SECURITY OF INFORMATION AND OF MILITARY INFORMATION SYSTEMS

Colonel (ret.) Professor Gheorghe BOARU, PhD

Full member of the Academy of Sciences of the National Security,
Full member of the Academy of Romanian Scientists,

Colonel Iulian Marius IORGA, PhD

Ministry of National Defence

The way of approaching the field of information security and military information systems is based on the fact that Romania is a NATO member and that, in joint military actions, it uses information systems that must be compatible and interoperable, but also protected.

From the informational point of view, in the military actions there is a fight for information, through information and against information and therefore its security is a special activity, particularly with a view to classified information.

The Alliance members, including Romania, must provide, individually or through bilateral cooperation agreements, the protected information resources, both as a process and as a system, necessary to fulfil the joint operations' objectives under NATO command.

Most of the informational threats come through virtual space. In this sense, it is considered that the security of the virtual space has become one of the most pressing security challenges of the 21st century.

Keywords: information, information system, vulnerabilities, threats, risks, cyber security.

INTRODUCTION

In order to fulfil the missions that respond to the new challenges of the security environment, the Romanian Armed Forces have engaged in a broad transformation process established in the *Romanian Armed Forces Transformation Strategy*[1].

In this sense, by 2025, the transformation process is planned to undergo the following three phases[2]:

- **the basic restructuring** (2005-2007);
- **NATO and EU operational integration** (2008-2015),
- **full NATO and EU technical integration** (2016-2025).

The third phase will ensure achievement of long-term transformation objectives: efforts, as well as financial and human resources will be focused on providing the capabilities assumed and included in the capability targets and on participating in NATO and EU – leading missions and operations; going on with improving and outfitting with new equipment and reaching the interoperability level with other EU and NATO armed forces etc.

The basic objective of the transformation process is to adjust the structure of the Romanian Armed Forces to the present and future security environment, in order to fulfil the national commitments to the Alliance, concordant with the processes and phenomena in the NATO transformation plan.

In this context, the basic objective of the transformation process is to adjust the structure of the Romanian Armed Forces to the present and future security environment, in order to fulfil the national commitments to the Alliance, concordant with the processes and phenomena in the NATO transformation plan.

The aim is to make the Romanian Armed Forces able to participate in the entire spectrum of missions carried out by the Alliance and the EU.

I consider this the legal context in which the Romanian Armed Forces can develop the military actions, actions in which the command and control processes are based on the specific information processes.

---

[1] *Strategia de transformare a Armatei României*, Bucureşti, 2007.

[2] See https://fcnap.ro/transformarea-fortelor-armate-ale-romaniei-un-raspuns-direct-la-noile-provocari-ale-mediului-de-securitate/, retrieved on 20 February 2020.

MILITARY INFORMATION AND ITS SECURITY

Thorough information is well known to result in an efficient command and control process.

In our armed forces, the intelligence support to operations is well regulated, representing the *"basic form of assuring the actions and the force protection, and establishing the set of measures and actions, continuously and unitarily carried out by all the participating forces and at all levels in order to plan, obtain, verify, process and capitalise on the data and the intelligence regarding the situational factors"*[3].

In our armed forces, the intelligence support to operations is well regulated, representing the "basic form of assuring the actions and the force protection, and establishing the set of measures and actions, continuously and unitarily carried out by all the participating forces and at all levels in order to plan, obtain, verify, process and capitalise on the data and the intelligence regarding the situational factors".

The field literature approaches information both as *"a powerful weapon and as a preferred target"*[4], or it is stated that *"information can be the most feared weapon in the technological developments of the battlefield"*[5].

If this information is correlated with other information already known and if it is analysed from the past experiences' perspective (collation and processing), they emerge in a new set of meanings with a different informational value, a process called *"intelligence"*.

By studying the relationship between data, information and intelligence, we can conclude that the processed information is transformed into intelligence products, which are obtained as a result of a structured process, called in the NATO doctrines or those of allied states, *the intelligence cycle*.

We assess that, in the case of NATO multinational joint operations, *"intelligence"* does not mean *"information"*, but a complex process determining the enemy's intentions and most likely course of action.

Within the basic systems and processes involved in the multinational joint operation planning – *intelligence* can have the attribute of[6]: combat function; combat ability; cycle; process and system.

---

[3] I.P.S.-3.1, *Manualul privind procedurile de informaţii militare pentru sprijinul operaţiilor*, SMG, Bucureşti, 2006, p. 14.

[4] *Cornerstones of Information Warfare,* Department of the Air Force, Washington DC, 1995, p. 2.

[5] Peter Grier, *Information Warfare,* Air Force Magazine, No. 3, March 1995, p. 23.

[6] Colonel (r.) Professor Dr Gheorghe Boaru, Colonel, doctoral student, Iulian-Marius Iorga, *Ciclul informațional ca proces, procesul și ciclul "Intelligence" – în cadrul acțiunilor militare moderne,* Revista de Științe Militare, published by the Academy of Romanian Scientists, no. 1, 2017, pp. 84-85.

In analysing the intelligence process, we take as a reference the NATO Doctrine for Intelligence[7], because to this are compared the intelligence aspects analysed in the NATO Forces activity, in allied states' Armed Forces, as well as in those forces' intelligence doctrines[8].

In order to achieve the intelligence requirements, intelligence structures adapted to the new realities of the operational environment are needed, based on a training process that will allow them to successfully tackle the challenges related to applying the new Allied concepts: *"hybrid operations"*, *"comprehensive approach"*, *"information sharing"*, *"need to know vs. need to share"*.

According to the opinion of some Romanian military specialists[9], in order to integrate the intelligence activities under a single name, the NATO member states' armed forces have standardised the ISTAR concept (Intelligence, Surveillance, Target Acquisition and Recognition). The same authors also specify that different ISTAR acronym variants are used, such as: STAR, RSTA, STA, ISR, exclusively to highlight partial information activities.

In the Romanian Armed Forces, according to the *Doctrine for Intelligence, Counterintelligence and Security of the Armed Forces*, the ISTAR[10] concept has been accepted and integrated in the specific national norms as an *"organisational solution, meant to functionally integrate all the available collection capabilities, normatively defined, under the circumstances of using a set of actions, procedures, measures and resources (technical, human, financial etc.)"*[11]. This concept has been normatively designed to provide *the connection between collection, processing and dissemination of data and intelligence in order to support the commander in reaching the operational objectives in the conflict spectrum*[12].

In order to achieve the intelligence requirements, intelligence structures adapted to the new realities of the operational environment are needed, based on a training process that will allow them to successfully tackle the challenges related to applying the new Allied concepts: "hybrid operations", "comprehensive approach", "information sharing", "need to know vs. need to share".

---

[7] AJP-2*, The Allied Doctrine for Intelligence, Counterintelligence and Security,* 2003.

