EDUCATION IN THE CYBER SECURITY FIELD AND IMPLICATIONS FOR NATIONAL SECURITY

Captain(N) Professor Sorin TOPOR, PhD.*

Abstract: *The purpose of this paper, by presenting relevant aspects related to cyber security training at the level of NATO states and partner countries, is to justify the need to establish a national strategy in order to prepare the population and the territory for dealing with hypothetical hybrid and cyber-attacks.*

Based on this strategy, any institution can identify the role, place and possibilities of its involvement, the investment in education thus becoming a strategic topic of the global equation of national security.

Keywords: *cyber security, cyber security education, cyber operations*

Introduction

Currently, the leaders of the governance structures are faced with the new challenges generated by adapting the security requirements of the information systems that must operate in a free cyber space. These result in the identification and establishment of new responsibilities, much broader than those known as belonging to the fields of IT&C and Communications Security (COMSEC).

The tendency of increasing, at an exponential rate, of the information systems functional abilities of each other interacting and communicating, is diversifying, their complexity being more and more present in the daily activities of the human society, in different forms, from the mobile communications devices to computers integrated into life insurance platforms. All provide the human life comfort, thereby understanding the raising of the living standard in a computer and robot assisted manner. Under these aspects, defense structures also follow the ways of integrating information systems, implementing or modernizing a

* Universitatea Națională de Apărare „Carol I”, topor.sorin@unap.ro

multitude of information technologies designed to function independently or integrated into complex targeting, communications or strike vectors.

In this context, the requirement of cyber security will increase, covering, in a short time, everything that represents the concept of national security. Even if this opinion seems a little random, we must accept that the information has far surpassed the other dimensions of a conflict environment. And I am not just talking about war. Conflict marks our human existence. Conflict occurs when there is no harmony. Conflict is present during the negotiation of a position in an organization, during the conquest of a new market, during the attempt to convince someone of something etc. Today, conflict is dependent on information. It is managed with and through information.

Depending on conditions, in order for a piece of information to be transmitted at a distance at which the receiver would normally not be able to perceive it through their senses, communication equipment is needed. The human-equipment-environment relationship determines the creation or the modernization of information systems. In figure 1 we sought to show how the remote communication functions in real time with so as to ensure a high level of information security which marked the rhythm and directions of evolution of the information systems.

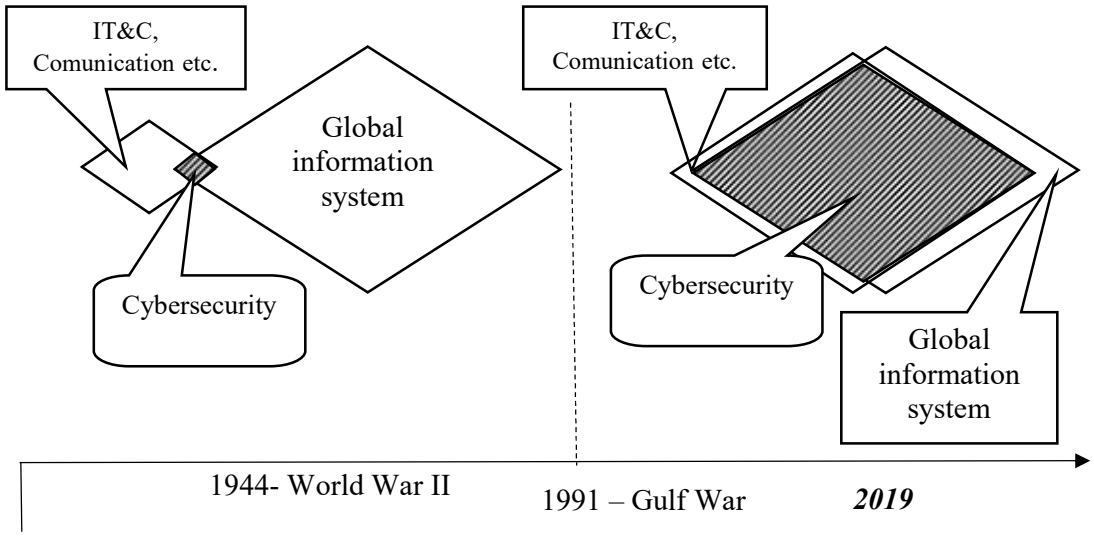

Figure 1 – The model of the evolution of cyber security compared to that of global information systems

In brief, we want to justify why we chose as temporary benchmarks the two years, 1994 - the reference year for the end of World War II and 1991 - the year of the Gulf War.

