11 December 2007.
- North Atlantic Council. "C-M(2008)0113(INV): The Primary Directive on Information Management". 18 December 2008.
- North Atlantic Council. "C-M(2008)0116: Public Disclosure of NATO Information". 20 November 2008.
- North Atlantic Council. "C-M(2009)0021: Policy on the Retention and Disposition of NATO Information". 2 March 2009.
- North Atlantic Council. "C-M(2009)0035 (INV): The NATO Information Management Authority (NIMA)". 03 March 2009.
- North Atlantic Council. "C-M(2011)0043: NATO Records Policy". 28 June 2011.
- "Riga Summit Declaration". 29 November 2006. <http://www.nato.int/docu/pr/2006/p06-150e.htm>, Accessed on 26 December 2016.
- "What is NATO". 26 December 2016. <http://www.nato.int/nato-welcome/index.html#>, Accessed on 26 December 2016.