[8] *Doctrine for Intelligence Support to Joint Operations* (of the Romanian Armed Forces, A.N.), 2003; *Doctrine for Intelligence in Joint Operations* (of the Canadian Armed Forces, A.N.), 2003; JDP 2-00, *Understanding and Intelligence Support to Joint Operations* (of the UK Armed Forces, A.N.), 2011; JP-2, *Intelligence in Joint Operations* (of the US Armed Forces, A.N.), 2007.

[9] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale militare – servicii şi tehnologie*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2010, pp. 24-25.

[10] *Ibidem.*

[11] *Doctrina pentru Informaţii, Contrainformaţiişi Securitate a Armatei*, Bucureşti, 2005, p. 34.

[12] *Ibidem*, p. 35.

The fact that there is such a normative and enforcement capacity in the military intelligence field, at the Romanian Armed Forces level, shows that the essence of the information support integrating efforts concept is to use all the possibilities offered for this field in an integrated environment, thus allowing the Romanian procedural environment integration with that of other NATO member states.

In this informational normative context, the security of information and military information systems is mandatory, so it requires knowledge and concern for this field, as well as establishing the most effective measures.

Therefore, we consider that, in the context of Romania's NATO membership, and in the perspective of adapting and transforming Romanian doctrinal and action approaches, the staff officers' concern to know and address the problem of information security according to the Alliance's demands is justified.

Modern armed forces pay special attention to this problem, considering it a key objective for winning the information battle, whose foundation is represented by the introduction, on an extended scale, of information technology and of the modern means of communication and information technology, in the whole space of the battlefield.

We also consider particularly important the aspects related to the classified information which requires protection against unauthorised disclosure and which carries specific identifiers, as well as non-classified information that is not intended for public use and is protected by internal measures specific to each organisation, as well as information of public interest, respectively that information which concerns or results from activities carried out by a public authority or public institutions.

Furthermore, measures for the protection of information against dangers and threats specific to the informational age are presented in the NATO and the Allied armed forces regulations and military handbooks.

In accordance with Law no. 182/2002, the Government Decision no. 585/2002 regarding the National Standards for the protection of classified information was issued. At the same time, the equivalence levels of the classified information from Romania with those

from NATO and/or the EU have been established, as shown in the table below.

Table no. 1

Levels of Equivalence in Romania – NATO – the EU[13]

Romania – classified information		**NATO – classified information**	**The UE – classified information**
Secret de stat	Strict secret de importanţă deosebită/SSID	NATO TOP SECRET/ NTS	TRÈS SECRET UE/TSUE
	Strict secret/SS	NATO SECRET/NS	SECRET UE/SUE
	Secret/S	NATO CONFIDENTIAL/NC	CONFIDENTIEL UE/ CUE
Secret de serviciu/SSv		NATO RESTRICTED/NR	RESTREINT UE/RUE

NATO information security[14] is ensured according to Law no. 423/2004, and, through the Government Decision no. 353/2002, the Norms regarding the protection of the classified information of the North Atlantic Treaty Organisation in Romania are established.

In this context, we consider that information security is a field whose importance is constantly increasing and which must be approached from all possible angles, starting from concepts, vulnerabilities, risks, and management.

SECURITY OF MILITARY INFORMATION SYSTEMS

In order to function, military organisations use information systems. The more complex they are, the more information they need. Therefore, the informational component of any system is constantly growing and diversifying, and the lack of information determines its disappearance.

In order to function, military organisations use information systems. The more complex they are, the more information they need. Therefore, the informational component of any system is constantly growing and diversifying, and the lack of information determines its disappearance.

Consequently, those information systems must be designed so that they are efficient and their security is assured in any situation. Only in this way can the security, accuracy and timeliness of the information necessary for the command and control process can be ensured, as a key component of military actions.

[13] Iulian Marius Iorga, *Securitatea informațiilor în acțiunile militare moderne,* Editura Universității Naționale de Apărare *"Carol I"*, București, 2018, p. 93.

[14] Law no. 423/2004 on Romania's Accession to the NATO Agreement on Information Security, adopted in Brussels, on 6 March 1997.

As specificity of the military field, the importance of the information systems continuously increases, achieving symbiosis with the command and control processes, functioning cohesively and rendering higher quality to the management of the organised and/or carried out actions.

Command and control activities, specific to the military field, but particularly, the effective conduct of military actions, the military entity's ability to successfully carry out a mission are influenced by the data and information needs, as well as by the ability to obtain the informational advantage, determined by the available information capabilities and the security of the informational-decision-making system.

As specificity of the military field, the importance of the information systems continuously increases, achieving symbiosis with the command and control processes, functioning cohesively and rendering higher quality to the management of the organised and/or carried out actions.

The concept of information system has been studied by specialists from different fields of activity, from the perspective of both its structure and its functioning, but no single definition has been reached.

The structure of the information system depends on its destination, on the complexity and the spatial distribution of the command and control elements assisted, as well as on its objectives and processes.

Different categories of information systems have been studied, such as security and national defence, technical, social, economic etc. systems, among which there are important dissimilarities and which have common structure elements, but also specific elements, which shape the difference.

We can consider that the structure represents the organisational component, which defines the systemic conception and allows an information system to be made up of modules (subsystems). This can be done by identifying, grouping, arranging and optimally interconnecting the infrastructure and management elements, also taking into account the technical resources, the databases, the software components and, essentially, the security elements.

A thorough informational assurance of the organisational structures, in which the command and control and the operational activities (of execution) are well defined, can be a favourable premise for the mission success.

In the military organisation, the structure of the information system is determined and basically depends on the structure of the command and control system. Between the two structures, there is a mutual, shared, interdependence.

Studying and analysing several **definitions of the information system**[15], presented in specialised military and/or civilian Romanian and/or foreign papers, we found that all are based on structural, technical, functional and management elements specific to the field addressed.

We present here five of the most significant definitions mentioned in the specialised literature, above-referred, in which the information system:

1. *"is a system of persons, data records and activities on data and information processing within an organisation, including processes of manual or automatic processing thereof. Information technology is a key component of the information system"*[16];

2. *"represents the integrated set of components for information collecting, storing, processing and communicating. Its main elements are: computers (hardware), software, databases, communication systems, human resources and procedures"*[17];

3. *"represents a set of equipment, methods and procedures and, if necessary, personnel organised to perform the functions of information processing"*[18];

4. *"includes the entire infrastructure, circuits and information flows, organised in a unitary conception, the personnel, all the components that collect, transmit, store, process, elaborate/process information and ensure their display and dissemination, in order to use them in the management process (command and control) and in carrying out military actions"*[19];

---

[15] Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare,* Editura Universității Naționale de Apărare *"Carol I"*, București, 2018.

[16] *Information Systems*, Wikipedia, the free encyclopaedia, http:/en.wikipedia.org/ wiki/ Information Systems, retrieved on 20 March 2020.

[17] *Britannica Encyclopaedia*, http://www.britannica.com/EBchecked/topic/287895/ Information Systems, retrieved on 20 March 2020.

[18] AAP6 (2008), *NATO Glossary of Terms and Definitions*, 2008, p. 2-I-4.

