THE ROLE OF CYBERSECURITY IN THE ROMANIAN DEFENCE EDUCATIONAL SYSTEM

Dumitru Daniel[1] and Ion Tiberiu[2]
[1) 2)] *Carol I National Defence University, Bucharest Romania*
E-mail: dumitru.daniel@unap.ro; E-mail: ion.tiberiu@unap.ro

Abstract
In the context of modern technologies, the dynamic expansion of cyberspace resulted in a numerical and complexity increase of cyber threats, with a direct impact on the national security of multiple countries. Romania, as a member of the North Atlantic Treaty Organization and the European Union, has become more aware of this problem, in the last decade, implementing a set of national strategies regarding cyber defence.
As a part of the national defence system, cybersecurity specialized training is experiencing both a knowledge and practical experience shortage. Therefore, using higher-education cybersecurity programmes as an interface for the development of the national defence system, represents a sustainable solution.
Thus, the present paper aims to highlight the importance of cybersecurity educational programmes in training future specialists. The starting point is a literature review regarding cybersecurity and Romania's perception on this subject, that contributes to identifying and understanding the need of a cybersecurity educational model for the Romanian defence system. By interrelating all universities and educational centres that activate in the defence system, a matrix has been outlined on how the future workforce in the defence system can achieve specialization by following certain institutional paths.

Keywords
cybersecurity, defence educational system, cybersecurity curricula, cybersecurity educational model

JEL Classification
I23, I28, O32, O38

Introduction

Nowadays, modern society can be characterized by an extensive process of international reorganizing, with direct implications for Romania, as a subject of international law. After more than 10 years since Romania became a member of the North Atlantic Treaty Organization (NATO) and the European Union (EU), multiple economic, social and political changes had been necessary for the transition to a democratic society and a market economy and part of these changes involved the national security domain. In fact, the concept of security is the basis of the North Atlantic Treaty Organization's fundamental principle, which is a strong commitment to mutual cooperation between member countries, focusing on indivisibility as a solution for long-term security.

On the other hand, the continuous improvement in the evolution of computerized systems have determine a new dimension of the modern society, known as cyberspace, that was formed by connecting multiple networks. Beside the benefits and the added-value that cyberspace brings to multiple sectors of the global economy and the environment itself, it can also generate unknown risks for both the public and private sector of a country.
In this context, the notion of cybersecurity has begun to emerge, as many international organizations are taking act of the potential threats, by designing cybersecurity strategies and other combat instruments against cyberthreats. Moreover, cybersecurity is being promoted as a discipline and a research domain upon computer science, being built upon elements from multiple domains like IT, communication systems, psychology, and many other related disciplines. The skills associated with the specialists performing in this domain tend to be more complex than those performing regular IT operations. Adding complexity to the assessment of a certain skill requirement is the risk associated with the security operations, therefore security specialists tend to have greater levels of access to critical data.
Previous studies (Bicak et al, 2015; Cabaj et al 2018) have identified a trending pattern regarding the need of cybersecurity specialists: there is a growing need that cannot be sustain by the current educational resources. Thus, the need of professionals and the primary activity of the institutions with responsibilities in cyber defence must be taken into account when implementing new educational programs.
For the current study, Romania was chosen as a geographic coordinate due to the small number of higher-educational programmes specialized in cybersecurity. Therefore, the current paper analyses a method of innovating a yet unaddressed issue regarding education programmes in the cybersecurity domain, as they must adapt to international guidelines.
A basis for the present study was the educational model in the defence system of the United States of America, where governmental agencies with attributions in intelligence and IT security, like Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Department of Homeland Security (DHS), Defence Intelligence Agency (DIA), National Geospatial Intelligence Agency (NGIA), have own specialized universities, training and research centres, or have partnerships with a number of higher education institutions to train cybersecurity experts.
The research methodology starts with a literature review in order to identify and analyse a set of immediate-impact strategies that Romania has on cybersecurity. Afterwards, current data is collected in order to identify the set of items that will be treated as variables for our model. Thus, the characteristics of the model will be defined so that it would be able to optimize the Romanian defence system and provide a better understanding of cybersecurity educational programs in higher-education.

