CYBERSPACE IN THE OPERATIONS PLANNING PROCESS

Lieutenant Colonel Nicolae-Sorin MACOVEI

"Nicolae Bălcescu" Land Forces Academy, Sibiu

Ensuring cyber security has become increasingly important and culminated in the recognition of cyberspace as an operational environment, along with land, water, air and space.

Operations in the cyber environment must be planned, integrated and synchronised with operations in other operational environments. The armed forces carry out cyberspace operations and support activities in this field as part of the joint operation.

In the modern war, the superiority in the cyber environment ensures a decisive advantage to the commanders from all echelons. This is achieved through a human, technological and procedural combination. The military is accustomed to seeing the effect of their actions on the battlefield, in a physical environment. However, cyber operations take place in a virtual environment, and their effects are sometimes difficult to identify.

Keywords: cyberspace; cyber operations; planning process; tactical level; operational environment;

INTRODUCTION

Technological progress is what has led to major changes in the physiognomy of military conflicts and continues to be the main factor of change in terms of both the spectrum of threats and the development of new weapon systems.

Technological progress usually leads to major changes as far as the action and concepts are concerned, and the laws of the armed fight, which refer to the dependence of organisational structures, forms and procedures, confirm that technological progress produces major changes in the theory regarding the armed fight in almost all areas. Moreover, technological progress has led to the emergence of new operational environments, and cyberspace is a concrete example in this respect. Thus, in this space without physical limits, it is necessary to adopt new forms and procedures of action under the new technological and tactical capabilities. These capabilities determine organisational changes by creating more flexible structures with increased mobility, as well as the emergence of new military structures and specialities.

Technological progress for both computer system components and hardware devices used in communications networks has evolved exponentially lately (*Moore's Law and the Future of Mathematics*). This progress brings great benefits for commanders and staff because functional applications are made available, operational or tactical situations can be viewed in near real-time and the exchange of information that takes place in a very short time helps to optimise decision-making. However, given these benefits, through the technology used and their configuration, modern communication and IT systems are as vulnerable as any other computer system. The more computerised a command and control system (C2) is, the more vulnerable it is, and the security of communication and IT systems is a continuous and major concern for specialised personnel.

CYBERSPACE – FROM CONCEPT TO OPERATIONAL ENVIRONMENT

Over time, ensuring cyber security has become increasingly important at both NATO and EU level. The 2002 Prague Summit was the first time the Alliance's cyber security was addressed at a strategic level among allied states, and the need to protect the computer systems used was emphasised. At the Riga Summit in 2006, the Alliance's first cyber security strategy was issued, a strategy materialised in *"Policy* *on Cyber Defence"*. After its recognition, at the Warsaw Summit in 2016, as an operational environment, along with land, air and water, cyberspace has been given due importance. The cyber defence has become part of NATO's basic collective defence requirements. The Alliance must be prepared to defend its networks and operations against increasingly sophisticated and numerous cyber threats and attacks. Since 2016, the Alliance has made the field of cyber defence a top priority.

In 2018, at the Brussels Summit, the Alliance agreed to set up a Cyber Operations Command as part of NATO's Command Structure, designed to become fully operational in 2023 (Emmott, 2018). The following year, in February 2019, the Alliance endorsed a NATO guide that set out a set of tools to further strengthen NATO's ability to respond to malicious cyber activities.

In Romania, 2013 was the year when *Romania's Cyber Security Strategy and the National Action Plan on the Implementation of the National Cyber Security System* appeared. Through it, *"Romania aims to ensure the state of normality in the cyberspace by reducing risks and capitalising on opportunities, by improving knowledge, capabilities and decision-making mechanisms"* (Decision no. 271/2013, p. 11).

In the *Security Strategy*, four directions of action have been established to achieve this goal:

- setting the conceptual, organisational and action framework necessary to ensure cyber security;
- developing national risk management capacities in the field of cyber security and response to cyber incidents based on a national programme;
- promoting and enhancing the cyber security culture;
- developing international cooperation in the field of cyber security (Ibid, p. 11).

The United States Armed Forces, as well as other NATO armed forces, have updated their doctrines and textbooks to the new concept of cyberspace. Thus, in June 2018, the *Joint Doctrine for Cyber Operations (Joint Publication 3-12)* was republished which supports the planning, execution and evaluation of cyber operations.

The tactics and procedures for coordinating and integrating cyberspace and electronic warfare operations in support of land and joint operations were published in Field Manual (2017) – *Cyberspace and electronic warfare operations*. In this manual, in addition to the fundamentals of cyber operations, the terms and definitions specific to the field, as well the role, resources of commanders and the way to evaluate operations are presented.

In *Army Doctrine Publication* (2019), cyberspace is integrated as an information environment, along with the other components of the combat space (land, air, sea, space).

The Romanian Armed Forces have tailored to meet NATO trends. On 1 December 2018, the Cyber Defence Command was established, as the authority of the Ministry of National Defence in charge of cyber security, cyber defence and information technology, and in August 2020 the *"Doctrine of Cyberspace Operations"* was drafted.

CYBERSPACE IN THE CONDUCT OF OPERATIONS

The operations environment is characterised by complexity and dynamism and can be extended to all operational environments, thus becoming a multidimensional one. These characteristics are the result of the interactions, relationships, conditions, circumstances and influences of the different variables existing in the battlefield.

Cyberspace operations need to be planned, integrated and synchronised with joint operations. The armed forces carry out cyberspace operations and support activities in this field, as part of the joint operation. In the modern war, the superiority in cyberspace ensures a decisive advantage to the commanders from all echelons.

In order to create the specific effects of this operational environment, cyberspace missions require the engagement of various types of actions. These consist of defence actions, attack actions, intelligence gathering, surveillance and reconnaissance (ISR), Operational Preparation of the Environment (OPE) and security actions, all related to cyberspace (Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition, 2020). In order to plan, carry out and evaluate these actions, it is important to understand the differences between them and the purpose of each.

The military men are accustomed with seeing the effect of their actions on the battlefield, in a physical environment. However, cyberspace operations take place in a virtual environment, and the effects are sometimes difficult to identify by non-specialised staff or are sometimes identified too late.

How an opponent can attack the hardware and software infrastructure, having as result the destabilisation of the Command and Control System, is represented by the cyber attacks that take place of course in cyberspace. The *cyber attack* is defined as a *"hostile action carried out in cyberspace that could affect cyber security"* (Decision no. 271, p. 7), several operations being carried out to reduce the attack area.

Cyber defence actions are those *"actions carried out in cyberspace to protect, monitor, analyse, detect, counter aggression and ensure timely response against threats to cyber infrastructures specific to the national defence"* (Ibid, p. 7). These types of actions are critical to ensuring the functioning of communications and IT systems and are usually taken by specialists who plan, organise and operate communications and IT systems and networks.

Information gathering, surveillance and reconnaissance (SRI) actions are carried out in cyberspace to gather the information needed to support future cyber attacks or defences. These actions support the planning and execution of current and future cyberspace operations *(figure 1)*.

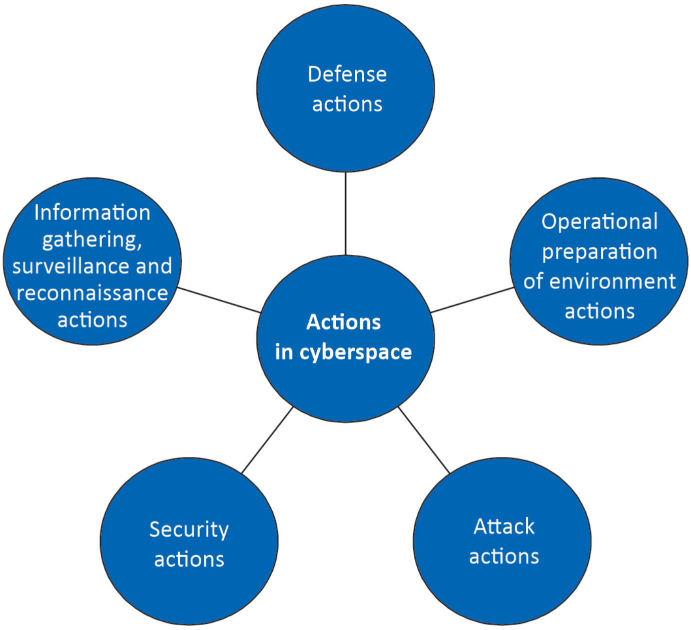
Defense actions
Information gathering, surveillance and reconnaissance actions
Operational preparation of environment actions
Actions in cyberspace
Security actions
Attack actions

Figure 1: Types of cyberspace actions (FM 3-12, p. 1-19)

Operational preparation of environment (OPE) measures are activities carried out for planning and preparing potential military operations, but not related to the information environment (Ibid.). These include identifying data and information, system/network configurations, or the physical structure that connects a network or system (applications used, ports, assigning network addresses, or other identifiers) to determine system vulnerabilities. We can add here actions taken to ensure access and/or control over the system, network or data during potential hostilities.