[19] FM 101-5-1, *Terms and Operational Symbols, Land Forces General Staff*, USA.

5. *"includes the entire infrastructure, organisation, personnel and components for collecting, processing, storing, transmitting, displaying, disseminating and acting on information"*[20].

Referring to **the management information system** (MIS), centred on managerial objectives, an interesting approach has the following two definitions:

1. *"The managerial information system (MIS) consists of all the data, information, flows and information circuits, procedures and means of information processing, meant to contribute to the establishment and achievement of the organisation's objectives"*[21].

The management information system – MIS is defined as a "combination of human and computer resources that aim at collecting, storing, organising, calling, communicating, distributing and using the data and information that managers use in exercising their management functions, in order to achieve efficient management. These systems provide direct, online access to the relevant information stored, friendly interface, in an easy-to-use dialogue".

2. MIS is defined as a *"combination of human and computer resources that aim at collecting, storing, organising, calling, communicating, distributing and using the data and information that managers use in exercising their management functions, in order to achieve efficient management. These systems provide direct, online access to the relevant information stored, friendly interface, in an easy-to-use dialogue"*[22].

Analysing the above definitions, it turns out that both essential components are highlighted, as well as certain features of the information system, each of which requires, in our opinion, certain additions, clarifications and updates.

Three specialists from *"Carol I"* National Defence University, taking into account the current achievements in the field and synthesising the opinions of different specialists, formulated the following general definition: "*the information system represents the integrated set of data, information and knowledge necessary for the organisation, mainly managed electronically, together with information infrastructure ...."*[23].

---

[20] US Army Field Manual 100-6, *Information Operations*, 1996; JP-02, DoD Dictionary of Military Terms, 2008, p. 261.

[21] Ovidiu Nicolescu et al., *Sistemul informaţional managerial al organizaţiei*, Editura Economică, București, 2001, p. 25.

[22] Club IT&C, *Cum să exploatezi informaţia în mod inteligent-Management Information Systems*, https://www.google.ro/Club+IT%26C, +Cum+s%C4%83+exploatezi+informa%C5%A3ia +%C3%AEn+ mod+inteligent-Management+Information+ Systems&tbm..., retrieved on 1 February 2020.

[23] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale – fundamente teoretice –*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2009, pp. 194-195.

According to the same authors, unlike other opinions, the information infrastructure includes, besides *the information and communication technology*, *the specialists* in the field, as well as the *information management structure*.

In line with the same approach, it is envisaged that the information system will provide the data and information necessary for the command and control process, in order to optimally achieve the stated objective or mission and to obtain *competitive advantages*[24]. *The competitive advantage* is a critical mass synthesis of the relative advantages in the following fields: information, knowledge, understanding and decision-making (command and control), also including moral and leadership qualities.

Specifically, *the military information system*[25] is a large, dynamic, complex system, made up of several interdependent systems (which, hierarchically, are subsystems), that must be singularised, with a high degree of automation and self-regulation, managed in a centralised way. It is, in fact, a super-system (federation of systems), which comprises a homogeneous set of interconnected networks, together with their integrated elements for management, having the necessary inputs, internal structure and outputs, being characterised by a high degree of autonomy and heterogeneity.

The C4ISR/C5ISR-D systems involve the provision of information and knowledge to the political-military decision-makers in order to ensure a higher situational awareness. Given that military operations will be conducted with greater precision than ever, the mission effectiveness will increasingly depend on C4ISR/C5ISR-D systems, which are complex subsystem networks.

The military information system represents the dynamic side of the command and control (management) system of which it is a part, which provides optimal decision making, its functioning and cohesion, a reason for which, in some specialised works, it is called information-decision-making system or, in Western literature, managerial information system[26].

ROMANIAN MILITARY THINKING

The military information system is a large, dynamic, complex system, made up of several interdependent systems (which, hierarchically, are subsystems), that must be singularised, with a high degree of automation and self-regulation, managed in a centralised way. It is, in fact, a super-system (federation of systems), which comprises a homogeneous set of interconnected networks, together with their integrated elements for management, having the necessary inputs, internal structure and outputs, being characterised by a high degree of autonomy and heterogeneity.

[24] D. Albert, J. Garstka, R. Hayes, D. Signori, *Understanding Information Age Warfare,* Washington DC, CCRP - Data publication, August 2001, p. 41.

[25] W.J. Karplus, *Sisteme de calculatoare cu divizarea timpului*, EdituraTehnică, Bucureşti, 1970, p. 227.

[26] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale, op. cit.*, p. 195.

"The information-decision-making system represents a cybernetic system, organised in a pyramid, in reciprocal, vertical and horizontal flows, based on a unitary mechanism for collecting and processing information, from the lowest hierarchical level to the highest, which allows for decision foundation, adoption and follow-up. This system ensures the implementation of the decision package and monitoring the effects of its application for the fulfilment of the organisation's objectives"[27].

The information system includes the status information (reports, information, proposals, syntheses, notices, ...) coming from the execution bodies, various information sources, sensor systems, elements with which to cooperate or collaborate and goes out the control information (orders, provisions, specifications, indications, guidelines, ...) produced by the control units.

The information system not only contains technical elements but it is constituted as a complex set of specialised people as well as practical activities, technical equipment for collecting information (including through sensors), communications, storage, processing and display of information, software, databases and procedures, focused on identifying the information needs and the ways of fulfilling them, for the informational assurance of the management processes (command and control), including the decision transmission to the subordinate operational levels (echelons).

In another approach, *"The information system is the link between the command and control system and the operational (execution) system, which contributes to the symbiosis (approach), strengthening the discipline and increasing the responsibility for the activities carried out. It should not only be considered as an interface between these systems, but also as an element of connection between the internal information environment of the organisation (the military structure) and the external one through which almost all the necessary data and information are obtained"*[28].

The information system includes the status information (reports, information, proposals, syntheses, notices, ...) coming from the execution bodies, various information sources, sensor systems, elements with which to cooperate or collaborate and goes out the control information (orders, provisions, specifications, indications, guidelines, ...) produced by the control units.

---

[27] Ion Ciobanu, Gheorghe Ilie, Aurel Nour, *Confruntarea informaţională şi protecţia informaţiilor*, Editura Detectiv, Bucureşti, 2006, p. 71.

[28] Vasile Dumitru et al., *Sisteme informaţionale militare*, Editura CERES, Bucureşti, 2000, p. 38.

Regarding the role of the information system, analysed in close correlation with its place within the organisation (the military structure), we can assess that it consists of:

- determining the volumes of required data, information and knowledge, so that the decision-making and execution processes of the military structure have optimal performance;
- allowing to determine the sources that can obtain the information;
- establishing the technical means, which will ensure the information flows circulation and the information means for the information processing;
- establishing the information resources (data, information), circuits and information flows to be ensured. *Information resources* consist of information together with personnel, technical equipment and information technology;
- ensuring the specific informational functions (the activities of collecting, transmitting, storing, processing and disseminating information operatively), necessary for the command, control (management) and execution of the activities;
- ensuring the qualitative parameters necessary for the information (objectivity, opportunity, precision, integrity, relevance, authenticity) for the organisation command and control systems (military structure);
- applying effectively security policies, targeting both information and information processes.