1. Romania's perception on cybersecurity. Literature review

In the past decades, the global socio-political context in accordance with the technological evolution have contributed to the creation of a new dimension, that isn't limited by any boundary, a new dimension known as cyberspace. Nowadays more and more conflicts are projected in cyberspace, where the amount of information and the data complexity are valuable resources. Cyberspace, as a word-wide notional trend, is addressed throughout multiple geopolitical discussions and forums, specialists considering that wars of the future will be represented by information wars and that cyberspace will become the next theatre of warfare (Carr, *2009;* Roldán et al, 2017; Cabaj et al, 2018).
According to the North Atlantic Treaty Organization, the first major cyberattacks took place between 2006 and 2008 when NASA and Estonia were the main targets. Thus, the need for cybersecurity appeared simultaneous with the development of the digital era, nowadays governments raising an increasing concern regarding cyber warfares and the public security itself, among international bodies that activate in this sector.

The year of 2018 marked the implementation of new strategies throughout many NATO member states as cyber-attacks usage has grown all over the world, including Russia's war with Georgia in 2008, and with Ukraine in 2015. Modern cyberthreats aim three major pillars of the world's economy: financial, infrastructure, and governmental, which are being constantly targeted with major repercussions worldwide. For example, financial attacks could interrupt the world's major markets by taking down electronically-controlled commodity exchanges, or by shutting down web-based operations of major banks or retailers (Bimal and Apeksha, 2013). A greater need of cyber technology is needed to win tomorrow's fight and, in this context, education will play a significant part by preparing competent and qualified cyber professionals.

In general, cyberspace is defined by two main characteristics: actions can be taken instantaneously and anonymously. As cyberspace extended, many challenges were addressed in order to ensure integrity of national security systems in different countries around the globe. Therefore, developing and implementing multiple well-structured security policies became mandatory and materialized as common objectives for international bodies activating in this field, one of the most important being the North Atlantic Treaty Organization.

Given Romania's NATO and EU membership, cybersecurity has become a topic of common interest over the past decade, generating a series of responsibilities for Romania, including the implementation of a National Cybersecurity Strategy. According to this strategy, cybersecurity is the state of normality resulting from the application of a set of proactive and reactive measures that ensures the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic form, of public and private resources and services in the cyberspace (Government decision no. 271/2013).

Among policy makers in Romania, there is an increasing awareness that persistent efforts are needed to better protect the state's interests in cyberspace against a wide range of dangerous threats. The intelligence, counterintelligence and security dimension of the Romanian state is to ensure mechanisms to prevent and counteract cyber-attacks targeting informational infrastructures of strategic interest, associated with promotion of national interests in the field of cybersecurity (Romania National Defence Strategy 2015-2019).

Romania's cybersecurity strategy provides a notional and organizational framework, offering also an action plan in the field of cyber defence, which responds to the current global needs of cyberspace security, while implementing the conceptual and legislative framework adopted within the rest of NATO and EU member states. The primary goal of this strategy is to create, besides other specialized bodies, an integrated national system - National Cybersecurity System, with a role in monitoring a coherent implementation of all prevention and response measures to cyber-attacks at national level and promoting inter-institutional cooperation. The task of coordinating the National Cybersecurity System falls under the Cyber Security Operational Council responsibility, which is composed of representatives from various institutions with responsibilities and capabilities in the cybersecurity area, such as: the Ministry of National Defence, the Ministry of Internal Affairs, the Ministry of Foreign Affairs, the Ministry of Communications and Information Society, the Romanian Intelligence Service, the Special Telecommunications Service, the Foreign Intelligence Service, the Protection and Guard Service, the National Registry Office for Classified Information and the Supreme Council of National Defence. As a main responsibility, the National Cybersecurity System has implemented a series of preventive and management procedures regarding cyber-attacks identified in the national cyberspace borders. The National Cybersecurity System's operational plan is described in the figure no 1.