Security actions aim to achieve the *"state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information saved or in transit, public or private resources and services, from cyberspace. Proactive and reactive measures may include security policies, concepts, standards and guidelines, risk management, training and awareness-raising activities, implementation of technical solutions for cyber infrastructure protection, identity management, consequence management"* (Decision no. 271, p. 7).

Cyber security is achieved through technical, procedural and human measures. The human factor is the one who combines all security measures. Thus, to ensure cyber security, the challenges and threats in the new (cyber) operational environment must be known by all users/operators of information systems. There is a need to create, develop and train a culture of cyber security. Most computer-system users are unaware of this phenomenon and identify the need to develop a cyber security culture among them.

Computer networks of own and enemy forces, communication systems, computers, cell phone systems, social networking sites and technical infrastructures are some of the main components of cyberspace.

Although cyberspace coexists with other operational environments, it is a separate environment. It penetrates land, air, sea and space operational environments through communications and computer networks interconnected through various transmission media. Freedom of manoeuvre in cyberspace allows mission control and freedom of manoeuvre in other areas. Each physical operational environment has its cyber environment, and taken together, they form the combined cyber environment.

CYBER SPACE IN THE PROCESS OF PLANNING OPERATIONS AT A TACTICAL LEVEL

Given the importance cyberspace has reached in conducting military operations, it should play a similar role in the planning of operations. Operations' planning in cyberspace is an integral part of the operations planning process, intending to develop the specific annexe to OPORD/OPLAN.

Commanders at all levels must be aware of the importance of cyberspace in achieving the objectives and mission received. A well-performed enemy cyber attack can have the same effect as an artillery fire on the command point, respectively its decommissioning.

Cyberspace operations can be very complex and, to carry out an efficient planning process, it is recommended that four levels of planning for these operations are considered: technical, tactical, operational and strategic. Therefore, compared to the process of planning operations in a traditional operational environment, where it is carried out on three levels, in the case of planning cyber operations, the technical level must be the starting point. Proper incorporation of technical aspects is of critical importance in the conduct of effective cyberspace planning *(figure 2)*.

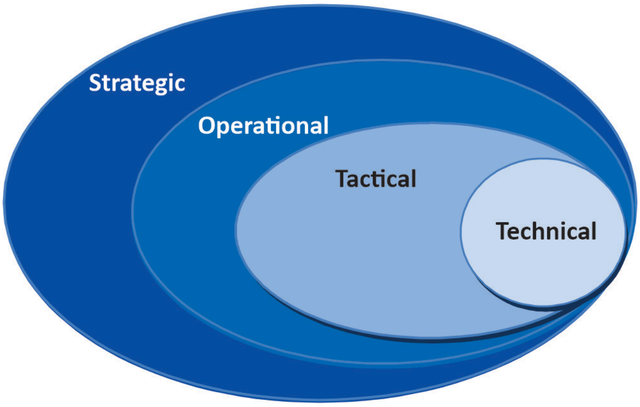

Figure no. 2: Planning levels (Barber et. al., 2015, p. 3)

Commanders do not as intuitively understand the technical details associated with cyberspace operations and planners as they do with the capabilities and limitations of combat technique (tanks, ships, or aircraft). The complex and dynamic nature of cyberspace, as well as its technical characteristics, often leads to the analysis and planning of operations beyond those planning practices and procedures found in traditional doctrine.

Cyberspace operations planning takes place simultaneously with the operation planning process, following its stages and phases. The products resulting from the planning are usually those provided in the Operations Planning Manual.

Given that there are still no specialised structures for cyberspace operations[1] at the tactical level, the planning tasks are distributed to the staff of the unit's staff. Staff members responsible for the planning and integration of cyber operations participate in the activities of the decision-making process.

[1] The new NATO capability targets stipulate the establishment of regulatory and command elements at the strategic and operational level, respectively tactical level execution structures, equipped and properly trained, able to execute specific actions in Cyber Security.