The safe and uninterrupted functioning of the information systems, which entirely depends on the organisational, technical and functional measures adopted, is a vital necessity for any organisation (military structure). Affecting, even partially, the work of the structural elements and their equipment (hardware, software), causes serious informational damage, by interrupting or delaying the command and control processes (management) as well as the operational ones (executional).

The safe and uninterrupted functioning of the information systems, which entirely depends on the organisational, technical and functional measures adopted, is a vital necessity for any organisation (military structure). Affecting, even partially, the work of the structural elements and their equipment (hardware, software), causes serious informational damage, by interrupting or delaying the command and control processes (management) as well as the operational ones (executional).

The use of information and communication technology has created the possibility of developing modern information systems, in which computer networks and communications have a decisive

role, but which also have significant vulnerabilities. At the same time, they are also subject to informational threats, due to the action of internal factors, but particularly external ones, which aim at limiting or interrupting the activities of information collecting, transmitting, processing and disseminating, for abnormal functioning or even blocking the system's functions.

Many of these threats come through virtual space. In this sense, it is considered that *"Securing virtual space has become one of the most pressing security challenges of the 21st century, due to its importance for daily life, for government, national security, business, as well as for citizens. The cyber world and associated technologies have created, on the one hand, more social, cultural, economic and political opportunities for all, and on the other hand, its borderless nature has brought with it threats such as cyber-attacks and cybercrime"*[29].

Internet connection is a facility, but most of the time, it creates major security issues for these networks, by creating breaches that can be accessed in an unauthorised way. The security services in the field of communications and information networks are aimed, on the one hand, at keeping them in operation, and on the other hand, at ensuring the security of the applications, as well as of the information stored on the storage base or transmitted through the network.

Essential questions about information network security: *"Who? When? Where from? What? Why?"* determine together a new phrase, *"of the five W's"* (*5W – Who, When, Where, What, Why?*). Who accesses the network? When and where does access occur? What information is accessed and why? These aspects must be monitored and secured, depending on the importance of the information, on the public or private character of the communications and information networks, regardless of the terminal used.

Internet connection is a facility, but most of the time, it creates major security issues for these networks, by creating breaches that can be accessed in an unauthorised way. The security services in the field of communications and information networks are aimed, on the one hand, at keeping them in operation, and on the other hand, at ensuring the security of the applications, as well as of the information stored on the storage base or transmitted through the network.

First and foremost, the security of these networks is ensured through strategies and doctrines, as well as through developing a security culture at national and European level.

[29] Colonel (ret.) Professor Dr Gheorghe Boaru, *Război și apărare în spațiul virtual,* Revista de Științe Militare, published by the Academy of Romanian Scientists, no. 2, 2018, p. 51.

We believe that these strategies must be applied both at European and national level. Thus, it is estimated that *"Improving the way the EU ensures cyber security is essential in order to continue to ensure the social, economic, financial and cultural benefits that citizens and businesses obtain from the Internet and, in a broader sense, the communications and information technology development. Moreover, it is essential for the EU to reach the goals it has set in the Digital Agenda for Europe (2010), and equally significant, the driving force of such an agenda – the Europe 2020 Strategy"*[30].

Fully concordant with the European actions, at the national level, the *National Strategy on the Digital Agenda for Romania 2020* was approved in February 2015[31].

This strategy *"defines four areas of action, of which only the first domain is worth mentioning here, namely: e-Governing, Interoperability, Cyber Security, Cloud Computing and Social Media. This document has taken over and adapted the elements of the Digital Agenda for Europe to the specificity of our country. The Digital Agenda thus defines the key role that ICT use must play in achieving the Europe 2020 goals"*[32].

The military information systems, such as C4I (C4I2, C4ISR, C5ISR, ...), a topical concept in European and Euro-Atlantic military theory and practice, integrate the command, information, communication and information subsystems, being based on doctrines and specific procedures, flexible structures, state-of-the-art equipment and, first and foremost, highly professional staff.

The military information systems, such as C4I (C4I2, C4ISR, C5ISR, ...), a topical concept in European and Euro-Atlantic military theory and practice, integrate the command, information, communication and information subsystems, being based on doctrines and specific procedures, flexible structures, state-of-the-art equipment and, first and foremost, highly professional staff.

In principle, any state or non-governmental organisation with hostile intentions may have the financial resources and the technological capacity to threaten a C4I system. Due to the low cost of the equipment needed for various forms of information attack, compared to the funds needed to develop a C4I system, as well as due to the fact that most of the knowledge required is freely spread around the world, threats can arise, including from terrorist groups or hackers.

[30] Colonel (r.) Professor Dr Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Științe ale Securității Naționale, no. 2, 2017, p. 71.

[31] The *National Strategy on the Digital Agenda for Romania 2020* was approved through Government Decision no. 245/7 April 2015.

[32] Colonel (r.) Professor Dr Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană, op. cit.*, p. 72.

Such attacks can be carried out for the purpose of disinformation, electronic espionage to obtain the global competitive advantage, clandestine change of sensitive data in the theatres of operations or for altering or interrupting the functioning of national critical infrastructures, such as those of energy, water, fuel, communications, banking or transport, which are essential for the society and economy functioning.

"At the military level, they can track sabotage, subversion, espionage or terrorism and are materialised in information leak exploitation/triggering, prevention of missions, inconsistencies in the course of operations"[33].

The specific threats to cyber security, which have become more and more serious lately, are also due to the fact that they are not limited by borders and they register a permanent increase in frequency and sophistication as well as to the universal belonging of the cyber space. The security risks involved in cyber-attacks and the global nature of their effects require joint international cooperation efforts to ensure the security of the information systems of the Alliance members.

In Romania, the general cooperation framework that brings together those authorities and public institutions with responsibilities and competences in the cyber security field is represented by the National Cyber Security System (NCSS). The NCSS activity is coordinated at strategic level by the Supreme Council for the Country's Defence.

"The common feature of confrontations in the cyber space is the continuous antagonistic relationship established between the threats that arise in the cyber space – terrorism, espionage, sabotage, subversion and organised crime, on the one hand, and information security, on the other hand. These threats are manifested in a very wide environment, provided by the information warfare, in a sharp conceptual and action interference between the electronic warfare, the hackers, the psychological warfare, economic warfare and in a complex typology of the cyber-attacks"[34].

To conclude, in the current information age, technological security is of particular importance and also concerns the computer networks (COMPUSEC) and the communication networks (COMSEC).

We consider that the specific threats to cyber security, which have become more and more serious lately, are also due to the fact that they are not limited by borders and they register a permanent increase in frequency and sophistication as well as to the universal belonging of the cyber space. The security risks involved in cyber-attacks

[33] Colonel (ret.) Professor Dr Gheorghe Boaru, *Război și apărare în spațiul virtual*, *op. cit.*, p. 54.
[34] *Ibidem,* pp. 54-55.

and the global nature of their effects require joint international cooperation efforts to ensure the security of the information systems of the Alliance members.

