ROMANIAN
MILITARY
THINKING

SECURITY OF COMMUNICATION AND INFORMATION SYSTEMS OF THE NORTH ATLANTIC ALLIANCE IN THE CONTEXT OF HYBRID THREATS

Colonel Professor BEng Cezar VASILESCU, PhD
Regional Department of Defense Resources Management Studies, Brașov
Lieutenant Colonel Daniel DOICARIU, PhD Candidate
"Carol I" National Defence University
10.55535/RMT.2023.3.7

The article briefly presents some arguments regarding the need to ensure the security of communication and information systems at the NATO level. In this context, a series of threats, vulnerabilities and risks to communication and information systems are mentioned, as well as preventive measures and indicators on the adversary's actions.

In order to ensure the security of communication and information systems, there is a need for securing the "deployment environment" of the information, which is the electronic protection and security of the cyber space.

For this scientific approach, we have chosen the type of descriptive research with the aim of documenting and understanding the importance of the security of communication and information systems at the level of the North Atlantic Alliance, through the analysis of specialized literature, for the issue covered by the article.

We consider it opportune to carry out this work because communication and information systems in support of military operations involve specific security measures in cyber operations and electronic warfare, in the field of radio spectrum management, on own communication and information equipment/ networks etc.

Keywords: alliance; security; hybrid warfare; communication and information systems;

INTRODUCTION

Hybrid threats exist where asymmetric actions make their way to avoid a direct confrontation with the adversary. *"A hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, terrorists, or criminal elements, acting in concert to achieve mutually benefitting effects"* (ADP 3.0, 2019, pp. 1-3). Hybrid threats introduce new and complex elements into the battle, using atypical forces, technologies and techniques, not seen in classical warfare. A hybrid action can start from a conventional military attack and continue with propaganda actions, to reduce confidence in the political-military factor, depriving the population of basic services, such as medical care, supply of electricity, water, access to the banking system etc., causing a humanitarian crisis. Such combined actions are more difficult to counter. From the perspective of communication and information systems, they must be able to act, react, adapt, be resilient and robust to ensure services and facilities in times of peace, crisis or war.

Hybrid threats introduce new and complex elements into the battle, using atypical forces, technologies and techniques, not seen in classical warfare. A hybrid action can start from a conventional military attack and continue with propaganda actions, to reduce confidence in the political-military factor, depriving the population of basic services, such as medical care, supply of electricity, water, access to the banking system etc., causing a humanitarian crisis.

A definition of security is provided by Arnold Wolfers, in the article *"National Security as an Ambiguous Symbol": "Security, in an objective sense, means the absence of threats to the acquired values, and in a subjective sense, the absence of fear that such values will be attacked".* (Wolfers, 1952, p. 485). It should be emphasized that proactive and reactive measures contain security policies, guidelines and standards, issues related to security culture and the application of INFOSEC (information security) measures. Information security is necessary to protect the growing number of users, in the context of the increasing threats in cyberspace and the diversity of emerging and disruptive technologies increasingly available in the information technology (IT) market.

SECURITY OF COMMUNICATION AND INFORMATION SYSTEMS IN NATO

The security of communication and information systems is defined in AJP 6 as *"an element of information assurance, and consists of the application of security measures for the protection of communication, information, and other electronic systems; and the information that is stored, processed, or transmitted in these systems with respect to availability, integrity, authentication, confidentiality, and non-repudiation".* (AJP-6, 2017, pp. 1-4).

The security of communication and information systems contains defensive measures to counter cyber attacks, to limit their effects and to prepare network users and administrators. In order to ensure the security of communication and information systems, encryption of information is necessary and essential, and *"in NATO, cryptography is used at all levels (i.e., from strategic to tactical, and in static and deployed) and for mostly all communication services (e.g., voice, video conference, real- and non-real time data)".* (Ib., p. B-6).