In the beginning, people provided information through human own senses. The study of phenomena or the observation of threats was done through their seven senses. To communicate with each other speech was invented. Later, to communicate at distance, they invented writing. For the fellows who would later go through that place were signs left or, later, letters would be sent through emissaries. For the achievement of an economic or military objective, the most important period was the preparation for the war. During this rather long stage, besides the military exercises, mobilization of the armed forces and preparation of the force, extensive diplomatic and information campaigns were conducted to aknowledge the adversary. Nothing was left to chance. But it all depended

on the commander and his capabilities in obtaining, understanding, knowing and performing his subordinate and enemy forces.

Also, in order to perform, the technology was used. Thus, in order to see observation towers were built, to strike targets at a distance the bow and arrow were invented, to be faster they used horses and to defend themselves they invented shield and armor. All of these technologies evolved to the level where the number of personnel engaged in a striking force became so great that the biggest problem became the timing of a carefully planned activity. Napoleon Bonaparte did not lose at the Battle of Waterloo (1815), in front of the armies led by the Duke of Wellington, because he was not able to command his troops. The vulnerability of his strategy, the strategy which was otherwise revolutionary at that time, was the excessive planning of the events and phases by moments of the warfare without taking into account the unexpected or unknown developments. Thus, without having the possibility of real-time communication and without a flexible maneuver plan, on June 18, 1815, a third of the French army, carefully positioned to prevent the Prussian reaction, marched in the wrong direction and was engaged in combat by a Prussian Army Corps at Wavre. These actions caused irrecoverable delays in the speed of the battle plan development and, consequently, the loss of war by Napoleon.

From that moment the combat technologies have developed or improved new parameters and systems. The bow and arrow were replaced with artillery and cannon balls, and then with rockets. The horses were replaced with the tanks. The armor was replaced with strong armor. The observation towers were replaced by airplanes. The communication at distance was improved by introducing telephony and, later, radio-wave communications etc. The Second World War was a glory peak for research and development of combat technologies. During this period, radar systems for the command of aircraft and fighter ships appeared, radio-navigation and communications systems were implemented etc. The information was much easier to obtain and transmit. Yet, jamming systems were also implemented for them. Speed and mobility increased to remarkable parameters, influencing the surprise actions and of the logistic support flexibility.

However, for the commands, the creation of the "unique image" of the battle space, which involves a resource of information, continued to be carried out much later than the battle space reality. The information was

obtained and transmitted in a rather long time. These influenced the decision-making process and the support of the action of those engaged in maneuvers or combat operations. Often, it came when it was too late to restore the fighting ability of those who requested it. The variables were numerous. The action may no longer take place in the place where the combat support was requested, one of the actors involved may have completely lost the fighting capability, the resources may be exhausted when they reached the ammunition or food support etc. All of these generated information. That information had to be analyzed in the decision-making loop. Military history presents numerous examples of commanders who did not take into account all the information received, implicitly, favoring the enemy in realizing surprise strikes against own forces.

The year 1991 represented a cornerstone for the evolution of combat technologies, by introducing the satellite use in military operations. Thus, during the Gulf War, the decision was made by observing, in real time, the evolution of the conflict situations. It could be achieved by overlapping aerial images with those obtained from satellites. The strategic command could be placed anywhere, not near the conflict zone. The satellites also provided communication support at all levels. Moreover, through satellite communications, online social connections could also be made, an extremely important aspect in maintaining the morale of the warriors.

At present, after the problems related to the information processing capabilities have been resolved, a new problem has emerged, related to what we know under the concept of information security. This problem is not only representative during the course of military actions but all the time, espionage activities, degradation of command and control facilities, theft of intellectual property, theft of personal information, disruption of services and the functioning of critical infrastructures etc., to produce damage in many economic, industrial etc. sectors, which can seriously affect the national security, even in peace time. It is well known that identifying and exploiting the vulnerabilities of an adversary is a major objective of command, at all levels. Moreover, the non-identification and limitation of own vulnerabilities can have extremely different implications on security, in general, and national security of activity on different levels and socio-economic fields.