❖ **Vulnerabilities.**

As in any other field of activity, in the area of information and information systems as well, there are certain vulnerabilities, i.e. *"weak parts and weaknesses of the system, infrastructure, control environment or network design, which are not generated by the actions of the adversaries, but by their own solutions adopted, which can be attacked and exploited relatively easily, to damage the integrity of that system"*[35].

From a technical point of view, the vulnerability is presented as a system's feature, which can cause precise degradation to the system (the inability to perform its designed functions), as a result of being subjected to a precise level of effects, in an unnatural hostile environment.

From a technical point of view, the vulnerability is presented as a system's feature, which can cause precise degradation to the system (the inability to perform its designed functions), as a result of being subjected to a precise level of effects, in an unnatural hostile environment.

In information operations, *vulnerability* is defined as a weakness in the information security system design, procedures, implementation or internal control, which can be exploited to gain unauthorised access to information or the information system. In communications and information systems, the vulnerability is represented by a point where a system is likely to be attacked. Any computer or with a significant degree of computerisation system is vulnerable to attack.

In the military information systems, we notice the much higher weight of those specific to computers and computer networks. This weight is explained both by the fact that, in the current information systems, the subsystem of computers has a systemic integrating role, and by the fact that the communication subsystem is, in its most important elements, computerised.

At the same time, it should be highlighted that both the hardware components (workstations, network wiring etc.) and the main

[35] *Noul dicționar universal al limbii române*, Editura Litera Internațional, București-Chișinău, 2006, p. 1645.

software (operating systems) used are of civil origin, which results in the following disadvantages, from the security point of view:

- many of these are available to the general public, so their technical characteristics are known in detail by the potential adversary;
- the components produced especially for the military system, which, although designed and manufactured under the security conditions established and monitored by the military system, can nevertheless be subject to the actions of industrial espionage, a phenomenon specific to the aggression of the high technology free market and the IT market, in particular;
- the respective components allow for a reduced personalisation, so the results of a vulnerability study on the civil systems can be applied, to a large extent, also to the military ones;
- there are, in overwhelming proportion, imported components or, under best circumstances, produced and verified outside the military sphere, intentionally and very well camouflaged;
- the military systems are based on a logical component – the software one – which can also be attacked by logical means, therefore means that do not require expensive technologies, their range being continuously diversified by the contribution of the informational criminals.

With regard to the field of communications and information systems, the vulnerability is represented by a point where a system is likely to be attacked. Any information system, which has a significant degree of computerisation, is vulnerable to a variety of forms of attack.

Therefore, it is intended that the modern technology in the information systems to be tackled also with advanced technology, confirming the conclusion of the specialists that, in the future military conflicts, the greater the advantage obtained from the information and communications technology, the more it will increase its potential vulnerability.

It can be concluded that the main objective of contemporary military conflicts should not particularly materialise in the total destruction of the technique, armament or living force of the adversary, but especially in neutralising and disintegrating its complex systems, mainly information systems.

With regard to the field of communications and information systems, the vulnerability is represented by a point where a system is likely to be attacked. Any information system, which has a significant degree of computerisation, is vulnerable to a variety of forms of attack.

Besides the specific, external, internal vulnerabilities, the *"human errors"* type are not to be neglected.

Security policies and products can reduce the chances and likelihood for an attack to penetrate the computer system or, through the adopted security architecture, may require the aggressor to invest so much time and other resources that the attack will no longer be profitable.

Experts from around the world unanimously agree that there are no fully secure systems, so vulnerabilities are present even in the most advanced systems.

❖ **Threats**

A *threat* is a potential danger to the system. The danger may be represented by a person (a system cracker), a material element (an imperfect technical equipment component, for example) or an event (natural disasters, fires etc.), which may exploit a system vulnerability.

Covert threats are: espionage, sabotage, subversive acts, terrorism, acts that make up the specific crime.

Threats are analysed in relation to events that may occur as a result of their activity, events called attacks, as well as vulnerabilities that can be exploited by them.

The specialised literature classifies the sources of threats according to several criteria, as described below.

According to the manifestation mode, the sources of threats can be:

- manifest or open, in sight, these being observable;
- covered, masked or conspired;
- accidental and natural.

Visible threats are: radio jamming, radio broadcasting or radio navigation; electromagnetic pulse (EMP); SIGINT activities; special operations.

Covert threats are: espionage, sabotage, subversive acts, terrorism, acts that make up the specific crime.

Visible threats are: radio jamming, radio broadcasting or radio navigation; electromagnetic pulse (EMP); SIGINT activities; special operations.

Accidental and natural threats are classified as follows:

- natural: lightning, floods, earthquakes, extreme temperatures, strong wind;
- accidental: human errors, software errors, as well as hardware failures;
- fires, water leaks, dangerous voltages in the supply network.

According to their origin, the sources of threats can be: from the inside, from the outside or from the environment.

Within the planned information aggression, the possible threats to the military information systems come from all three types of sources.

When a message is transmitted through a communication channel, there are many general, voluntary or accidental threats.

❖ **Risks**

As a general approach within the military domain[36], the *risk* is defined as the probability and severity of a loss, related to the existence of dangers. Distinctly, the risk is seen as a limit, a maximum threshold for which a countermeasure established by norms has been shown to be effective in eliminating a vulnerability, in correlation with a given level of susceptibility and threat.

The risk defines an indicator, which represents the probability and the rate of occurrence of an event or action that, whenever occurring, causes the information itself or the material support of the information to deteriorate.

The risk defines an indicator, which represents the probability and the rate of occurrence of an event or action that, whenever occurring, causes the information itself or the material support of the information to deteriorate.

There is a directly proportional relationship between vulnerability and risk in relation to threats[37].

Given that we cannot influence threats in any way, implicitly not the probability of occurrence, the only way to reduce the risks is the leverage of action on the vulnerability, respectively the degree of vulnerability.

ATTACKS ON COMMUNICATIONS AND COMPUTER NETWORKS

Attacks on communications networks can be grouped according to certain criteria. Depending on where they are executed, the attacks can be: local or remote.

Local attacks materialise by compromising the security of a network by a local user.

---

[36] Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare, op. cit.,* pp. 39-40.

[37] Gheorghe Boaru, Vasile Păun, Marcel Răducu, *Managementul riscurilor în acțiunile militare,* Editura AÎSM, București, 2003, pp.17-25.

The risk of compromising the security of a network can be addressed (eliminated, diminished, distributed) in several ways:

- granting privileges strictly necessary to the local users, for the fulfilment of daily tasks, according to the tasks assigned in the job descriptions;
- network surveillance, in order to prevent possible attempts to breach the norms required to comply, including after the end of the working hours;
- access restriction to important network equipment;
- balanced distribution of complex tasks to personnel within the military organisation.