The security of communication and information systems is integrated throughout the planning and execution of all military operations. Cyber defence activities are also essential elements in ensuring the security of communication and information systems, allowing services to operate in the context of hostile enemy actions in cyberspace. The information must be provided and protected correctly, based on three main and two secondary pillars: confidentiality, integrity, availability, as well as authentication and non-repudiation (*figure no. 1*), on which we will focus in the following:

The security of communication and information systems contains defensive measures to counter cyber attacks, to limit their effects and to prepare network users and administrators. In order to ensure the security of communication and information systems, encryption of information is necessary and essential, and "in NATO, cryptography is used at all levels (i.e., from strategic to tactical, and in static and deployed) and for mostly all communication services (e.g., voice, video conference, real- and non-real time data)".

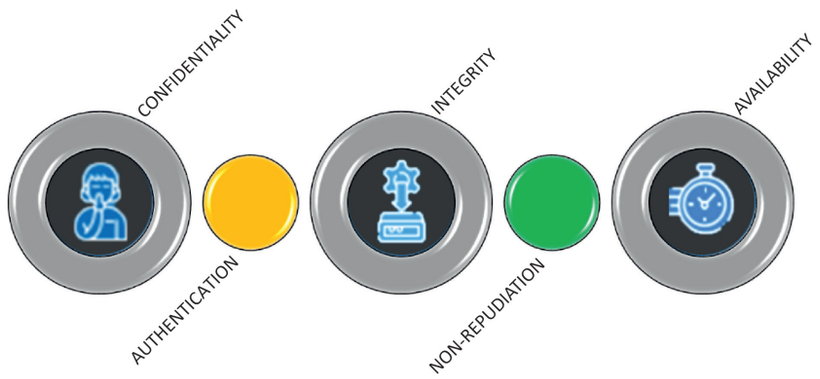

Figure no. 1: Characteristics of information security (authors' conception)

❖ *Confidentiality* implies that information is not made available or disclosed to unauthorized persons, entities or processes. It prevents the disclosure of unauthorized information.

❖ *Authentication* is the act of verifying the identity claimed by an entity.

❖ *Integrity of information* (including data) assumes that it has not been altered or destroyed without authorization. It prevents the manipulation of information by compromising its correctness, integrity or reliability.

❖ *Non-repudiation* is an assurance measure for the recipient that the information was sent by a certain person or organization and for the sender that the information was received by the intended recipients.

❖ *Availability* means that the information is accessible and usable at the request of an authorized person or entity. It consists of protecting information against intentional or accidental unauthorized attempts by denying information or systems. (Ib., pp. 1-13 _ 1-14)

For support with communication and information systems, NATO doctrine specifies several essential features. One of these essential features of communication and information systems is security, which *"guarantees the required levels of confidentiality, integrity and availability for services, systems and information, commensurate with the mission requirements"* (AJP-6, pp. 1_10).

The relationship between information assurance and the security of communication and information systems (including cyber defence) is also closely related to the other security environments, such as industrial, physical and personnel, according to *figure no. 2.*

The security of communication and information systems involves securing information, by applying security measures to the technique, equipment, networks and information transmitted or received. Cyber defence counters cyber attacks or mitigates their effects by integrating efforts for incident responses, preventive measures for the security of communication and information systems, but also the awareness of operators regarding the need to protect equipment.

When we talk about the security of communication and information systems, it also includes cyber defence *(according to Allied Joint Publication – AJP-6).*

Cyber defence counters cyber attacks or mitigates their effects by integrating efforts for incident responses, preventive measures for the security of communication and information systems, but also the awareness of operators regarding the need to protect equipment.