An important role in the operations planning process is played by the information structure, which will carry out the activity of information preparation of the battlefield, including the cyberspace. It is a challenge for the intelligence structure because the employees involved in this activity must be trained and know the peculiarities of the cyberspace. To perform this task as efficiently as possible, it is recommended that the intelligence structure cooperates closely with the planning structure of the IT and communication networks, namely the communications and IT structure.

A complex analysis provides the people involved with the relevant information to understand, visualise and describe the operational environment, and the decision made may be relevant.

Cyberspace, as part of the operational environment, must be analysed in the first phase from the perspective of the information environment. The information environment is characterised by the physical, information and cognitive dimensions.

The physical dimension of the cyber environment is represented by the physical elements of the network that include communication networks, computer systems and network infrastructures. The physical dimension provides access and control of information and data by users, represented by individuals or groups.

The information dimension is represented by the information that can be found in one of the two states: in transit or saved on disk. This dimension is directly connected to cyberspace due to the volume of information saved or in transit; it ensures the collection, processing, storage, dissemination and display of text, images or data. The informational dimension ensures the connection between the physical and the cognitive dimension.

The cognitive dimension includes the knowledge of those who transmit, receive, respond to or act on information. The cognitive dimension in cyberspace is represented by individuals, groups or organisations. Cyberspace connects the data and ideas of those who send, receive, respond to, act on, or add new information (FM 3-12, p. 1-13).

At the same time, the cyberspace is described as a sum of 3 layers: the physical layer, the logical layer and the *"cyber-persona"* layer (FM 3-12, Ibid.), layers that allow the understanding of the context and the creation of operational opportunities.

The physical layer of cyberspace refers to that geographical component as part of the physical dimension. The geographical component, in the present situation, represents the location of the network elements in one of the terrestrial, aerial, maritime or cosmic operational environments. The physical layer consists of hardware components, system applications and infrastructures (wire, wireless, cable links, electromagnetic, satellite or optical waves) that make up the network and the existing physical connections (wires, cables, radio frequencies, switches, servers and computers).

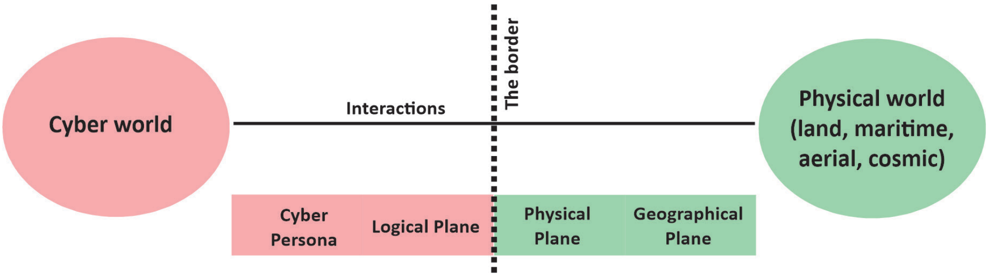

Figure 3: Planes of cyberspace (Azmi, 2019, p. 25)

The logical plane consists of the interconnection of the components of the physical network in an abstracted way. For example, network nodes in the physical plane can logically connect to form entities in cyberspace, but physically they do not depend on a particular node, path, or individual.

The cyber-persona plane is a digital representation of individual identity or entity in cyberspace. This plane is represented by users or consumers of network services.

It can be said that cyberspace is represented by communication networks and computers interconnected by the logical plane, which allow information to be accessible from any point, using the physical plane consisting of wired or wireless connections with high data transfer speeds, which is accessed by people using the cyber-persona plane.

In the intelligence analysis of the cyberspace, the analysis of these dimensions and planes provides an overview, but to have a complete image, its characteristics must be taken into account.

To identify the characteristics of cyberspace, we must start from the definition – an extensive and complex network, consisting of network nodes that are found in each operational area, connected by different transmission media. Therefore, the first feature of cyberspace is the *network feature*. The core of these networks is the technological infrastructures consisting of several distinct enclaves connected in a single logical network that allows the transport of data. The identification of these infrastructures and operations is done by analysing the planes of cyberspace, the dimensions of the information environment, the variables of the operational environment and other technical aspects specific to wired and wireless communications and IT networks (FM 3-12, p.1-15).

