INFORMATION ASSURANCE-INTELLIGENCE-INFORMATION SUPERIORITY RELATIONSHIP WITHIN NATO OPERATIONS

COL. (ret) Professor, Ph.D., Gheorghe BOARU*
LTC Ioan-Mihai ILIEŞ**

*"CAROL I" National Defense University, Bucharest, Romania
**HUMINT Center of Excellence, Oradea, Romania

There is a tight relationship between information assurance, the intelligence cycle and information superiority within NATO operations. The intelligence cycle has a discrete architecture and provides on-time and relevant intelligence products to the joint force commanders and to other authorized users in a specific joint area of operations. The intelligence cycle must follow the evolution of the operation. A permanent intelligence estimate will be performed during the military decision making process and operations execution. Information superiority is one of the most powerful intelligence cycle achievements. and decisively infuences the success of NATO joint operations. Information superiority must be preserved and enhanced through information assurance. Information assurance is an information operation that must be planned by the military in charge of operation security or by non-military experts, executed by all personnel during the entire intelligence cycle life time and employed during the planning and execution of NATO joint operations.

Key words: *NATO, information, information assurance, intelligence, information superiority.*

1. INTRODUCTION

The aim of this article is to provide a brief theoretical overview of the relationship between information assurance-intelligence-information superiority and thus enhance the existing knowledge about the preparation and execution of operations in a multinational environment. As a result of the research conducted in this field the article is structured in two main parts. The first one provides a comparative terminological analysis of the following terms "security of information", "information security (INFOSEC)" and "information assurance". The references used for this part are the NATO Security Directive, the experience gained in this field by the U.S. Army and by the Romanian Army, and the practices of some international players and non-military personnel working in the area of information security. The second part focuses on the role and principles

of intelligence within NATO, as well as on the relationships between data, information and intelligence at NATO level by highlighting the role of information assurance in achieving and maintaining information superiority in North Atlantic Treaty Organization. Depending on the views expressed in the doctrines, manuals, courses, studies or papers consulted for this article, the authors take the liberty to express their agreement or disagreement on the issues under discussion.

At a bird's eye view, the various international and national military directives and handbooks in the fields of information, information security and information assurance, intelligence and information superiority consulted for this article talk about similar concepts by different names. This is all too natural since a military theory is continuously evolving depending on the transformations lying ahead. Thus, the meanings associated to the aforementioned terms have varied in time and they still do depending on the contexts in which they are used. In this respect, it is worth reminding that Romania's status of NATO member does not rule out the necessity to make full meaning of the concepts currently employed in operations.

Another important conclusion issuing upon the consultation of various provisions of NATO, the U.S. and Romanian battlefield handbooks concerning concepts related to operating systems/functions of fighting in general and operating system/fighting function in particular is that no clear cut parallelism is to be drawn among these. Thus, one should emphasize the fact that for reasons such as mentality, level of technical training and fighting equipment not all the provisions of NATO and American handbooks can indiscriminately be applied to the Romanian military doctrines.

Even though from a theoretical standpoint one can state that there are no marked differences in concepts usage between the Romanian military and its allies, at a practical level the differences are more than obvious. For example, in their intelligence doctrines, allies like the USA, United Kingdom, Germany provide the right amount of detail in accordance with the type of work to be done. Moreover, when focusing on the field manuals of these state militaries, any researcher can conclude that the latter not ony mirror the doctrines, the terms and concepts related to operational language but also clearly present and explain them with no redundant terminology, no interpretations, no unnecessary additions.

By comparison, Romanian provisions related to some of the basic aspects concerning the decision making process (including information security or information assurance) are approached from different perspectives depending on the Romanian handbooks presenting

them. Thus, commanders often find themselves in an uncomfortable position when they have to make a summary of the basic aspects to be taken into account when making decisions, a summary that is vital in achieving the desired end-state, namely inclusion in the higher echelon commander's intention and executing the mission received from the latter. Such a situation is to be understood simply because, at present, the Standing Operating Procedure (SOP) drawn up by the military staffs, especially the chapter on information/intelligence, is a solution adopted by the Romanian commanders out of necessity.