However, there is the unfortunate possibility that these protection measures may be ineffective, if there are traitors within the network that contribute to compromising the security measures of the system.

Therefore, in order to grant privileges to use the network resources, users must be ranked on several levels of trust, depending on how long they have been acting in that network, their behaviour and the severity of security events in which they were involved.

Remote attack is an action initiated on a communications network or on a network equipment, when the aggressor initially has no control.

The remote attack can be carried out in three stages:

The first stage is an information one, in which the attacker must discover information about:

- network administrator;
- network equipment and their functions;
- operating systems used;
- vulnerability points;
- network topology;
- security policies etc.

This first stage is assimilated to an attack, called a **reconnaissance attack**, and consists in the unauthorised mapping of a computer system, its services and its vulnerabilities.

The second stage is one of tapping and consists of cloning a target and attacking it, to simulate the response mode.

The third stage is to launch the attack on the network. A successful attack runs fast when the network presents vulnerabilities.

According to another classification of the attacks addressed to the communications/information networks, according to the way they are carried out, as a destination and source, the attacks can be **focused** on a single target (a particular server from a single device is attacked) or they can be **distributed** (initiated from multiple locations or by multiple equipment at the same time).

According to the way the attacker interacts with the unauthorised accessed information, as a result of the successful action, two categories of attacks are distinguished: **passive** and **active**.

Passive attacks are those attacks where the attacker only monitors the way information flows through the system without interfering in this flow. Also, in the category of passive attacks, the interception itself (radio, fibre/optic fibre) and the goniometry (radio) are included.

Passive attacks are those attacks where the attacker only monitors the way information flows through the system without interfering in this flow. Also, in the category of passive attacks, the interception itself (radio, fibre/optic fibre) and the goniometry (radio) are included.

Passive attacks may have some common characteristics:

- they do not create immediate and detectable damages, because they do not delete or modify data, do not block the network, do not disturb the traffic;
- they violate the confidentiality rules;
- the goal is to listen to the data exchanged on the communication channels;
- the listened data are subject to other processing stages, in order to extract the information useful for other operations, including other passive attacks;
- they are difficult, even impossible, to notice.

These attacks can be carried out by various methods, such as: surveillance of telephone calls, radio or radio broadcasts, exploitation of emitted electromagnetic radiation, for the purpose of transmitting information or compressive parasitic radiation, data routing, through weaker protected secondary nodes.

Active attacks are attacks through which the attacker materialises his action in the destruction, theft, alteration or resuming the messages or inserting false messages.

Active attacks are aimed at stealing or falsifying information transmitted or stored in the network, reducing network availability, by overloading it with packets (flooding), disrupting or blocking communications, by physical or logical attack on network equipment, and communication paths.

These attacks are more dangerous because they change the state of the computing, management and switching systems, as well as the data. There are a number of active attacks, in which case a new analysis is required, according to the criterion of the effect produced by them, as follows:

a. Attacks that mainly affect the organisational state:

- electronic jamming – consists in modifying the reception signals;
- disinformation – is achieved by intercepting and modifying the content of the message, followed by a timely retransmission of the communication;
- masquerade – is an attack, in which a network target (user, client, service or server) indicates another identity to retrieve confidential information (passwords, identification data, encryption keys, credit card information and other);
- replay – occurs when a message or component thereof is resumed (repeated), with the intention of producing an unauthorised effect;
- modification of messages – the message data are subjected, in an unauthorised way, to modification, insertion or deletion;
- Denial of Service attack (*DoS*) – occurs when an authorised entity fails to perform its function or when an intruder performs actions, which hinders another entity in performing other functions;
- service repudiation – occurs when an entity does not want to recognise a service performed.

b. Active attacks with a predominantly destructive effect – in the systems dependent on the computerised components, are realised by means of programs created for this purpose, which sometimes affect the computer security, including the servers. These attacks aim at unauthorised reading of information, but most often, partial or total destruction of data or even processing equipment. Of these destructive programs, we mention the following:

- viruses – represented by computer programs, which multiply by themselves in the programs of the attacked system, using the resident space in the memory/hard disk and blocking

the computer or, after a programmed number of multiplications, they can even cause damage;

- software bomb – is a part of a code or procedure, inserted in a necessary application, which can be launched by a scheduled event. The bomb maker informs about this event, letting it carry out the destructive actions programmed by the effect of the *"explosion"*;
- worms – most often produce destructive effects, similar to those of bombs and viruses. The difference is that the worms do not reside at a fixed address or multiply by themselves. Instead, they move permanently, which makes it very difficult to detect;
- The Trojan horse – is an application, which comes in the form of a known use function and which, concealed, fulfils another function.

Software bomb – is a part of a code or procedure, inserted in a necessary application, which can be launched by a scheduled event. The bomb maker informs about this event, letting it carry out the destructive actions programmed by the effect of the "explosion".

There are many possibilities of attacking information systems, which can exploit their vulnerabilities.

SPECIFIC INFORMATION SYSTEM VULNERABILITIES

Informational vulnerabilities are a component of the security vulnerability of the systems, generated by the factual states or internal processes of the organisation, which can reduce the response capabilities to possible threats, of any kind, including information.

Generally, information vulnerabilities are greater as the information networks and information structure are more complex, so they are harder to manage, being harder to organise and protect.

Also, it is considered that *"vulnerabilities increase directly proportional to the technological level implemented in the construction and operation of information systems equipment (particularly digital)"*[38].

The most known vulnerabilities, in the case of military information systems, are:

- errors in system design and operation;
- possibility of some technical components to fail;
- difficulties in the integral and integrated testing of the system;

[38] C. Alexandrescu, G. Alexandrescu, Gh. Boaru, *Sisteme informaţionale militare – servicii şi tehnologie*, Editura UNAp *"Carol I"*, Bucureşti, 2010, p. 294.

- excessive amount of information to be analysed;
- dispersion of users and access points over a wide geographical area;
- insufficient training of personnel in the national security field;
- failure to execute a new security accreditation, after a system modification;
- connecting computers from unclassified local networks to other classified networks;
- incorrectly configured/entered routers and firewall addresses;
- non-compliance with TEMPEST norms;
- exceeding the deadlines for changing passwords and encryption keys;
- non-restriction of Dal-in connections in LAN and non-restriction of electronic mail service;
- use of unclassified channels, for the transmission of classified information.

Regarding the analysis of the information infrastructure, it is considered that the main vulnerabilities could be the following[39]:

- the possibilities of intercepting information in the communications networks and computers both inside (by users) and outside (by opponents);
- the very large volume of information produced, transmitted and processed in the information systems, which can be subjected to research and attack, destroyed, forged or stolen by potential adversaries;
- the difficulty of managing the information infrastructure, due to its complexity, which determines the impossibility of detecting fraudulent access to information and favouring cyber-attacks;
- using the same frequency bands of both their own means and of potential adversaries;
- standardisation of the technical equipment, software components and databases used;

[39] C. Alexandrescu, *Ameninţări şi riscuri electronice privind sistemele informaţionale militare moderne în spaţiul de luptă*, in the volume of the Scientific Papers Session organised by *"Carol I"*, NDU – Information Systems SI-2007, pp. 107-115.

- the use of common elements of the national information infrastructure, which creates conditions for fraudulent access and disinformation;
- the possibility for the equipment supplying companies to previously incorporate, in the computing and communications equipment, some malicious software modules, which can be activated by the opponents, at certain times established by them, creating clutter and chaos in the information and in the decision-making networks;
- vulnerabilities to unauthorised intrusions (with malicious intent or lack of attention) due to the fact that organisations are connected to the Internet, Intranet or Extranet;
- failure to fully comply with EU and NATO requirements and standards regarding the compatibility and interoperability of information systems, particularly in terms of information exchange (message format), access to databases, automatic encryption of communications and the connection channels' characteristics;
- the possibility of using by potential opponents of the electronic warfare against the radio-electronic means of the main information and communication systems, especially on the channels that ensure the connection of the sources of information with the central bodies of fusion and data processing;
- the interception by the adversary (hostile forces) of the communications transmitted by radio, their decryption in a timely manner, in case of using non-performing cryptographic systems, and the use, for their own purposes, of this information, in order to obtain the information superiority;
- the current technical means of the information systems have not ensured the sound protection against the physical, electromagnetic and cyber-attack, these can be destroyed, damaged or extracted;
- placing the technical equipment (mostly the communication and computing means) of the information system in areas considered inadequate from the functional and physical/ electromagnetic security point of view, which increases

the vulnerability of interception of the information and of physical attack;

- using, for the information systems exploitation, of insufficiently verified and not loyal persons, predisposed to be recruited by potential adversaries and determined to carry out sabotage actions or to provide them with information obtained fraudulently;
- neutralising the shortwave radio link, especially at long distances, based on the propagation of electromagnetic waves, through the ionosphere, by changing its electrical characteristics;
- the existence, to the potential adversaries, of the electronic weapons with infra-acoustic radiation, based on the propagation in space of the subsonic waves, which act on the personnel, causing serious failures, vomiting, nausea, fear, depression etc., determining their inactivation, for certain periods of time, and, implicitly, the interruption of the information systems' functioning;
- installing antennas of the communication means in the open field or in spaces without natural protection properties, which allows slight malfunction and interruption of the connections, especially those made with radio stations and/or high-power radios;
- suppressing the information systems' access to the Internet, in order to isolate them and prevent the use of information from open sources;
- use of the Internet for terrorist actions, disinformation and cyber-attacks on information infrastructure;
- improper infrastructure design, with reduced information redundancy, excessively centralised and with low possibilities of existing information replication in the databases;
- insufficient concern for the concealment and masking of the information infrastructure elements, inadequate security and defence measures;
- insufficiently studied measures to ensure communications security (COMSEC), computers security (COMPUSEC) and electronic

equipment as a whole by prohibiting (restricting) parasitic radiation interception (TEMPEST – Transient Electromagnetic Pulse Emanation Standard protection).

From the analysis carried out, it turns out that there are numerous vulnerabilities, but, among these, the most important ones are those concerning: optimal organisation of information systems, improper choice of the technical equipment used and of the commercial software products, the manufacture of the application software and the databases, as well as software, for the automatic encryption of information in information systems, unfair or insufficiently verified personnel.

There are numerous vulnerabilities, but, among these, the most important ones are those concerning: optimal organisation of information systems, improper choice of the technical equipment used and of the commercial software products, the manufacture of the application software and the databases, as well as software, for the automatic encryption of information in information systems, unfair or insufficiently verified personnel.

CONCLUSIONS

In the new global information environment, technological development has brought, along with the advantages and facilities it provides, a series of threats, risks and vulnerabilities to the security of information and information systems.

Concerns about addressing threats, vulnerabilities and risks, in the specific dynamics of the last decades, include an extended area, important efforts being concentrated in the information field.

Considering that information attacks are a threat to the information systems security, specialists are trying to implement new methods of fighting against information and information attacks, which are mainly aimed at protecting their information and information systems.

Starting from the fact that there can be no absolute control, but merely a limitation, the experts have launched a new offensive, in order to improve the legislation, strengthen the role of the profile agencies and to perfect the products necessary for the detection of IT and information crimes.

For a vulnerability to be exploited, it must be known or discovered by a threat. This makes it important to follow the application of the "*need to know*" principle, while complying with security measures and their application both by personnel and in the field of technology.

This makes important the appropriate reaction of the institution, in identifying any vulnerability that may affect it.

We appreciate that estimates can be made, with a certain level of confidence, but it is difficult, scientifically, to accurately analyse threats

to information systems. These estimates depend, first and foremost, on the human factor, its mindset, its subjectivity and the implying uncertainty.

Ensuring the security of military information systems is a complex and difficult activity, as this is done through the implementation, within or outside the national territory, based on the international and coalition/national and international laws and regulations, of some specific measures which, as a rule, are: general, organisational, physical protection, personnel protection, document protection, legal and procedural protection, industrial security, as well as particular measures, computer system and communications security.

The security of the communications and information system, a component of the information system (C4I), aims at protecting information, the hardware and software components, through efficient measures, which can prevent the access to information and the interference in the information processes (collection, transmission, storage, processing, distribution, conversion, display).

In local computer networks and in the communications system, security measures must ensure: authentication (verification of the identity of a remote communication entity); control of access to resources; data confidentiality; data integrity; physical protection of technical equipment.

Generally, the security of information systems is a very complex field, in which the entire personnel is involved and which, through the restrictions and algorithms that they adopt and impose, often generates excess contradictions and bureaucracies. With all the shortcomings and drawbacks it can generate, it is better to follow the rules than to jeopardise the mission.

The increasing dependence of the command and control activities on the security of information systems leads to the increase in the typology of vulnerabilities that organisations must face.

Moreover, the issue of protection often has to consider the interconnection of private networks with public services. If we add to this aspect the problem of information sharing, a rather complicated picture is outlined, in which the implementation of effective controls becomes a difficult task for the IT&C specialist.

We consider that information security is not just a technical problem, but it is, first of all, a managerial problem.

The ISO/IEC 17799 security standard responds to the needs of organisations of any type, public or private, through a series of information security management practices. The standard can be used, depending on the degree of exposure of each organisation individually, to raise awareness, at the management level, of information security issues, or to create an organisational culture regarding information security, or to obtain information certification for the security system.

The ISO/IEC 17799 security standard responds to the needs of organisations of any type, public or private, through a series of information security management practices. The standard can be used, depending on the degree of exposure of each organisation individually, to raise awareness, at the management level, of information security issues, or to create an organisational culture regarding information security, or to obtain information certification for the security system.

Establishing the security requirements, the necessary measures to ensure the desired level of control, has a subjective component, being difficult to quantify, in monetary terms, the loss suffered, in the event of a security incident.