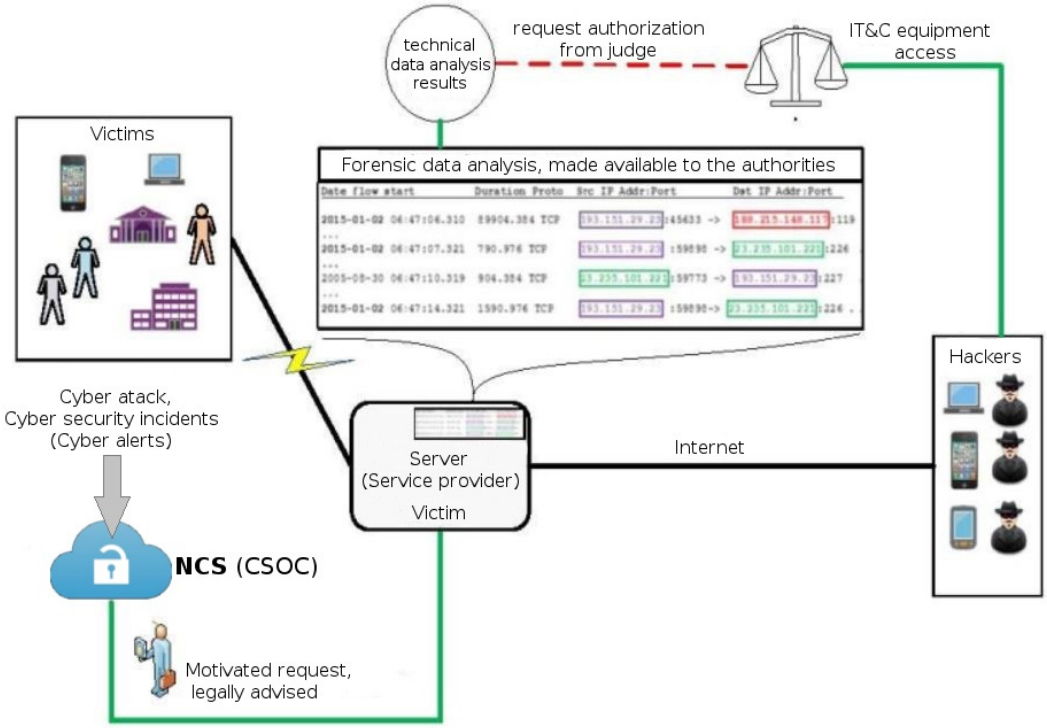

Fig. no. 1 NCS procedure - Investigating cyber attacks identified witin Romanian cyberspace

Source: Ministry of Communications and Information Society – Cybersecurity – Network and Information Systems Security

One of the many directives proposed in Romania's cybersecurity strategy focuses on the effort of promoting and consolidating a security culture in the cyber field, as a development resource for educational programs. In this sense, there are three main developing directions (The Cybersecurity Strategy of Romania):

- within the compulsory education cycles, implementing a curricula concerning the safe use of the internet and computing equipment;
- performing appropriate professional training for people working in cybersecurity;
- a widespread promotion of professional certifications in this field should be improved.

The defence and military sector is one of the main beneficiaries of cyberspace technology. Therefore, implementing a military global command and control instrument for operations and forces, is necessity for modern armies, in the operating context of a globally distributed logistics system. Intelligence organizations, commandments and war fighters alike benefit from the instant and constant flow of information. One of the main national security goals of the Defence White Paper, adopted by the Romanian Government, based on the National Defence Strategy, is to improve the capabilities of the Romanian army cybersecurity and to integrate them within the National Cyber Defence System.