Under these conditions, the training of the entire population in the "security sciences" field is no longer a vision of military specialists but a vital requirement for ensuring the existence of the state. Cyber security is a sub-domain of security science. In the same logic, cyber security training has exceeded the scope of IT&C training, with profound echoes in management and legal sciences. We are convinced that in the short run, cyber security will influence all activities carried out by humanity. Indeed, the Georgia War has shown us that hybrid conflict actions have transcended the sphere of the three physical environments and that cyber space is becoming a new battle zone in which the actors involved are both military and civilian. In this space, the classical laws of war, recognized by the Geneva Conventions, are no longer respected, anyone being able to execute cyber strikes under the protection of anonymity and distance.

We consider that the present exercises and trainings done by the armies of the NATO member states and not only, have as main purpose both the strengthening of the functional cooperation and the preparation of the population and of the national territories for the defense against the hybrid and cyber warfare.

1. Lessons learned from exercises and trainings of the cyber operations specialized structures

I chose to analyze a series of conclusions drawn from the military exercises, being known that they are characterized by a high realism of the scenarios and an impartiality of the resulting conclusions. Based on the so-called "lessons learned", the management of the military structures establish solutions for the development of the knowledge and skills of the subordinate personnel, update the procedures and correct or integrate those elements observed as generators of irregularities for future military operations. Thus, even if the scenario of a cyber space exercise is not limited to the physical environment, the lessons learned can be benchmarks for anyone concerned with raising the level of a military or civilian structure security.

In October and November 2018, NATO conducted the TRIDENT JUNCTURE exercise in Norway. It involved a number of approx. 50,000 people, military and civilians, from all categories of military forces. During the exercise, the operational capabilities to achieve the collective defense of the population and the territory of a possible NATO adversary were tested.

This exercise was considered the largest field exercise in recent history[1]. Briefly characterizing this exercise, Secretary-General Jens Stoltenberg said that it was very transparent, all members of the European Security and Cooperation Organization, including Russia and partner countries, such as Finland and Sweden, being invited to send observers. Also, an invitation for cooperation in several areas was launched, among which we mention the neutralization of hybrid threats, the neutralization of the specific threats to the cyber space and the improvement of the mobility of the military capabilities[2].

We consider that TRIDENT JUNCTURE was an important form of verification for integrating cyber space into NATO military operations. However, public reports provide little information about the importance and the role of cyber space in affecting other sectors of activity and directions that are not included in the relations specific to the military environment. Moreover, the aspect of non-involvement of other civil sectors is confirmed by the fact that NATO's main cyber defense exercise, Cyber Endeavor, was conducted at the end of November, following TRIDENT JUNCTURE and was not correlated with exercises[3] or other socio-economic fields.

Usually, the NATO exercises are carried out on many levels, from the lowest tactical level to strategic level, the final objective being the development and integration of cybernetics issues. On the background of applying the cyber defense concept in joint military operations, it is aimed at establishing a unitary and progressive approach to this type of exercises. It can be observed that such training, even if it covers the whole spectrum of cyber operations or only sequences of them, can be classified into the following categories:

1. Exercises for checking and correcting strategies and policies;
2. Exercises for verifying and optimizing operational integration functions;

[1] ***, „Trident Juncture 18", at https://www.nato.int/cps/en/natohq/news_158620.htm, visited on 21.10.2019.
[2] ***, „Pre-ministerial Press conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Defence Ministers in Brussels", at https://www.nato.int/cps/en/natohq/opinions_158684.htm, visited on 21.10.2019.
[3] NATO Communications and Information Agency, „NCI Agency Responds to Fictional Threats in Successful Cyber Exercise", press release, December 11, 2018.