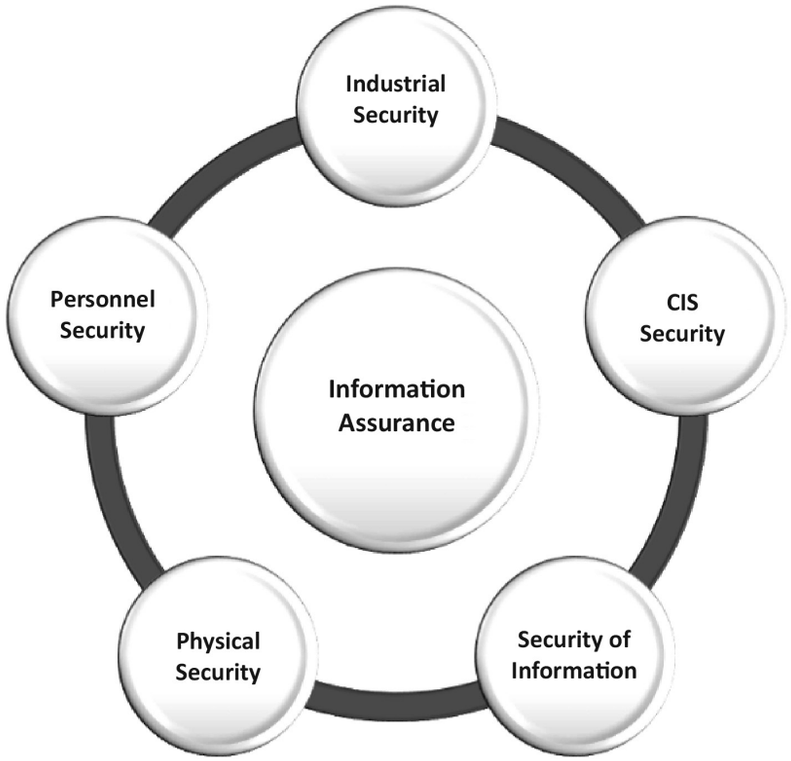

Figure no. 2: Relationship between Information Assurance and Communication and Information Systems (CIS) Security (Ib., pp. 1-14, adaptation)

In order to ensure and maintain the security of communication and information systems, it is necessary to guarantee the security of cyberspace. "Cyberspace security actions protect the networks and systems through all phases of network planning and implementation".

In order to ensure and maintain the security of communication and information systems, it is necessary to guarantee the security of cyberspace. *"Cyberspace security actions protect the networks and systems through all phases of network planning and implementation. Cyberspace security activities include vulnerability assessment and analysis, vulnerability management, incident handling, continuous monitoring, and detection and restoration capabilities to shield and preserve information and information systems".* (Wade, 2019, pct. 2_12, lit. E).

The operational environment is much larger than an area of operations. It includes the physical areas of the land, maritime, air and space domains, as well as cyberspace and the electromagnetic spectrum. The conditions and operational context that may influence a commander's decisions or the ability to act of forces and technical means. Communication and information systems provide services

and equipment depending on the mission, to support the exercise of command and control. Hybrid threats are carried out mainly in the information environment, the cyberspace and the electromagnetic spectrum being its components. In hybrid conflicts, control of the information environment is as important as control of physical areas. Moreover, the two environments are integrated and any activity that takes place in one affects the other.

Cyberspace includes *"the interdependent networks of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers"* (see JP 3-12, 2018, p. I-1).

The electromagnetic spectrum ensures the connection between the cyberspace and the physical domains in which the military actions take place. Own forces must ensure the security of their own communication and information systems in cyberspace and the electromagnetic spectrum and, as far as possible, to control the adversary's capability in an operation in these components of the information environment.

INFORMATION SECURITY AT THE NATIONAL LEVEL

In the *National Defence Strategy for 2020-2024 (SNApT)*, one of the national security objectives, from an internal perspective, aims at *"ensuring the security and protection of information and communication infrastructures that are critical to national security, as well as identifying, preventing and countering cyber threats posed by actors with strategic extremist-terrorist motivation or financially motivated"* (SNApT, 2020, p. 15). In this regard, in the Defence White Paper, a priority for action is represented by *"running continuous improvement programmes in the line of ensuring cyber security, communication systems and combating hybrid threats, in order to increase resilience in the face of new challenges"* (Defence White Paper, 2021, p. 18). In the two strategic level documents that regulate national defence, we have, among the priorities and objectives, cyber security and that of the communication and information system, which need to be implemented through Planning Directives and Major Procurement Programmes. Also, in the National Defence Strategy are found some of the threats, risks and vulnerabilities aimed at the field of communications and information at the national level, as it can be seen in *table no. 1.*

In the National Defence Strategy for 2020-2024 (SNApT), one of the national security objectives, from an internal perspective, aims at "ensuring the security and protection of information and communication infrastructures that are critical to national security, as well as identifying, preventing and countering cyber threats posed by actors with strategic extremist-terrorist motivation or financially motivated".