Thus, there is a major need that Romanian educational institutions must cover, by embracing new research and learning fields such as cybersecurity, especially for the defence educational institutions. This will set the basis for a modern educational system dedicated to train cyber defence specialists, in order to be prepared for future security challenges and provide technical knowledge, with direct implications on the national security strategy.

2. The need of a Cybersecurity educational model for the Romanian defence system

Worldwide, more and more universities have introduced a series of educational programs with a designation including the phrase "Cybersecurity" in their curricula. Most of these universities are located in the United States, Great Britain, Australia, New Zealand, France, the Czech Republic, Germany, Netherlands, Israel and Spain. For Europe, the European Union Agency for Network and Information Security (ENISA) has contributed to the implementation of an interactive database, which includes a list of available courses and certifications in the field of network and IT security.

According to ENISA, there are only four higher-education accredited programs in Romania, in the field of cybersecurity, in three different universities, each of the program having a different approach on cybersecurity (Table no 1).

Table no. 1 - Higher-education courses on cybersecurity available in Romania

	University	Course level	Course title and type	Focus areas
1.	Military Technical Academy, Bucharest	Master	Information Security (offline)	cryptographic mechanisms, services and protocols, PKI infrastructures and bridge technologies, security of network protocols, E-mail and document security, information security developing, deploying and auditing, Cyber defence.
2.	Alexandru Ioan Cuza University Iasi	Bachelor	Information Systems Protection and Security (offline)	threat analysis, information classification, access control, security policies, cryptography, internet security
3.	Bucharest University of Economic Studies	Master	IT Security - Cyber Security (offline)	secure applications development, applied computational cryptography, smart cards, embedded secure element and TEE, audit - risk management and QA/SQE
4.	Bucharest University of Economic Studies	Master	IT Security - Cyber Security (offline)	secure application development, thread analysis, ethical hacking, audit - risk management and QA/SQE

Source: ENISA – Education Map
https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities

As it can be observed in Table no. 1, only one of the four programs is being hosted by a higher educational institution belonging to the Ministry of National Defence, more exactly the Military Technical Academy from Bucharest. Comparing Romania's actual situation with other EU and NATO countries, where higher education promotes and facilitates access to a larger number of cybersecurity courses, within multiple universities, we can identify an emerging need, with possible repercussions on national security.

Taking Germany as an example, there are 148 German universities with available courses and certification programs linked to IT security. France has a cybersecurity curricula implemented in 31 universities, while Italy has 15 institutions that provide cybersecurity specialization programs and the number is far greater if we compare Romania to regions outside Europe, like the United States of America.

On the other hand, a larger number of universities with accredited programs and courses in network and IT security does not necessary guarantee a long-term improvement in national cybersecurity defence. Different studies highlight that the existing cybersecurity workforce is not sufficient for satisfying the increasing demand for qualified cybersecurity professionals (both in public and private sector), and the shortfall will increase by the next decade (Bicak et al, 2015; Cabaj et al 2018).

Given the broad character of cybersecurity as a science domain, Romania needs to optimize its military defence educational system, to be more specialized when talking about cybersecurity, but in the meantime to be more extended, in other words to expand cybersecurity specialized educational programs to all universities and education centres that act in the military or national security field (Figure no 2).

In Romania, militarized institutions with major responsibilities in preventing, acting and supervising cybersecurity threats, like the Ministry of National Defence, the Ministry of Internal Affairs, the Romanian Intelligence Service, the Special Telecommunications Service, the Foreign Intelligence Service and the Protection and Guard Service should benefit from specialized personnel educated and trained in militarized universities. Specializations in cybersecurity or IT security should exist in all militarized universities and not only as master courses or postgraduate course, but also as bachelor courses. Also, when integrating cybersecurity in the defence education curricula, the model should consider the field of activity of each institution, for a more efficient division and allocation of the subsectors linked to cybersecurity, as a complex domain.