3. Exercises for checking and testing technical applications and devices.

Usually, the verification of strategies and policies is taking place during the management exercises, for the training of the personnel with command attributes or in mass exercises with forces and means. For the senior level, the structure that plans and manages the exercise focuses on resolving the problems related to strategies and policies that allow the consolidation of the operational agendas. Studying the achievement of several specific objectives, without distracting the human force involved in different phases of the exercise, can be secondary elements. The general objective of these exercises is to identify the challenges, to familiarize them with the strategic and operational level concepts, as well as to inform about the doctrinal updates, policies and planning directions. The "Cyber Coalition" exercise of 2018 can be considered the equivalent of an operational-tactical cyber exercise. It apparently did not bring together non-cyber exercises. The scenario focused, among other things, on protecting electoral systems and other critical information infrastructures against cyber-attacks, while TRIDENT JUNCTURE focused on field exercises to defend the territory of NATO member states subject to conventional attacks

During the exercises it was noticed that the integration of the cyber domain in the common operational processes is a crucial issue. This conclusion resulted from the recognition of organizational changes and the way in which any organization plans and executes belligerent activities, in common with the traditional military forces. It is estimated that the next step is to integrate cyber solutions in maintaining an efficient combat rate of the command staff, from different levels.

Other aspects of cyber space operations refer to the effects-based planning process and to the authorization of the execution of cyber activities specific to the offensive and defensive maneuver. Understanding these differences is the key to cyber operations.

Operational exercises should lead to results to improve operational planning and execution, training staff for planning, executing and evaluating all the operations in cyber space.

At tactical level, the cyber action applied is usually simpler than at the operation, strategic and political level, because it is limited by the performances of the technology. They can only focus on tactics, techniques

and concrete procedures. Usually, the exercises of this area aim to achieve limited objectives within the network operations during the phases of the cyber defense actions. Integrated electronic warfare platforms or other targeting systems can be tested in this exercise. Various methods can be evaluated in decision-making processes. New warning indicators regarding cyber threats can be implemented.

Therefore, the training staff being able to plan and lead cyber operations requires a different exercises range that do not affect functions of real life operable systems and do not compromise local computer networks, in real time. Given that NATO will not develop offensive cyber operations per se (though it may integrate effects of the action of the Allied nations), analyzing the results of the exercises is the only way to study how the tasks to be resolved are set. These requirements must be determined by the effects identified in the cyber security level of the national systems, to be integrated in the planning process. [4]

We believe that the NATO approach is a good example for planning and fixing-up this level exercise that could be extended to the technical level. We are convinced that any manager who carries out activities in cyber space would be interested in training those responsible for functions related to cyber space through scenarios to which other actors react.

Controlled training environments for cyber security exercises are useful because they allow all cyber capabilities to be employed in a simulated network where real solutions can be tested. In such an environment the results can be different, from the effects of functional discomfort to the destruction of data or to the loss of entire functionality of the systems. For this reason, it should be avoided to manage the previous activities in free cyber environments.

Such training involves the existence of an opponent that can be simulated by a workstation or a game in double match. Depending on the objectives planned to be achieved, the complexity of the exercise also increases. It is worth mentioning that a training organized in a double match is the most difficult one. Usually, the red team is the one attacking the real

[4] Don Lewis, „What Is NATO Really Doing in Cyberspace?", War on the Rocks, available at https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/ visited on 21.11.2019.

cyber-networks. Attacks can be network penetration tests or engaging defensive forces in the most realistic way possible. In other words, the red team represents a number of "bad guys" who attack.

Even if this type of exercise can also be performed in real computer networks, it is recommended that sequences that require the use of computer viruses should be performed in a simulated environment like "cyber range" or "cyber gym". This reduces risks in real networks. At the same time, such an approach allows a dynamic action between defenders and attackers, even if deviations from an everyday reality of the cyber environment can be observed.

Without being an objective in itself, also the red team, through their activities, prepares and improves their attack techniques. In such a controlled environment, various types of cyber-attacks can be launched to test or verify variants of networks of both cyber and physical defense systems. Moreover, only such an approach can correctly assess the level of risk for large and complex IT networks, one of them being the NATO CSI (Communication and Information System Network).

We can say that the partnership of NATO with the Government of Estonia, from 2014, through which Estonia provided the national "cyber range" platform for establishing cooperation in the field of cyber defense and security[5] through the USA, represents a gain for everything that encompasses the contemporary cyber environment. Currently, all the major international exercises, such as Locked Shields, Crossed Swords and Cyber Coalition, as well as a series of conferences including CyCon, are held at the Tallinn Center for Excellence as NATO Cyber Range. In Estonia there are also a series of events and exercises aimed at strengthening the cyber defense position of the EU and NATO states. Of these we mention EU CYBRID. This is a cutting-edge cyber defense exercise involving EU defense ministers. [6]

[5] ***, „Agreement on defense cooperation between the government of the United States of America and the government of the Republic of Estonia", available at https://www.riigiteataja.ee/aktilisa/2160/6201/7002/Est_USA_agreement.pdf, accessed on 14.11.2019.