Table no. 1: Threats, risks and vulnerabilities in the field of communications and information
(extract from SNApT, pp. 25-29)

Threats	*- **Hostile actions of influence carried out in the public space** aimed at changing perceptions and influencing the civil society's behaviour are a constant threat to social security, and have the potential to proliferate due to the increasingly diversified means of communication in the online environment.* *- **Cyber-attacks** launched by state and non-state entities (cybercrime groups, hacker groups with or without ideological, political or extremist-terrorist motivation) on critical information and communications infrastructures.* *- **The integration of emerging and disruptive technologies** among the cyber entities' offensive instruments exponentially multiplies the sources of threat and enhances solutions to conceal cyber operations in order to create the appearance of false membership.* *- **Cybercrime** is on an upward trend, with more and more local groups specializing in illicit cyber activities (compromising ATMs and POSs, card cloning, unauthorized access to computer systems, illegal interception of computer data, posting of fictitious ads on intensively accessed trade sites, infecting information systems with ransomware, taking control over computer resources for virtual currency mining, as well as the use or exploitation of cryptocurrency for the conduct of illicit operations in the economic area).*
Risks	*- The **new technologies' use** by organized crime and cybercrime entities, terrorist or extremist groups and organizations, and actors interested in developing offensive actions **will be on an upward trend**.* *- The dependency of communications services on a **limited number of technology providers** and the existence of **unsecured flows of procurement of technologies** used in the provision of essential or critical services are phenomena with impact on the communications networks' availability and integrity.* *- **The risk of an interstate armed conflict remains low, yet there is an emerging risk of adapting hybrid offensive operations** to technological developments by continuously diversifying the modus operandi and coordinated resources in order to negatively impact the national interests, security included.*

The integration of emerging and disruptive technologies among the cyber entities' offensive instruments exponentially multiplies the sources of threat and enhances solutions to conceal cyber operations in order to create the appearance of false membership.

Vulnerabilities	*- **The low level of cybersecurity** of communication and information technology infrastructures in strategic areas (including as a result of vulnerabilities in terms of technology and procedures of communication operators' infrastructures) makes way for the conduct of cyber-attacks by state or non-state actors.* *- **Deepened technological gap** and under-exploitation of the benefits provided by the use of new technologies in most of the fields of activity may have a negative impact in terms of economic development and competitiveness, from the perspective of the research-development-innovation, as well as on medium and long term in ensuring national security.* *- **The poor security culture** at the level of civil society and decision-making apparatus may be exploited by hostile intelligence entities for the purpose of collecting information or carrying out influence actions.*

According to some specialists, *"in future military conflicts, the greater the advantage obtained from information and communication technology is, the greater its potential vulnerability would be"* (Boaru, Iorga, 2018, p. 31).

An action of particular importance at the national level was the establishment of the National Cyber Security Directorate (NCSD), which replaced the Romanian National Cyber Security Incident Response Team (CERT-RO), a fact materialized by Emergency Ordinance no. 104 of 22 September 2021, published in the *Official Gazette* no. 918 of 24 September 2021. Among the objectives of the NCSD activity, we highlight a few:

- *ensuring the security, confidentiality, integrity, availability, resilience of the elements of the national civil cyberspace, in cooperation with the institutions that have powers and duties in the field;*
- *ensuring the framework of strategies, policies and regulations to support the implementation of the national vision in the field of cyber security;*
- *the creation of the national cooperation framework between public, private, education and research institutions, to ensure*

Deepened technological gap and under-exploitation of the benefits provided by the use of new technologies in most of the fields of activity may have a negative impact in terms of economic development and competitiveness, from the perspective of the research-development-innovation, as well as on medium and long term in ensuring national security.

a realistic, common and coherent vision and approach regarding Romania's cyber security;

- *the international promotion and support of the national strategy in the field of cyber security* (Emergency Ordinance no. 104, 2021, art. 4).