From the study of this very complex field of information security and military information systems we consider a few distinct measures:

- optimal organisation of information systems, so as to ensure the fundamental condition, for their efficient functioning – their reconfiguration, mobility and adaptability to the constantly developing information environment;
- keep in mind the conditions, restrictions and standards that are set, as a member of the EU and NATO. These require to be fully respected and applied firmly, in order to meet the compatibility and interoperability criteria with other organisations in the country and abroad;
- the classified information will be disseminated only to persons who hold an appropriate security certificate;
- compliance with NATO regulations[40], whereby the application of the minimum standards for ensuring the security of information is mandatory for all personnel who has access in the information system;
- increasing responsibility and control for the protection of classified information by each person who owns, processes or is aware of such information;

[40] *AD 70-1, ACO Security Directive*, NATO HQ, Brussels, 2006, p. I-2-4.

- periodically carrying out risk assessments on information systems and their processing in front of military personnel, in the form of lessons learned;
- purchase of new information technologies to take into account the purpose of reducing the specific vulnerabilities;
- the professional training to include topics in the field of information security and information systems.

In conclusion, in the current information age, technological security is of particular importance and also concerns the computer networks (COMPUSEC) and the communication networks (COMSEC).

Unfortunately, there is no 100% safe security system. However, by defining a realistic security policy, the most effective ways of avoiding the risks to which the military information network is subjected must always be found.

BIBLIOGRAPHY:

1. ***, AAP6 (2008), *NATO Glossary of Terms and Definitions*, 2008.
2. ***, AD 70-1, *ACO Security Directive*, NATO HQ, Brussels, 2006.
3. ***, AJP-3(C), *Allied Joint Doctrine for the Conduct of Operations,* NATO, 2019.
4. ***, AJP-2*, The Allied Doctrine for Intelligence, Counterintelligence and Security,* 2003.
5. ***, *Doctrine of the Romanian Armed Forces*, Bucureşti, 2012.
6. ***, *Doctrine of Intelligence in Joint Operations* (of the Canadian Armed Forces), 2003.
7. ***, *Doctrine for the Armed Forces Intelligence, Counterintelligence and Security*, Bucureşti, 2005.
8. ***, *Doctrine of Intelligence Support to Joint Operations,* 2003.
9. ***, FM 3-13, *Information Operations*, Washington DC, December 2016.
10. ***, FM 101-6, *Information Operations*, 1996.
11. ***, *Guidelines for the National Defence Strategy for the period 2015-2019*, Presidential Administration, București, 2015.
12. ***, IPS-3, *Doctrina pentru informații, contrainformații şi securitate a Armatei*, București, 2005.
13. ***, JP 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 2016.
14. ***, JP-2, *Intelligence in Joint Operations* (of the US Armed Forces), 2007.
15. ***, *Law no. 182/2002 on classified information protection.*

16. ***, *Norms regarding classified information protection in the Ministry of National Defence, approved through the Order of the Minister of National Defence no.M.9/2013,* published in the Official Gazette of Romania, Part 1, no. 115, on 28 February 2013.
17. ***, *National Strategy regarding Digital Agenda for Romania 2020,* approved by Government Decision no. 245/7 April 2015.
18. ***, *Romania's National Defence Strategy: "For a Romania that guarantees future generations security and prosperity"*, București, 2010.
19. ***, *Romania's National Security Strategy*: *"European Romania, Euro-Atlantic Romania: for a better life in a democratic, safer and wealthier country"*, Bucureşti, 2007.
20. ***, *Romanian Armed Forces Transformation Strategy*, București, 2007.
21. D. Albert, J. Garstka, R. Hayes, D. Signori, *Understanding Information Age Warfare,* Washington D.C., CCRP-Data publication, August 2001.
22. C. Alexandrescu, *Ameninţări şi riscuri electronice privind sistemele informaţionale militare moderne în spaţiul de luptă*, in the volume of Scientific Papers Session of *"Carol I"* NDU – *"Information Systems SI-2007"*.
23. Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale – fundamente teoretice –*, Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2009.
24. G. Alexandrescu, G. Boaru, C. Alexandrescu, *Sisteme informaţionale pentru management,* Editura Universităţii Naţionale de Apărare *"Carol I"*, Bucureşti, 2012.
25. Francisco Martínez Álvarez, Alicia Troncoso Lora, José António Sáez Muñoz, Héctor Quintián, Emilio Corchado, *Synthesis Informational Security International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019): Seville, Spain, 13-15 May, 2019 Proceedings,* Series: Advances in Intelligent Systems and Computing 951, Springer International Publishing, 2020.
26. Colonel (ret.) Professor Dr Gheorghe Boaru, *Război și apărare în spațiul virtual,* Revista de Științe Militare, published by the Academy of Romanian Scientists, No. 2, 2018.
27. Colonel (r.) Professor Dr Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Științe ale Securității Naționale, No. 2, 2017.
28. Colonel (r.) Professor Dr Gheorghe Boaru, Colonel Iulian-Marius Iorga, *Ciclul informational ca process, procesul și ciclul "Intelligence" în cadrul acțiunilor militare moderne,* Revista de Științe Militare, published by the Academy of Romanian Scientists, No. 1, 2017.

29. Gheorghe Boaru, Vasile Păun, Marcel Răducu, *Managementul riscurilor în acţiunile militare,* Editura AÎSM, Bucureşti, 2003.
30. Ion Ciobanu, Gheorghe Ilie, Aurel Nour, *Confruntarea informaţională şi protecţia informaţiilor*, Editura Detectiv, Bucureşti, 2006.
31. Abhishek Chopra, Mukund Chaudhary, *Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines,* Apress, 2020.
32. Vasile Dumitru et al.*, Sisteme informaţionale militare*, Editura CERES, Bucureşti, 2000.
33. James Dunningan, *O nouă ameninţare mondială Cyber-Terorismul*, Editura Curtea Veche, 2010.
34. Iulian Marius Iorga, *Securitatea informațiilor în acțiunile militare moderne,* Editura Universității Naționale de Apărare *„Carol I”*, București, 2018.
35. W.J. Karplus, *Sisteme de calculatoare cu divizarea timpului*, Editura Tehnică, Bucureşti, 1970.
36. Ovidiu Nicolescu et al., *Sistemul informaţional managerial al organizaţiei*, Editura Economică, București, 2001.
37. Ramjee Prasad, Vandana Rohokale, *Cyber Security: The Lifeline of Information and Communication Technology,* Springer Series In Wireless Technology, 2020.
38. *ENISA-Country Reports, 2008*, http://www.enisa.europa.eu.
39. *Information Systems*, Wikipedia, the free encyclopedia, http:/en.wikipedia.org/wiki/Information Systems.
40. *Information Security*, http:/en.Wikipedia.org/wiki/information security, 2009.
41. https://*fcnap.ro/transformarea-fortelor-armate-ale-romaniei-un-raspuns-direct-la-noile-provocari-ale-mediului-de-securitate/*.
42. www.dodccrp.org.