Therefore, the authors of the article emphasize the clear cut difference that must be made from the onset between the terms of information and intelligence. Moreover, when analyzing these, one should also take into account the following relationship: data -information - (products) intelligence - relevant information - execution information, a relationship already detailed in other papers of this article's authors. In this respect, mention should be made of a landmark document issued in 2005, namely the Romanian Army Doctrine for Information, that plays a major role in making clear delineations among often confused and misused concepts and terms, some of which will also be presented in this paper. Thus, one final aim of this paper is to provide better knowledge of NATO operations mechanism by focusing on some elements, phenomena, and processes in accordance with the relationship between information security and information superiority.

2. SECURITY OF INFORMATION - INFORMATION SECURITY (INFOSEC)-INFORMATION ASSURANCE: A TERMINOLOGICAL OVERVIEW

Within NATO operations there is a distinct relationship between the nominal phrases: security of information, information security and information assurance. The first term, security of information, refers to information in general, in other words, security of all types of information. Moreover, the same phrase encompasses the term of information security (INFOSEC) since the latter means security of information handled in electronic systems. In other words, one can say that INFOSEC is security of electronic information. Moreover, both these terms are part of the information assurance term, the latter referring to information systems security in general.

However, "information systems" is a comprehensive term that includes all the aspects related to infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

As far as the relationship between data – information – information assurance – intelligence and the comparison betwen the process of data transformation into knowledge and the understanding of intelligence as a warfighting function, one can underline three distinct aspects.

First, intelligence is a very important process for the military decision making process (MDMP) during the preparation and execution of NATO operations. The intelligence process has a cycle which includes four phases: direction, collection, processing and disemination of intelligence products to the commanders, staffs and other users. In addition, two more phases are permanently performed, namely the evaluation and the feedback.

Second, intelligence is an important warfighting function that provides allied comanders with an important instrument that allows for the use of the combat power of their military structures at the right moment and in the right place.

Third, information assurance is vital for the intelligence cycle and must be performed in order to assure the disemination of the intelligence products only to authorized personnel and in an extremely secure mode.

Upon the thorough analysis of the information assurance and intelligence processes within NATO operations, the authors of this article can only conclude that the main effort of the Allied Operations is initially focused on intelligence, information assurance and logistics. For mission execution, commanders need early development of a secured intelligence architecture in Theatre of Operations. That means deployable information security personnel and resources, military intelligence forces/structures/groups and a flexible approach to the command and control relationship. Performing the operations objectives requires the Joint Force Commander to determine with his commanders, as soon as possible, the critical information requirements. The intelligence community has to put in place a robust and versatile intelligence network in designated Area of Operations. The security structures must perform complex information assurance operations for intelligence cycle protection.

However, information assurance determines all information flows within the specific information systems, while security of information ensures protective measures of all types of information in general, providing the Confidentiality, Integrity and Availability (CIA) for all-source-information.

For a clearer understanding of security of information and for achieving a very good level of security for classified information a clear access authorization must be established. Security classification is of utmost importance for information protection and applied to information

to indicate the possible damage to the security of NATO and/or its member nations if the information is subjected to unauthorized disclosure. The security structure should maintain a list indicating the levels of access for each assigned individual who is granted access to NATO information and should verify NATO access authorizations for all personnel. In our opinion, as with classified information, access is not based on duty position, rank, or level of clearance. Access is based on need-to-know, the proper level of clearance, and an access briefing for a specific level and type of classified information.

Within NATO, there are many concerns over security assurance. In our opinion, these concerns that are very clearly expressed by the allied military analysts are related to the strategic dilemma of nowadays global information environment, namely the desire to exploit the Computer Network Operations advantage as opposed to the protection of the global information environment. In order to solve the dilemma, those working in the military have to focus on the lessons learned in the field.

Thus, after the 9/11 events, one can discuss about another kind of war, the war against terrorism that invoves anti-terrorist and counter-terrorist actions. The terrorist attacks are not only by bombs and arms. Therefore, taking into account that contemporary society is an information society based on computer networks, in the war against terrorism a very important confrontation is the cyber one. Cyber confrontation means cyber attack and cyber defense. In our opinion, the cyber terrorist actions are cyber attacks and not only the reactive but also the proactive actions are cyber defence.

All this considered, the question for the Romanian military, but also for all those working in the field approched by this article should ask themselves if they and/the state is prepared in case of a terrorist attack. The terrorists have sufficient means and determination to perform cyber attacks. Moreover, the question should also focus on whether people are prepared for a cyber terrorist attack. In our opinion, managing to clarify the inherent concepts associated to these may ensure the winning of a battle in the field.