Also, according to the Practical Guide for Operators of Essential Services (OES) – *Implementation of minimum measures to ensure the security of networks and information systems*, information security is a concern *"protecting the organization's assets against internal and external threats, threats that are classified according to the potential damage they can cause to the protected assets"* (Munteanu, Păuna, Constantinescu, Măgdălinoiu, Voinea, Găbudeanu & Anghel, 2021, p. 22). In this regard, the relationship between assets and vulnerabilities, threats and risks, according to ISO/IEC 27032 (Information Technology – Security techniques – Guidelines for Cybersecurity) is shown in *figure no. 3*.

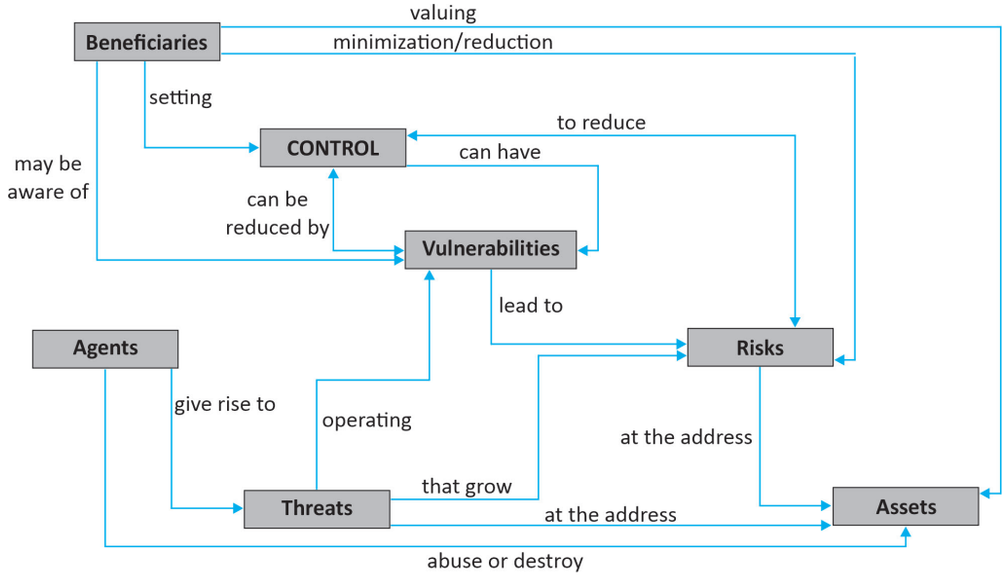

Figure no. 3: Relationship between assets and vulnerabilities, threats and risks (Ib., p. 23)

It is clear, therefore, that any analysis should consider the relationship between vulnerabilities, threats and risks. Risk relates

to each individual threat and vulnerability. If the probability of threats occurring is difficult to estimate, then risk reduction can be achieved by reducing vulnerabilities.

SECURITY OF COMMUNICATION AND INFORMATION SYSTEMS IN SUPPORT OF OPERATIONS

The military experiences of NATO forces in Iraq and Afghanistan can no longer be taken as a benchmark in the development and strengthening of the communication and information system. The military operations in the two countries have been characterized as counterinsurgency, support and stability missions. However, the conflict in Ukraine, presents us with a different reality, in which the pace of operations is accelerated, and human and equipment losses are considerably higher. The effects on the economies of European countries, and not only, have been felt since the beginning of this conflict.

The management, dissemination and control of the information transmitted through the communication and information equipment are essential from the perspective of mission accomplishment. Potential adversaries have understood this aspect and, in order to achieve their goals, are gathering technical and tactical intelligence to act with electronic warfare operations.

Such elements include:

- jamming on communications systems using the radio frequency spectrum;
- interception of communications in radio/radio relay/satellite networks;
- interference with the adversary's communication flow, and so on.