[6] Josh Gold, „How Estonia uses Cybersecurity to Strengthen its Position in NATO", available at https://icds.ee/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/, accessed on 14.11.2019.

It is obvious that the number and diversity of NATO exercises in cyber space will increase in the future, which indicates an increased need for internment units, educational capabilities and technological changes and, not least, mentalities. NATO could supplement existing capabilities with cyber structures available in the private environment and which mainly use cloud architectures. We estimate that the benefit of using full-service providers instead of a generic cloud service provider (such as Amazon Web Services, Google Cloud etc.) is the ease of generating network traffic and controlled cyberattacks. Moreover, these providers also provide the infrastructure that allows those enrolled in an educational program to connect and "play" on the respective platform. Adopting such a solution also allows the provision of specialized consultants, by making available the expertise of the personnel of the respective company, directly, physically or online, through courses and by indicating bibliographic sources.

2. Advantages for the national security system

In all the states of the world, training and equipping the armed forces is a responsibility of the nation-state. It has the responsibility of passing the cyber units into operational level, validation of the force being executed by certification, responsibility similar to any structure intended for NATO missions. Therefore, in accordance with the principle "prepare as you fight - fight as you prepare", the purpose of the existence of an infrastructure for education and training in the cyber field is learning and training for NATO missions, through joint exercises combined with national cyber structures that do not belong to national defense and security institutions. During these exercises, the personnel involved learn and train for various methods for further action, independently or within a specialized infrastructure, national or under NATO command.

Currently, more and more states are using own infrastructure for preparing and training their operators, military and civilians, for testing, developing, operationalizing and experimenting various cyber solutions and products. And Romania, as a NATO member state, trains its cyber operators in various exercises, on NATO cyber platforms. Moreover, NATO may choose to provide access to its cyber range to other states or partners, the major objective being to integrate cyber effects into military operations also through the full domain operationalization. For example, the United States

has experienced approaches to the development of the cyber operations planning process and to the integration of specialized personnel within the operational structures, as Cyber Liaison Officers for the Commands and staff of the operational units, military or other, for the creation of local cyber centers, which combine the work of information, management, planning and communications personnel with that IT specialized personnel. During these exercises it was noticed that one of the biggest problems does not consist in conducting operations with offensive character but in the way of applying the defensive measures, which explains why greater attention is paid to the elaboration and modernization of strategies, policies, other norms etc., for the identification of solutions and alternative technologies while establishing the procedures for evaluating the functional cooperation solutions in the Alliance.

In terms of preparing the future workforce, more and more voices are advocating the training not only of the cyber engineers and of the command and planning staff, but also of the categories of support personnel, in the field of management, legal, logistics etc., which not only understand the soft aspects of cyber space, but they will not understand how cyber operations can contribute to the overall success of the action and how other domains and disciplines can strengthen cyber security. We consider that these could be the main reasons why NATO is beginning to adapt its educational programs in such a way so as to allow a comprehensive range of cyber issues to be addressed.

The NATO Communications and Information Agency has built a new school in Portugal to support its mission and to educate staff on the operation of NATO information systems. [7] Other academic institutions, such as the NATO Defense College, the Oberammergau NATO School or the Center of Excellence for Cyber Defense Cooperation, will also implement courses in the field of cyber security organization and operations.

The requirement for qualified personnel in the field of cyber security, on the market, is increasing. The Cyber Security Certification Organization (ISC) 2, mentioned in the report of 2018 that the shortage of workforce of these professionals is increasing globally, reaching 2.15

[7] NATO, „NATO Breaks Ground on Portugal IT Academy", press release, May 23, 2017.

million positions. [8] According to the same report, the demand for cyber security personnel is expected to increase in the coming year, underlining the certainty that this will not diminish. Professionals in cyber security are predominantly technical but will undoubtedly also belong to the administrative staff, managers, lawyers etc., both military and civilian. In addition, the staff with experience in training will bring with them in addition to personal experiences and new levels of expertise for the positions they will occupy. Where there is no experience, it will have to be "imported" from another partner, until ensuring the integration of all cyber capabilities into joint operations, including the operational premises that only military or civilian infrastructure manage, from the public space or private. And this is done only through education and training.