One of the biggest potential threats to information security is the people who operate the computers. A workplace may have excellent information security systems in place, but security can be easily compromised. If a help desk worker gives out or resets passwords without verifying who the information is for, then anyone can easily gain access to the system. Computer operators should be made fully aware of the importance of security. Simple security measures can be used by everyone to keep data secure. For example, changing passwords on

computers, and using combinations of letters and numbers makes it harder for hackers to gain access. Also, a note of passwords is not to be made where it can be easily accessed. However, there has never been such a thing as a totally secure system. Hackers will always find more sophisticated ways to gain access. However, with technology implementing higher levels of information security, such as iris recognition systems, security systems should keep us out for a little longer.

In conclusion, there is a distinct relationship between security of information, information security and information assurance, as already highlighted in this part of the article.

3. THE RELATIONSHIP BETWEEN INFORMATION ASSURANCE AND INFORMATION SUPERIORITY

As pointed out in the introduction, the research already conducted in the field of information security manageemnt yielded another relationship that is worth analyzing and clarifying, namely the one between information assurance and information superiority. Thus, one has to emphasize the tight and discrete relationship between data, information, information assurance, and intelligence within NATO. Intelligence is not only the product resulting from the intelligence cycle but also intelligence generate through the intelligence warfighting function. Intelligence staffs direct collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.

The approach taken towards the analysis of information and information threats and to the explanation of the information assurance role in obtaining and preserving the information superiority within the NATO operations resembles that of NATO military operations Thus, the key words of this part of the article are: NATO, information, intelligence role and cycle, information assurance and information superiority. Moreover, the information assurance role in the data - information - intelligence relationship must also be underlined. In this respect, when analyzing this relationship one can easily observe that when the intelligence cycle is performed the information assurance for it is fundamental. In other words, information must be protected during the intelligence process. The intelligence products have to be made available for authorized users in a very secure mode. Thus, even though data and information collection and evaluation processes can be by the book, clear estimations and interpretations can be achieved, excellent conclusions

can be presented to commanders, if a very strong system for security of information is not in place, all of the above are in vain. In this respect, it is the the breaches and gaps in the security of information systems that enemies always look for. Therefore, good information assurance is the basic element in information protection. More than that, in our opinion, information assurance is an information operation that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. In other words, information assurance is a very important information operation performed to protect information systems.

Thus, the need for information assurance within the information operations conducted by the Alliance must be emphasized. Moreover, the cue for a real understanding of the role played by information assurance in NATO forces achieving information superiority in theaters of operations lies in the explanation of the relationship between information security, intelligence cycle in NATO operations, and the role of information security to achieve and maintain information superiority in NATO.

Accordingly, the intelligence cycle is defined as a discrete transformation of data and information into intelligence products. The intelligence cycle phases overlap and coincide, so that they are concurrent and continuous rather than sequential. The intelligence cycle decisively directs the military commanders' decision-making process and operation execution. The intelligence products have to be predictive and support the commander in understanding the common operational picture of his designated operation area. The intelligence products are the result of obtaining relevant information. A permanent intelligence estimate is be performed during the "plan, prepare, execute" operations cycle. Information assurance has the role of protecting all information flows and systems. Information superiority is greatly influenced by the information assurance operation and the intelligence cycle products. The information superiority is decisive and determines the success of the joint operations. It is not only the security personnel who must be involved in the security and information assurance of the NATO operation, but also all the military and non-military personnel deployed in a specific theatre of operations.

The role of information assurance is a basic one in maintaining the information superiority within the national and NATO doctrines. A very short analysis of the relationship between information superiority and

information assurance is absolutely necessary. According to the Romanian doctrine [1], information superiority means the collection, processing and dissemination of an accurate and credible information flow, and denying similar actions of enemy forces. As defined by Romanian military experts [2], information superiority refers to relevant information processed for a comprehensive understanding of the operational environment, enemy actions and intentions, and for generating the common operational picture. Within NATO doctrine [3], information superiority is analyzed as part of the operational concept. Thus, information superiority within allied operations is a very complex process which comprises an information operations strategy established by the designated allied structure inside the Joint Force Command. This allied structure coordinates special operations, intelligence operations, civil-military cooperation (CIMIC) operations, communication and information systems installation, command and control systems, security operations, deception operations, psychological and electronic warfare operations.

