THE GROWING NEED FOR TECHNICAL SPECIALIZATION IN CYBER DEFENCE OF FUTURE OFFICERS: DEVELOPMENT AND FUTURE TRENDS

Mihaela Anamaria BOSTAN-POP*, Romana OANCEA**

*Training School for Communications, Information Technology
and Cyber Defence, Sibiu, Romania

**“Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania
mbostanpop@gmail.com, oancea.romana@gmail.com

Abstract: *Considering that the level of cyber threats is constantly increasing, a necessary demand emerges from organizations and corporations worldwide to protect their networks against possible cyber-attacks. In the future all malicious actions that occur in cyberspace will continue to alter the way we approach the security of an entire network. The article presents the most stringent need concerning the technical specialization of future officers, highlighting the knowledge entailed in order to better understand the complexity of a mission that takes place in virtual space. Undoubtedly, modern battlefield incorporates a virtual component where nearly all weapons systems rely upon information and communication technologies in order to connect and achieve operational level. The demand for future cyber defence specialists in the military domain reached a high level all over the world, and there will be a challenging process to be able to create a highly skilled workforce to fight against a large scale of malicious activities that have impact upon the national security system.*

Keywords: cyber-defence, military education, technical specialization, cyber workforce

1. Introduction

In a unique and all-encompassing environment such as cyberspace, there are numerous vulnerabilities, threats and risks regarding the security of the embodied networks. All social, medical, economical, or other domains that are connected to the virtual space through cyber infrastructures are currently investing money and knowledge in order to achieve cyber resiliency. In comparison with the human immune system and its important role to protect our body against diseases, all computer networks connected via cyberspace need protection against numerous existing malicious software, a

virus for example. In pursuance of a secure cyberspace, from the cyber resilience perspective a set of goals need to be appointed. The main goals that cyber resilience stands upon are the ability to anticipate, withstand, recover and adapt [1] to the constant alterations and possible attacks that may take place in cyberspace. In the light of this perspective, all network users must actively participate to achieve the goals mentioned earlier.

Over the last several years a high demand for experts in cyber domain has been identified. The significant knowledge gap that appeared is starting to reduce due to the various types of education and training

programs developed by states worldwide in this domain. On the other hand, the need for technical specialists is on a growing path as cyber-crime incidents multiply and become more sophisticated. In the light of the current situation, people are considered to be the most vulnerable element in cybersecurity. Users vulnerability is exceedingly utilized by hackers for launching cyber-attacks [2]. Regarding this issue, an angle of approach could be facilitating a proper training or retraining for finding answers to difficult situations for all users, not just for one person or a small team of experts. Unquestionably, the difference between technical specialists and other common users will be the advanced set of skills obtained after completing a series of technical specialization courses. A general solution has been discovered and is related to an ongoing training and specialization courses addressed to future cyber-workforce personnel.

Cyber defence domain is characterized by a certain degree of technical concepts and terms that in the vast majority of cases are challenging to comprehend. It is therefore not surprising that technical specialization knowledge is required in order to become an expert in this field. The process of attaining a high level of technical competencies for subsequent generations of officers will be tough but not impossible in the future.

2. Technical specialization in cyber defence domain

Defending a computer-generated environment is challenging taking into account that cyberspace constantly changes, improves and therefore possible malicious actions could emerge from all over the world, at any point in time. Even though cyberspace consists mostly of physical infrastructures, computers systems and networks not owned by the military, a small proportion of them have an exclusive use in the military domain. Therefore, future cyber-workforce must be trained

appropriately in order to reach a high level of technical specialization in cyber defence domain.

In Romania's Cybersecurity Strategy official document cyber defence is explained as: actions designed for protection, monitoring, analysing, detection, counterattacking and responding promptly against threats towards national defence cyber infrastructures [3]. Cyber defence actions are also referring to a particular technical analysis in order to determine directions and well as locations that could be targeted by attackers [4].

Since July 2016, a collaboration between North Atlantic Treaty Organization and European Union regarding cyber defence domain enhanced a set of priorities for all member states. In order to be able to generate a clear image of what cyber defence means and how it could be implemented throughout the two organizations, cyber defence policies frameworks have been formulated. Referring to EU's Cyber Defence Policy Framework several priorities such as: developing cyber defence capabilities, training and exercises, research and technology and civil-military collaboration [5] have been established. Similar perspectives are stated in NATO Policy on Cyber Defence, regarding international collaboration, sharing information and good practices in order to withstand and recover from potential cyber-attacks. Also, cyberspace is now considered an operational domain, providing the opportunity for NATO member states to concentrate upon their military training and planning [6]. Moreover, Military Computer Emergency Response Teams (milCERT's) are an important component in the military organizations, constituted from military and civilian cyber experts. Their mission is to prevent and respond firmly when significant Information and Communication Technologies infrastructures are at risk and could compromise the cybersecurity or a military operation.

From a military point of view protecting the national cyber infrastructures and all of the information and data stored inside represents a critical mission.