Communications and information systems planners can take steps to mitigate adversary threats in the radio frequency spectrum. Among the measures to reduce the electromagnetic signature in command points and in communication centres, eloquent are those specified in FM 6.02 (2019, p. A-1), as follows:

- careful site selection for communication equipment;
- employment of directional antennas;

ROMANIAN MILITARY THINKING

The military experiences of NATO forces in Iraq and Afghanistan can no longer be taken as a benchmark in the development and strengthening of the communication and information system. The military operations in the two countries have been characterized as counterinsurgency, support and stability missions. However, the conflict in Ukraine, presents us with a different reality, in which the pace of operations is accelerated, and human and equipment losses are considerably higher. The effects on the economies of European countries, and not only, have been felt since the beginning of this conflict.

- operations using the lowest power required;
- limiting radio transmissions;
- using burst transmission to minimize transmission time;
- using a random battle rhythm schedule.

Also, various measures can be taken to mask the radio, to capitalize the battlefield, electronic protection measures etc. These measures are applicable under optimal conditions, for short periods of time. Without continuously assured communications, command and control of forces suffers, which can result in loss of initiative. *"An enemy can use radio frequency direction finding equipment to locate any radio frequency emitter, such as a radio, satellite communications terminal, counter-improvised explosive device system, radar, or cell phone. Once they determine an accurate location, the enemy can direct lethal fires to destroy the capability"* (ATP 6-02.71, 2019, p. 3-20). Any of the mentioned situations is possible, if the security measures in the electromagnetic environment are not respected.

Information and communication systems support is much more than the transmission of information within a military operation, it is the link between information and decision, as well as between decision and action. Therefore, there is a concern about the security of communications and information to protect the content of their own information against the adversary.

Information and communication systems support is much more than the transmission of information within a military operation, it is the link between information and decision, as well as between decision and action. Therefore, there is a concern about the security of communications and information to protect the content of their own information against the adversary. Cryptographic systems allow the protection of information transmitted by users: *"Including COMSEC key management in operations planning is essential to enabling secure communications"* (FM 6.02, pp. 2-38), as shown in *Signal Support to Operations*, combat manual in the US Army. Communications security implies *"actions designed to deny unauthorized persons information of value by safeguarding access to, or observation of, equipment, material, and documents with regard to the possession and study of telecommunications or to purposely mislead unauthorized persons in their interpretation of the results of such possession and study"* (JP 6-0, 2019, p. GL-4). These electronic protection techniques support the security of communications, by preventing the enemy from identifying the electromagnetic signature. The existence of a CEMA (cyber and electromagnetic activities) officer can play a key role in electronic protection planning.

Radio operators should recognize and react when they identify electromagnetic jamming actions, in the context where enemy jamming and own electromagnetic interference are difficult to differentiate, complicating their tasks. For example, interference can be unintentionally caused by other own or adversary radio stations, electrical and electronic equipment in the surroundings, atmospheric conditions or malfunctions of own equipment etc.

Lieutenant General Ben Hodges, Commander of the US Land Forces in Europe, mentioned, in an interview granted in 2015, the shortcomings in the area of *"information technology"*, emphasizing the following aspects:

❖ *"Secure FM radios so US troops can talk securely and to allies without being jammed;*

❖ *Shared data that allows troops to see a common operating picture (COP), so that US and allies' commanders see the same situation on their screens;*

❖ *Secure digital networks to call in artillery fire by linking human observers and radars to the guns themselves".* (Freedberg Jr., 2015).

The use of technologies specific to communication and information systems can be hampered by various aspects, such as protocols, security measures, bandwidth and equipment interoperability, so that "a corps must be supported by a signals brigade at all times, with multinational elements attached to work through interoperability challenges prior to the first shot fired (…).

The use of technologies specific to communication and information systems can be hampered by various aspects, such as protocols, security measures, bandwidth and equipment interoperability, so that *"a corps must be supported by a signals brigade at all times, with multinational elements attached to work through interoperability challenges prior to the first shot fired (…). As communications architectures continue to develop at pace, it is also worth reiterating that the most effective capabilities of many member states will be dependent on systems that for security reasons cannot be brought in line with NATO STANAGS"* (Watling, MacFarland, 2021, p. 22). Standardization and interoperability agreements, the same paper says, assume *"network integration and protection efforts are only possible with the active participation of all key members of the corps team"* (Ib.).

The most important attacks that can be executed on communication and information systems are:

- *COMPUSEC attacks*, which may lead to: the unavailability of some services; unauthorized access to classified information stored, processed and transmitted through communication

and information systems; unauthorized access to management information; copying and evasion/stealing of sensitive information; complete blocking of some communication and information centres;
- *COMSEC attacks* materialized through cryptanalysis action or TEMPEST attacks (Turcu, 2014, pp. 17-18).

The COMSEC components in *figure no. 4* include:

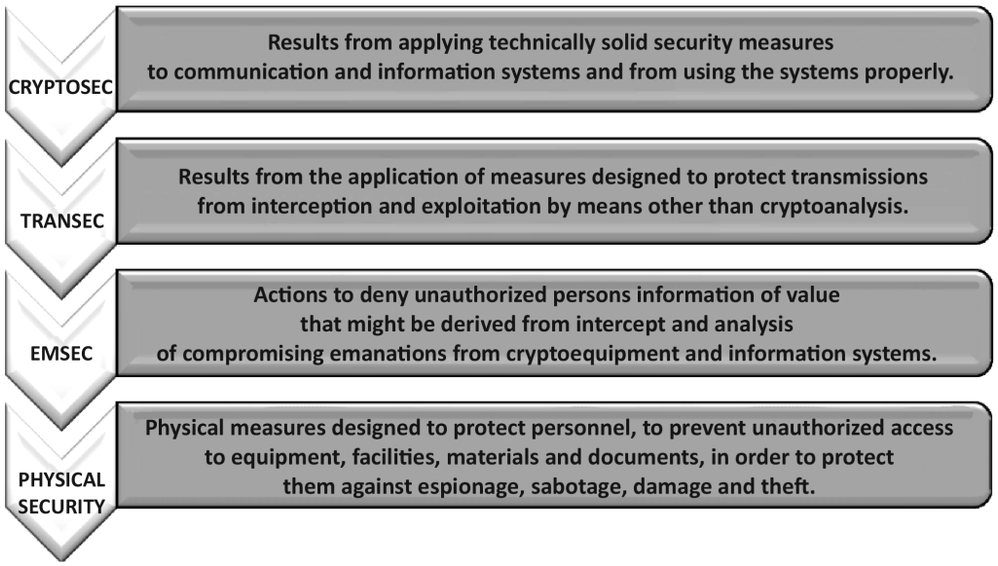

Figure no. 4: COMSEC components (ATP 6-02.75, 2020, p. 1_1)

Computer security – COMPUSEC involves the application of hardware, software and firmware security measures to prevent the unauthorized disclosure, modification or deletion of information or the unauthorized invalidation of functions in computer networks. COMPUSEC comprises the *"set of measures and controls that ensure the authenticity, confidentiality, integrity, availability and non-repudiation of information processed and stored in computers (servers and workstations)"* (Alexandrescu, C., Alexandrescu, G., Boaru, 2010, p. 256). The information transmitted through communication and/or information systems is vulnerable to interception and technical exploitation by the adversary. Also, *"communications are a particularly important component of the military information system*

and, implicitly, their security is of exceptional functional importance, therefore protection measures must be adequate, timely and effective and of great informational value" (Boaru, Iorga, p. 77). Countering the adversary's actions requires protecting information during its transmission and reception. The transmission of information at the level of large units and tactical units is carried out through the infrastructure of communication and information systems. NATO, at the corps/division level, requires the support of a communications and information brigade/battalion, made up of elements from several allied forces. In this regard, we believe that special attention should be paid to aspects related to interoperability, standardization and security. Information must flow uninterruptedly and safely, horizontally and vertically, and efforts to integrate and secure networks are possible only with the active participation of all Alliance members.

CONCLUSIONS

After the Cold War, the conflicts that took place did not hamper the HF, VHF and UHF communications of the NATO Alliance. Electronic warfare activities have been reduced or non-existent, but these conditions are changing in a potential conflict that opposes approximately equal forces. Under these conditions, electronic warfare will have a much greater role, and military communications will be unsafe or interrupted.