NATO's training policy in this area is based on the efforts of its member nations to send, in specific missions, personnel by rotating it. In NATO, there are personnel who have performed long service in the field of cyber security, both military and civilian. Regardless of the level of experience gained in its missions, at NATO level it is desired to provide a specialized workforce, with a solid base of skills and knowledge. In addition to the mission, these people must be able to develop educational modules that enable the development and support of human capital.

In this regard, the US Department of Defense (DoD) has developed a framework of cyber security specialties that comprises four levels and a number of main categories of personnel such as[9]:

–*The common level of cyber security* with specialists in: Networking, Software Development, Systems Engineering, Financial and Risk Analysis, Security Intelligence;

–*Lower level of cyber security* with specialists in: Cybersecurity Specialist/Technician, Cyber Crime Analyst/Investigator, Incident Analyst/Responder, IT Auditor;

[8] (ISC)2*, „*Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)2 Cybersecurity Workforce Study 2018", October 17, 2018, p. 4, available at https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx, accessed on 19.11.2019.

[9] Cyber Seek, „Cybersecurity Career Pathway", available at https://www.cyberseek.org/pathway.html, accessed on 19.11.2019.

–*Medium level of cyber security* with specialists in: Cybersecurity Analyst, Cybersecurity Consultant, Penetration & Vulnerability Tester;

–*Advanced level of cyber security* with specialists in: Cybersecurity Manager/Administrator, Cybersecurity Engineer, Cybersecurity Architect.

We appreciate that such an approach allows, at least in the initial stages, providing essential support through the expertise of specialized structures and through consultative support for the development of personnel training programs that will be designated to participate in missions. Subsequently, during the rotation periods they could disseminate their knowledge gained and experience to other categories of personnel in the country, through various forms of education and training.

Conclusions and proposals

It is well understood that the experience gained in missions or in the systematic exercises organized by NATO will bring added value in the field of cyber security. A first step for NATO to ensure that it receives real support through the involvement of qualified personnel is to evaluate it and establish the appropriate positions and qualifications associated with its preparation for positions within the Alliance's cyber space missions. These functions may include planners, operators, cyber defenders, logisticians and specialists in areas that are not as obvious as diplomacy and strategic communication.

If we accept that cyber security is not just the IT&C attribute, we will notice that this domain is and will long be a strong link between the sectors of education, industry and the military. Generalizing the cyber defense functions scheme, very well done by Northrop Grumman Corporation in a 2013 presentation, supported by Bill Russell, under the title "Why Do COTS-Based Architectures Fail to Protect Your Enterprise", we will see that real cyber security is achieved by adopting a cumulative measures grouped by security levels and related fields as in figure 2.

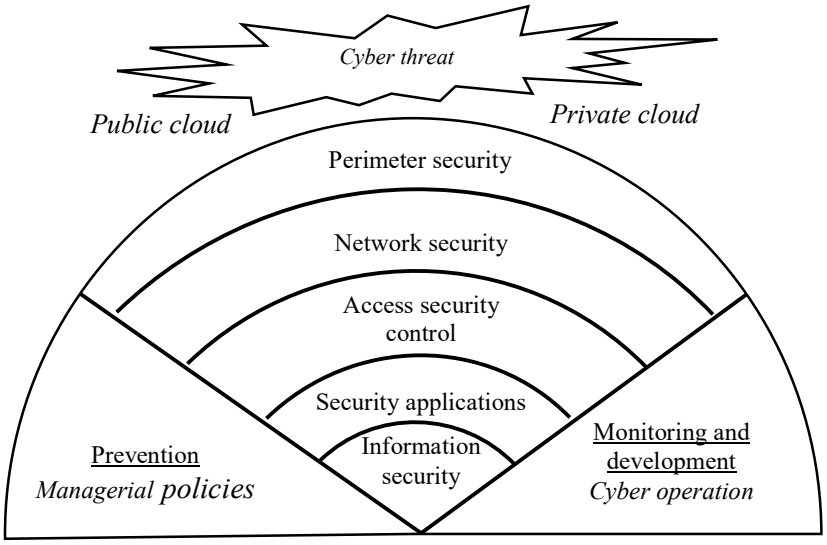

Figure 2 – The levels of the cyber defense framework of an information system

In order to achieve these ambitious goals, cyber defenders need to be trained by a militarized structure, within an educational framework provided by a high-profile industry. The exchange of information can be ensured through various products that an educational institution can provide such as: training courses, university programs, conferences, workshops, exhibitions, documentation lessons and visits etc. Each structure will play an extremely important role in this whole, by creating its own cyber defense capabilities and contributions, as far as it can, so as to ensure knowledge transfer.

It is obvious that in this paper we have highlighted only the key areas that we need to focus on in terms of the role and place of each sector in developing a skilled workforce or, at least, aware of the need to apply cyber security measures. Numerous other institutions such as hospitals, pharmacies, public administrations, social services, industrial facilities, tourism and other economic sectors etc., all because they benefit from

access to personal information, regardless whether they will target the physical or legal platforms, they need real cyber security.

Only using cyber capabilities in an integrated way will facilitate the achievement of the desired objectives. But all this cannot be achieved overnight. It takes will and time.

We consider that adopting such a strategy at the national level, in addition to initiating standards, could bring in a new way of thinking and could enhance the valuable experience of the private environment. Educational institutions, regardless of whether they conduct under-graduate or higher education programs, will play an essential role in the development and support of the workforce for the cyber security. The training by courses can cover relevant topics, on a wide range, from strategies and policies to strictly technical fields.

Some of the topics we suggest to include in the initial training and orientation courses may include:

• Organizational structures and organizations, at national level and of EU and NATO institutions, which relate to and have missions in the field of cyber security.

• Aspects regarding the planning and management of cyber operations during crisis management.

• Technical topics for those less familiar with the various levels of cyber defense, from physical infrastructure to virtual domain or to "cyber identity".

• Knowledge of some aspects regarding the capabilities of the cyber space, with emphasis on the defensive ones.

• Aspects of the legal framework and policies applicable to cyber conflict etc.

Finally, at national level, a curriculum should be developed in which graduates of a form of education would know how to apply for a job in this field, as well as the policies for recruiting and retaining qualified personnel for a job/ certain position, in order to attract talented people and/or people with high level of expertise. These initiatives could include financial incentives, offers of collaboration with private sector, scholarships and funding for career and personal development, and last but not least, stronger links with academic institutions across the country. It must be understood that education costs and without both material and knowledge investments,

only a continuous weakening of cyber security levels will be achieved that will certainly affect national security.

Without pretending to have exhausted the topic, we want to draw attention to the fact that the lack of education in cyber security in the future will block any chance of finding a job and the people under a cyber-attack strike will be the perfect victims unable to understand what hit them.

BIBLIOGRAPHY

GOLD J., „How Estonia uses Cybersecurity to Strengthen its Position in NATO", at https://icds.ee/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/, visited on 14.11.2019

LEWIS D., „What Is NATO Really Doing in Cyberspace?", War on the Rocks, at https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/, visited on 21.11.2019

RUSSELL B., „Information-Driven Cybersecurity, Why Do COTS-Based Architectures Fail to Protect Your Enterprise", 4 June 2013, (slide),https://its.ny.gov/sites/default/files/documents/presentations/Bill-Russell.pdf, visited on 14.11.2019

***(ISC)2, „Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: (ISC)2 Cybersecurity Workforce Study 2018", October 17, 2018, p. 4, at https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx visited on 19.11.2019

***„Agreement on defense cooperation between the government of the United States of America and the government of the Republic of Estonia", at https://www.riigiteataja.ee/aktilisa/2160/6201/7002/Est_USA_agreement.pdf, visited on 14.11.2019

***„Pre-ministerial Press conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Defence

Ministers in Brussels", at https://www.nato.int/cps/en/natohq/opinions_158684.htm, visited on 21.10.2019.

***TridentJuncture18",https://www.nato.int/cps/en/natohq/news_158620.htm, visited on 21.10.2019

***Cyber Seek, „Cybersecurity Career Pathway", at https://www.cyberseek.org/pathway.html, visited on 19.11.2019.

**NATO Communications and Information Agency, „NCI Agency Responds to Fictional Threats in Successful Cyber Exercise", press release, December 11, 2018

***NATO, „NATO Breaks Ground on Portugal IT Academy", press release, May 23, 2017.