Considering the comprehensive national and international activities in which the national defence structures are involved, there is a need of cybersecurity specialists, trained in multiple interrelate domains. Cybersecurity specialists work with IT and communication systems, which are different, depending on their field of activity. Therefore, future specialists need to be trained efficiently, but also differently in order to be able to act and prevent cyber threats in the specific subsector where they will activate.

In Romania, land forces, air forces, naval forces and intelligence are examples of subsectors within the defence system, that needs to be treated self-dependent when it comes to cybersecurity training, thus a more optimized prevention mechanism its achieved.

As a practical approach of our model, the Ministry of National Defence IT specialists should graduate the first cycle of higher education (bachelor degree) from the Military Technical Academy from Bucharest and continue their studies (complementary courses, master or doctoral cycles) in cybersecurity within universities that promote specialized programs, that focus on a specific domain of interest.

Another pertinent example can be the case of an engineer in computer science, graduated from the Military Technical Academy from Bucharest and working in the air force subsector, should have the possibility to continue to study cybersecurity at the Air Force Academy, where educational programs are built on an air force experience basis and also offer the possibility of training on specialized IT equipment, software and hardware specific for this subsector. Thus, both knowledge and practical experience are achieved.

Therefore, cybersecurity educational programs should represent a valuable resource for the defence system and its educational centres and universities, while facing present security causes, preparing for the future cybersecurity challenges and building a foundation of technical knowledge for future security professionals.