Depending on terrain, weather, adversary and so on, own communication and information systems must be redundant and resilient to ensure information security. Even if satellite communications systems provide essential support in command points, commanders must be prepared to conduct military operations also by radio or wire communications as needed.

User training, security culture and compliance with security measures are among the aspects that are necessary in the security of communication and information systems. Also, redundance is a measure to resolve some COMSEC situations (when the need arises), and frequency spectrum management is essential in ensuring the security of communications.

Depending on terrain, weather, adversary and so on, own communication and information systems must be redundant and resilient to ensure information security. Even if satellite communications systems provide essential support in command points, commanders must be prepared to conduct military operations also by radio or wire communications as needed.

For effective interoperability in communication and information systems, it would be ideal to have a single central authority in NATO, allowing the joint application of algorithms and encryption keys, this solution being able to ensure command and control at the level of the North Atlantic Alliance. However, it would also represent a challenge for implementing and ensuring security in national communication and information systems.

BIBLIOGRAPHY:

1. ADP 3.0 – *OPERATIONS* (31 July 2019). Department of the Army. Washington, DC.
2. AJP-6, *Allied Joint Doctrine for Communication and Information Systems* (February 2017). Edition A, Version 1.
3. Alexandrescu, C., Alexandrescu, G., Boaru, G. (2010). *Sisteme informaționale militare – servicii și tehnologie.* Bucharest: Editura Universității Naționale de Apărare *"Carol I"*.
4. ATP 6-02.75 (May 2020). *Techniques for communications security*. Headquarters. Department of the Army. Washington.
5. ATP 6-02.71 (April 2019) *Techniques for department of defense information network operations*. Department of the Army. Washington, DC.
6. Boaru, Gh., Iorga, I.M. (2018). *Securitatea sistemelor informaționale militare*. Bucharest: Editura Universității Naționale de Apărare *"Carol I"*.
7. FM 6.02 (September 2019). *Signal Support to Operations*. Department of the Army. Washington, DC.
8. JP 6-0 (October 2019). *Joint Communications System*.
9. JP 3-12 (February 2018). *Cyberspace Operations*.
10. Munteanu, A., Păuna, A., Constantinescu, C., Măgdălinoiu, G., Voinea, I., Găbudeanu, L., Anghel, T. (2021). *Ghidul practic pentru OSE – Implementarea măsurilor minime de asigurare a securității rețelelor și sistemelor informatice*. Editura Sitech.
11. Emergency Ordinance no. 104 on 22 September 2021, published in the Official Gazette no. 918 on 24 September 2021.
12. SNApT/*Strategia Națională de Apărare a Țării pentru perioada 2020-2024 „Împreună, pentru o Românie sigură și prosper într-o lume marcată de noi provocări"* (2020). Administrația prezidențială. București/National Defence Strategy for the period 2020-2024 – "*Together, for a safe and prosperous Romania in a world marked by new challenges"* (2020). Bucharest: Presidential Administration.
13. Turcu, D. (2014). *Securitarea Informațiilor*. Bucharest: Editura Universității Naționale de Apărare *"Carol I"*.
14. Wade, N.M. 2019). CYBER 1 – *The Cyberspace Operations & Electronic Warfare SMART book*. USA: FL, The Lightning Press, Lakeland.
15. Watling, J., MacFarland, S. (January 2021). *The Future of the NATO Corps*. Royal United Services Institute for Defence and Security Studies (RUSI).
16. Wolfers, A. (December 1952). *National Security as an Ambiguous Symbol*, p. 485, in *Political Science Quarterly*, vol. 67, no. 4.
17. https://breakingdefense.com/2015/09/upgraded-radios-networks-needed-for-russian-challenge-troops-fine-lt-gen-hodges/, retrieved on 17 June 2023.
18. https://sgg.gov.ro/1/wp-content/uploads/2021/03/CARTA-ALBA-A-APARARII-.pdf, retrieved on 17 June 2023.