Because cyberspace provides interaction between individuals, groups, organisations, and states, another feature of cyberspace is the social feature. Computer systems and computer networks enabled the possibility of quickly creating, storing, processing, manipulating and transporting data and information for a small or very wide audience. Text messaging, e-mail, social networking sites and other forms of interpersonal communication are possible due to cyberspace.

Technological progress increases the complexity of the hardware and software components and devices of the communications and computing system, and as cyberspace is dependent on these components, it can be said that technological progress directly influences cyberspace. In other words, another feature of cyberspace is the *technological feature*. Moreover, it is a requirement that the personnel operating these pieces of equipment be one with intensified technical skills.

Interdependence and interrelationship are also specific to cyberspace, as operations in the other four operational environments are dependent on cyberspace. Besides, there is interdependence and interrelationship between cyberspace and the information environment. The distribution of information and data, their timeliness and quantity are directly dependent on the capabilities and limitations of the network infrastructure.

Easy access, the complexity of networks and applications, lack of security considerations in network design and application development, inadequate user activity give cyberspace the *characteristic of vulnerability*. Access to cyberspace by an individual or group of individuals who own a network device is easy, and an individual with a single device may be able to disable an entire network. The vulnerability of systems operating in cyberspace requires that measures be taken to reduce risks and protect cyberspace. The effects generated in cyberspace can have a global impact on physical domains.

Understanding the vulnerabilities and components of the operational environment allows the decision to be relevant, context-related. The continuous application of these analytical frameworks allows the commander and staff to analyse the cyberspace from different perspectives throughout the operational process.

CONCLUSIONS

Cyberspace is playing an increasingly important role in leading the armed fight. Some cyberspace actions are ongoing, regardless of the existing alert state or the occurrence of a conflict. Defence and security cyberspace actions must be a constant concern of specialised structures and must also be in the attention of commanders of all structures. The new weapons systems, in addition to offering numerous operational advantages, also present vulnerabilities due to the interconnection with cyberspace.

Cyberspace plays an important role in the planning process, and if used properly, actions planned and carried out in this environment can replace some of the effects of other types of military action involving high resource consumption. As a specificity of the operational environment, there is the time when hostile actions are carried out - long before the official launch of the other operational environments.

Therefore, the process of cyberspace operations planning may not take place at the same time as the planning of the operation to be performed.

BIBLIOGRAPHY:

1. Azmi, R., Kautsarina, K. (2019). *Revisiting Cyber Definition*. ECCWS 2019 18th European Conference on Cyber Warfare and Security, https://books.google.ro/books/about/ECCWS_2019_18th_European_Conference_on_C.html?id=b8-hDwAAQBAJ&redir_esc=y, retrieved on 22 September 2020.
2. Barber E.D., Bobo T.A., Sturm P. K. (2015). *Cyberspace Operations Planning: Operating a Technical Military Force beyond the Kinetic Domains in Military Cyber Affairs*. The Journal of the Military Cyber Professionals Association. Vol. 1, no. 1, art. 3, https://core.ac.uk/download/pdf/71958458.pdf, retrieved on 24 September 2020.
3. Emmott, R. (2018). *NATO Cyber Command To Be Fully Operational in 2023*, https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9, retrieved on 24 September 2020.
4. ADP 2-0, *Intelligence*, 2019.
5. Congressional Research Service (4 June 2020). *Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition*, https://crsreports.congress.gov, retrieved on 12 September 2020.
6. FM 3-12, *Cyberspace and Electronic Warfare Operations*, April 2017.
7. FM 3-38, *Cyber Electromagnetic Activities*, February 2014.
8. *Decision no. 271/2013 to Enforce Romania's Cyber Security Strategy and the National Action Plan on the Implementation of the National Cyber Security System*. Government of Romania, 23.05.2013.
9. *Joint Publication 3-12, Cyberspace Operations*, 8 June 2018.
10. *Moore's Law and the Future of Mathematics*, https://rum.journal-headerpop.com/make-mine-double-moores-law-824535, retrieved on 14 August 2020.

WEBOGRAPHY:

1. https://www.cybercommand.ro, retrieved on 15 September 2020.
2. https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber/157270/, retrieved on 13 September 2020.

3. https://intelligence.sri.ro/evolutia-amenintarii-cibernetice/, retrieved on 26 September 2020.
4. https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9, retrieved on 10 September 2020
5. https://rum.journal-headerpop.com/make-mine-double-moores-law-824535, retrieved on 21 September 2020.