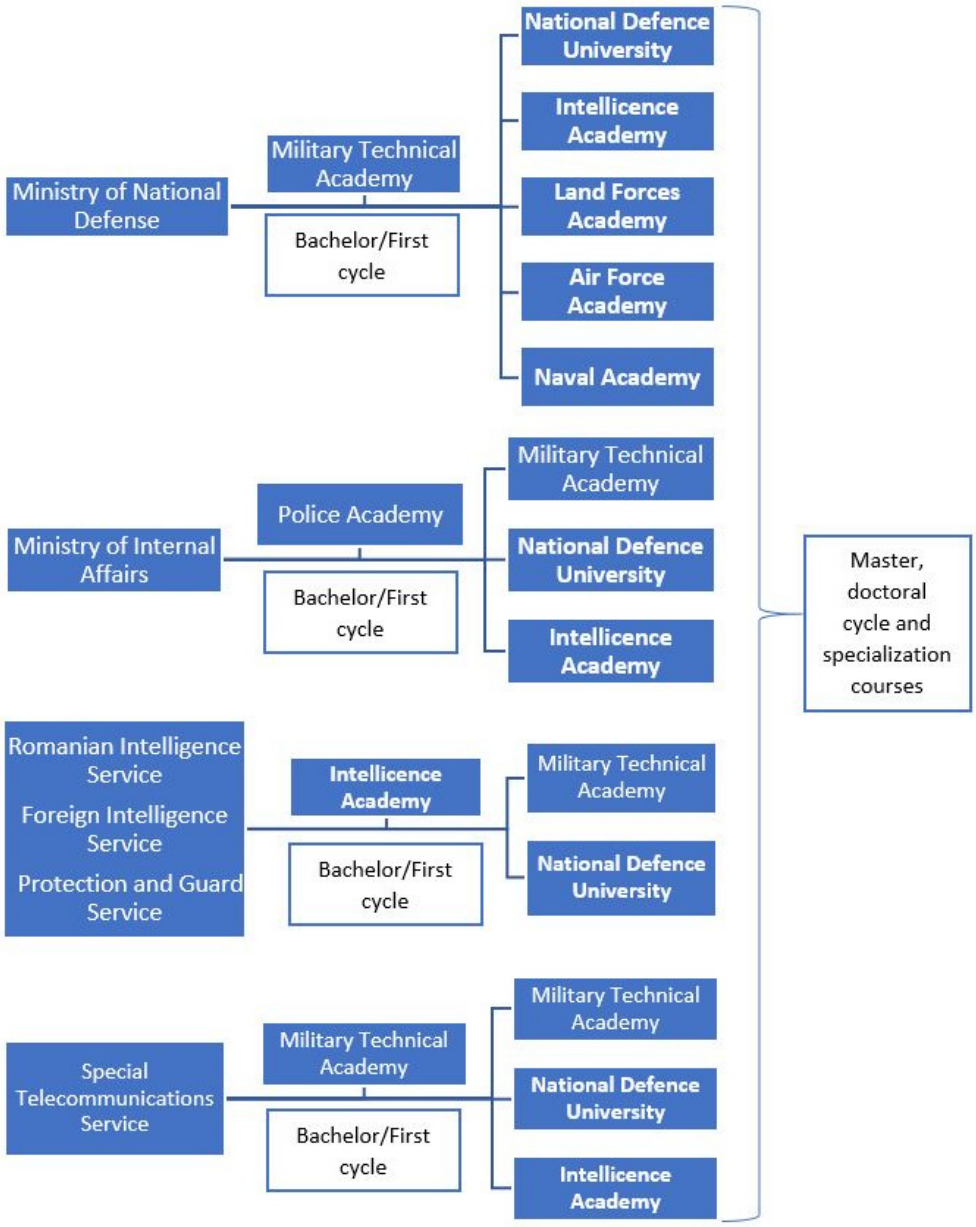

Fig. no. 2 Cybersecurity educational model for the Romanian defence system

Conclusions

Cybersecurity represents a dynamic modern discipline, that is closely linked with the evolution of the IT sector, embracing both benefits and threats resulted from the emergence of cyberspace. While the number and complexity of cyberattacks increase, the need for cybersecurity specialists is expected to grow exponentially, in the next years. Specialists consider that the demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million (Cabaj et al, 2018).

In this context, a national security threat is identified and addressed by multiple countries and global organizations within inter-governmental meetings and congresses. Education in specialized institutions should play a strategic role in preparing this workforce and the need for cybersecurity specialties is one such strategy (Bicak et al, 2015).

Romania's situation was carefully analysed throughout the evolution of cybersecurity discipline in the defence educational system. The results highlight an insufficient coverage of this subject in the existing curricula of various universities. Thus, a set of recommendations were expressed and a cybersecurity educational model was outlined, regarding the need for specialization of higher-education programs, on existing subsectors of the Romanian defence system, in order for future specialists to achieve both knowledge and practical experience.

References

Bicak, A., Liu, M. and Murphy, D., 2015. Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. *Information Systems Education Journal*, 13 (3), pp. 99 – 110.

Bimal, K. and Apeksha, P., 2013. Modelling and Simulation: Cyber War. *Procedia Technology,* 10, pp. 987 – 997.

Cabaj, K., Domingos, D., Kotulski, Z., Respicio, A., 2018. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security,* 75, pp. 24 – 35.

Carr, J., 2009. *Inside Cyber Warfare.* Sebastopol: O'Reilly Media Inc.

European Union Agency for Network and Information Security, 2018. *Education Map.* [online] Available at: <https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities> [Accessed 11 March 2018].

Ministry of Communications and Information Society, 2015. Cybersecurity – Network and Information Systems Security [online] Available at: <https://www.comunicatii.gov.ro/wp-content/uploads/2016/02/CyberSec_nov2015.pdf> [Accessed 15 March 2018].

Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadao, C., Yevseyeva, I. and Basto-Fernandes, V., 2017. A Comparison of Cybersecurity Risk Analysis Tools. *Procedia Computer Science*, 121, pp. 568–575.

The Presidential Administration of Romania, 2015. *National Defence Strategy 2015 – 2019*. [online] Available at: <http://www.presidency.ro/files/userfiles/National_Defense_ Strategy_2015_-_2019.pdf> [Accessed 10 March 2018].