Information superiority and air superioriy/supremacy and naval presence before the joint forces engagement in battle are the main aspects of a successful combined joint task force in NATO operations. Information systems and networks provide the predominant source from which the warfighter generates, receives, shares, and utilizes information. The installation of an advanced communications and information system which is able to sustain the dissemination of products through a certain intelligence cycle

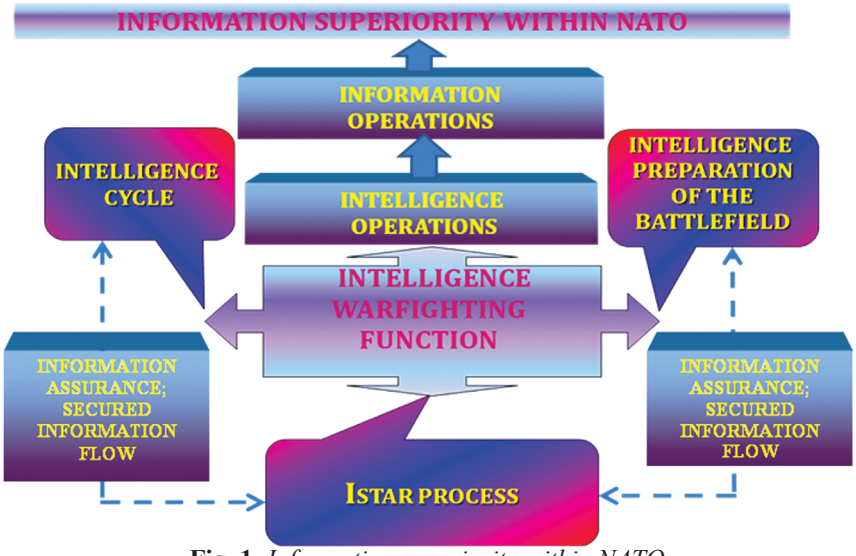

Fig. 1. *Information superiority within NATO*

(properly applied during the military decision making-process), leads to information superiority, which is essential to achieving success in all military operations.

The power of superiority in the information environment mandates the joint force commanders to fight for it as a first priority even before hostilities begin. The quality of information depends upon the accuracy, timeliness, relevance, usability, and completeness of information from all sources. A top responsibility of command is to ensure access to all relevant information sources within and among all military and non-military organizations which are involved in joint military operations or non-military operations (according to NATO comprehensive approach), and in multinational operations with mission partners. The continuous sharing of information from a variety of sources facilitates joint force mission execution in a specific area of operation and timelineness awareness for multinational military and non-military structures.

In conclusion, information superiority cannot be achieved without information operations, namely without information assurance operations. The security quality criteria of the information must be assured and preserved by the entire personnel during a NATO operation. In this respect, it is worth reminding the the new NATO concept: "need to know vs. need to share" and the two approaches to this subject. Thus, while the former refers to the intelligence products which need to be shared to partners in an area of operation, the latter is about the necessity to know how to share information by applying all the security measures needed when transferring information. Otherwise, the Wiki leaks lessons learned can repeat.

Last but not the least, the importance of information assurance for the intelligence cycle and for information superiority within NATO operations must be emphasized. The intelligence provides on time and relevant intelligence products to the joint force commanders and other authorized users in a specific joint area of operations. The intelligence cycle must follow the evolution of the operation. A permanent intelligence estimate is performed during the military decision-making process and operations execution. Information superiority is one of the most powerful intelligence cycle achievements and decisively infuences the success of joint operations. Information superiority must be preserved and enhanced through information assurance. Information assurance is an information operation that must be planned by the military staff and executed by the entire personnel during the entire intelligence cycle life time.

4. ACKNOWLEDGEMENT

The information in this paper is public or unclassified. Some of the ideas presented in the article were discussed during the postgraduate course in Information Security Management attended in 2011 at the Regional Department of Defense Resources Management Studies, Braşov. Moreover, the opinions already expressed are the result of consulting an extensive bibliography as part of the PhD research project of LTC Ioan-Mihai ILIEŞ undertaken at "CAROL" I National Defense University of Bucharest, Romania under the supervision and guidance of COL (ret) Professor, Ph.D., Gheorghe BOARU.

REFERENCES

[1] Information support of Joint Operations, (Bucharest, 2003), 58.

[2] Constantin Alexandrescu, Gelu Alexandrescu and Gheorghe Boaru, Military Information Systems, (Bucharest: National Defence University "Carol I", 2010), 25.

[3] AJP-03, Allied Joint Operations, (2002), 2-22, 4-13.