Given the above consideration, a stringent need concerning the technical specialization of future officers emerges. In order to better understand the complexity of a mission developed in cyberspace military students must learn and understand the procedures and methods in order to defend a computer network. Cyberspace is now incorporated in almost all segments of our life, even in the modern battlefield where the attacks generate dual effects – firstly in virtual space compromising data, and secondly at a physical level. The evolution of Information and Communication Technologies generated a major progress in the way modern weapons systems are controlled and operated.

Obtaining a technical specialization in cyber defence, our future officers will have the abilities to prevent and protect national cyber infrastructures against the actions of malicious cyber entities. From our standpoint, the steps required in order to become a military specialist in cyber defence entails activities such as:

- Installing and performing maintenance upon cyber infrastructures in a way that will discourage the adversary;
- Being able to analyze, detect and fix or patch network vulnerabilities;
- Be capable to find solutions in the moment a day-zero attack occurs;
- Restore the system to full capacity after an effective attack.

All of the above are general measures that will be applied in courses and laboratory activities. Throughout the educational process, future cyber defence officers will develop their abilities to detect and subsequently undertake an immediate and unyielding response to a cyber incident. With a focus upon minimizing the results of the attacks, cyber defence oriented exercises will facilitate learning by enable

the participants to detect and isolate addressing threats at the right moment.

Future officers are the most important resource and if properly trained they will meet tomorrow's expectations regarding the considerable demand of technical specialists in the field.

3. Development and future trends

Nowadays the cyber defence skilled personnel shortage triggers a sensitive issue among organizations and corporations worldwide. Their desire is to be able to ensure the security of their computer networks and generate a continuously safe environment despite the hostile activities. Cyberspace has become a conflict ground, characterized by a state of everlasting tension. There is a strong linkage between military and civilian domain since a large number of cyber infrastructures are shared. Therefore, international organizations alongside NATO and EU encourages civil-military collaboration within cyber defence domain. Military organizations benefit from a large and well-designed civil cyber infrastructure through which they are able to digitalize a part of their services on one hand and on the other hand to reduce the expenses of having their own large-scale infrastructure. Taking into consideration this fact, it becomes apparent that military cyber capabilities are vulnerable in front of similar cyber threats as civilian ones are. An important part of the development regarding technical specialization of future officers in cyber defence field is the ability of sharing information and solutions at national and international level with all the entities that are involved. Providing efficient cyber security requires both military and civilian effort in combating the spread of cyber criminality. Regarding military operations new opportunities emerge from using cyber defence capabilities. Cyber defence experts will be able to deliver support for the armed forces conducting the missions, generating a stronger, more capable strike force. In the

future malicious actors will benefit from the improvement of the ICT sector and discover new ways to attack. A long-term solution apparently will be using artificial intelligence (AI) technology. Regardless whether the number of experts in the cyber defence domain will exponentially grow, the difficulty in managing extremely numerous attacks without any help is impossible. It may be possible that artificial intelligent agents will maintain our networks safe and secure. In anticipation of using AI technologies for defending cyberspace, numerous technical and policy related questions are now waiting to be answered. Despite the fact that AI tools might solve a significant number from the current problems concerning cyber defence, trained cyber workforce are an important resource for the moment.

4. Conclusions

The evolution of technology is modelling our future and the way we live. In order to adapt to all the challenges that emerge in virtual space, a solution for the future cyber defence officers is clearly a long-term learning and re-training approach. Technical specialization in cyber defence

domain has been identified as a growing need not only for civilians, but for military personnel to. A cooperation between civilian experts and skilled military specialists is mandatory. Exchanging information and good practices between organizations will add value and bring victory in a never-ending war between cyber defenders and malicious cyber actors. The more perspective we have upon the future solutions for generating a safer cyberspace, the fewer blind spots there are. Implications of using artificial intelligence and automatic self-learning tools are major. We need to approach these paradigms with caution and find the best solutions we can for the moment.

This paper therefore surmises that there is a stringent necessity for future cyber defence specialist in the military organizations and that there are solutions for creating a highly skilled cyber workforce. Without the implication of armed forces in the fight against the growing number of malicious activities against national cyber infrastructure this battle would not be an easy one to win.

References

- [1] Ross, R. et al., *NIST Special Publication 800-160, Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, Vol. 2, p. 9, 2019.
- [2] Oancea, R., Bârsan, G., Giurgiu, L., *Approach on Increasing User Security Awareness*, International Conference Knowledge Based Organization, p. 46, Sibiu, Romania, 2019.
- [3] *Cyber security strategy of Romania*, <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>
- [4] Galinec, Darko & Možnik, Darko & Guberina, Boris. *Cybersecurity and cyber defence: national level strategic approach*. *Automatika*. 58. 273-286. 10.1080/00051144.2017.1407022, 2017.
- [5] *EU CYBER DEFENCE POLICY FRAMEWORK*, Nov. 2018, <https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf>
- [6] *NATO Cyber Defence*, July 2016, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf