AiMT

Advances in Military Technology
Vol. 14, No. 2 (**2019**), pp. 291-305
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.01296

Human Factors Approach to Cybersecurity Teamwork – The Military Perspective

C. Krasznay[1*] and B.P. Hámornik[2]

[1] *Institute of E-Government, National University of Public Service, Hungary*
[2] *Budapest University of Technology and Economics, Hungary*

The manuscript was received on 21 February 2019 and was accepted
after revision for publication on 7 November 2019.

Abstract:

Successful national cyber defence requires talented experts who can work together in teams. In military organizations, there has been a long history of methods defining how talents and teams can be developed. Drills and practices can serve as a unique opportunity for setting up successful groups to protect military IT systems even in the most hostile environment, however the cyberspace might be different from the physical space from the human perspective. In this paper, we introduce some ways of how cybersecurity incidents are managed in the military environment; in addition, we describe the main requirements towards humans in milCERTs and how these requirements differentiate from civilian CERTs. Further on, we highlight the institutional background of Hungary's cybersecurity training, specifically underlining the role of National University of Public Service in it, which is responsible for the education of all public servants, including cadets. The paper also focuses on the major challenges and some suggestions from Academia how to respond to them by building successful teams for the protection of national cyberspace.

Keywords:

capacity building, CERT, CSIRT, cyber command, cybersecurity, cyber training, incident management

1. Introduction

Cybersecurity is a major national security issue for all modern countries. Hungary is also struggling with this problem. Criminal activities in cyberspace have reached the point where national interests need to be represented in cybersecurity-related discussions both within the European Union (EU) and NATO. Governmental and military IT systems should be protected from criminals, foreign intelligence services and armed forces in cyberspace, just to name a few challenges. These elements require a new approach to cybersecurity especially in national security.

[*] *Corresponding author: Institute of E-Government, Faculty of Science of Public Governance and Administration, National University of Public Service, H-1083 Üllői út 82., Budapest, Hungary. Phone: +36 1 432 9000/20150, E-mail: krasznay.csaba@uni-nke.hu*

In nationwide cybersecurity, the first milestone used to be the establishment of a national Computer Emergency Response Team (CERT) which is usually followed by some sector and organization-specific Computer Security Incident Response Teams (CSIRT) or Computer Incident Response Capability (CIRC). On the highest maturity level, these CSIRTs are evolving into Security Operations Centres (SOC) or Fusion Centres. In this paper, we do not distinguish between these forms of cyber defence teams, however their capabilities might be different. Besides the sufficient technological background, the fundamental cornerstone of success in all cases is the well-trained human who can work together with his or her colleagues in teams.

In accordance with NATO's capacity-building initiatives, virtually all member states have set up their military CERTs (milCERT) and are working on the enhancement of these groups to the highest possible capability level. Therefore, national defence forces also need many qualified officers who can work together in often boring – yet sometimes quite challenging – environments. As the main source of young officers who are willing to work in cybersecurity and militaryCERT is usually the national defence university, such individual and teamwork skills can be successfully improved there. Moreover, as they will not work alone in the national cyber defence, their inter-organizational cooperation skills should also be improved to facilitate incident information exchange. Our motivation in this paper is to highlight the issue dealing with why and how milCERTs are different from civilian CERTs, why the military environment needs specially trained security analysts from the human perspective and what kind of special education is required for those who are planning to serve as a cyber warrior.

In the early 2011, the Hungarian Parliament approved a resolution to establish a new university for the different professions of state administration. As a result, the National University of Public Service (NUPS) was established, and it started to work in the beginning of 2012. The University has three predecessors – the Zrínyi Miklós National Defence University, the Police College, and the Faculty of Public Administration of Corvinus University of Budapest. Moreover, in the past six years the University has enlarged by adding two new university faculties: the Faculty of International and European Studies and the Faculty of Water Sciences.

As part of the Hungarian higher education system, the main objective of the National University of Public Service is threefold. Firstly, to train professionals carrying out administrative, defence and law enforcement activities; secondly to provide new officers and public servants for the Hungarian public administration, defence and law enforcement agencies; and thirdly to create an opportunity for interoperability among numerous public service career pathways [1].

As all faculties and institutes of the University are involved in training and education of cybersecurity and cyber defence, there is a great opportunity to support the national defence forces and to provide highly qualified military officers with a broad view on cybersecurity, who are able to solve cyber incidents both inside the military IT environment and together with other state actors in the national cyberspace. The NUPS' Cybersecurity Academy was established at the beginning of 2017 to support all educational activities and this Academy works together with the University's Cybersecurity Research Center, also established in 2017. Together they provide the background of the above-mentioned capacity-building efforts from the academic side.

2. Security Incident Management in Military IT Systems

In the case of NATO member states, military doctrines and resulted investments should be in line with the Alliance's strategic goals. As cybersecurity is one of NATO's major focal points with cyberspace being named as a domain of operations in 2016 Warsaw Summit, member states should pay special attention to choosing the right directions in their national capacity-building activities. As Jamie Shea, former Deputy Assistant Secretary General for Emerging Security Challenges at NATO emphasized:

"… the cyber domain will require NATO to increasingly work top down on anticipating the strategic trends and adjusting policy and doctrine more quickly, while working bottom up at improving basic cyber hygiene to lower its attack surface and reduce the scope for own goals due to basic human error [2]."

The bottom-up activities are described by Shea [2] in the following order:

- in accordance with the cybersecurity Memorandum of Understanding signed by most of the member states, intelligence sharing, crisis management and exchanging lessons learnt from previous cyberattacks should be enhanced,
- the new intelligence division should be fed with early warning and advance notice of cyberattacks or malware as such information can help other member states to be better prepared,
- training and exercises should be organized for not only the 200 operators of NATO Computer Incident Response Capability (NCIRC), but for the national incident managers as well. Locked Shields won by the Czech Republic in 2017 is a good example for such activities,
- NATO must train civilian and military personnel regularly in the basics of cybersecurity in order to improve cyber hygiene,
- national experts should be sent to NATO HQ and to the most important and advanced cybersecurity centres, like Cyber Command and the National Security Agency in the United States, and the Government Communications Headquarters (GCHQ) in the United Kingdom.

As we can see, NATO recommends a highly technical approach in its bottom-up plans that inevitably requires a fully-operating milCERT, as all the above-mentioned goals are tightly connected to its core functions. Without further defining the differences between CERTs, CIRC, CSIRTs and SOCs, we assume that national defence forces should target the most mature level and operate a cyber defence team with advanced incident management capabilities.

Deshpande [3] defined Security Operations Centres as both organization units and teams. In a multinational environment, they often operate in shifts around the clock. SOCs can also be defined as facilities dedicated to preventing, detecting, assessing and responding to threats and incidents coming from the cyberspace, as well as to fulfilling and assessing regulatory compliance. SOCs usually cover multiple security activities that require different skill sets. A fully-functional SOC running 24/7 requires a team of a minimum of eight to 10 people just to maintain two people per shift, working three days on, three days off, four days on and four days off in opposing, 12-hour shifts [4]. The main activities that an SOC covers are monitoring functions, detection, triage of alerts, resolution of incidents (by taking actions or escalations), handling of issues (aligned with the internal or external processes required, e.g. ticketing system or reporting), and threat hunting and threat intelligence (TI) [5]. We use the words "SOC" and "CSIRT" interchangeably as most of the referenced articles use the term "CSIRT". We emphasize that such cyber defence teams are set up in accordance with the mission and goals of the organizations, which is more relevant from our perspective than the naming of these teams.

Maturity levels are well defined by the European Union Agency for Network and Information Security (ENISA) using many already existing schemes. The SIM3 model describes 45 parameters under four categories (Organization, Human, Tools, Processes) which are measured on a five-scale rating. Governmental CSIRTs, like milCERTs, are strongly advised to follow this guideline as emphasized in the document:

"Historically, many national and governmental CSIRTs have developed from very informal, sometimes ad hoc groups of highly skilled and motivated people. Given the growing number of tasks and responsibilities, there is a need for an adequate level of organization and governance. There needs to be thorough understanding about CSIRT internal processes that ensures consistency in the provision of services and a clear pattern of development and improvement of the team's capabilities [6]."

3. Human Requirements in MilCERTs

According to ENISA, one of the major elements of a mature CSIRT is the human and his or her capability of working in a team. Steinke and colleagues [7] have conducted research to examine what other emergency response teams' experiences can be used to set up an effective CSIRT. They found that besides Emergency Medical Systems Teams and Nuclear Power Plant Operating Teams, Military Response Teams can serve as an example for computer emergency response teams. The authors found that adaption, shared knowledge of expertise, trust, collective problem solving and communication are the key factors to team effectiveness [7]. These factors differentiate the milCERT personnel from business CERT personnel. In the business environment, main selection criterion of an analyst is the technical skillset; however, special trainings on the improvement of human abilities are rare. Therefore, in a military environment, CERTs have a better chance to build a good service not solely from the technical perspective, but also from the teamwork perspective. As all these skills are well-improved in a military environment, our basic assumption is that milCERTs can be built upon a good personal and team base from the human side which is essential in case of groups who are defending the national security and where personal requirements are higher than in a civilian environment. For further improving this skillset, defence universities should maintain and extend their classical trainings and drills and should improve them with some specific knowledge areas of the cyber domain. Like in Nuclear Power Plant Operating Teams, the milCERT trainings and drills should emphasize the human skills required to work effectively as a team besides "hard skills" of the domain.

3.1. Leadership in Military Cybersecurity

Conti and Raymond [8] argue that officers serving in the cyber domain need a different type of leadership than in regular military units. As the cyber domain needs mostly intellectual skills instead of physical power, cyber warriors are different from the others. They are more introverted and might not interact with their teammates like the others do in the physical field. Therefore, the already-learnt military drills might not work with the same efficiency in a computer room as they would on the battlefield.

"This is not to say that all facets of existing leadership should be discarded, the underlying principles of leadership remain the same, but these principles must be adapted with the cyber warfare mission, environment, and warrior in mind. Some tried and true leadership practices are likely to result in failure, and some principles, such as maintaining technical and tactical proficiency take on an entirely new meaning [8].”

In practice, this argument is confirmed by the case study of the Portuguese Navy. According to the Decree No. 13692/2013 of the national Minister of Defence, a sectoral CSIRT should be set up for the Portuguese armed forces. Das Neves [9] summarizes the achievements, following the Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability (DOTMLPF-I) framework. In the leadership section he points out that:

“The leader of this group should be someone with recognized technical skills, coordination of teamwork, with enough experience and current knowledge of the problems related to information security. Based on their own experience, skills and training, they must have the power to decide on the incident management, particularly its escalation to other entities; moreover, they should be the point of contact with external entities to the Navy for exclusively technical matters. They have to establish themselves as a reference for the other team members [9] .”

As we can summarize, defence universities should enhance their leadership trainings with a special module for future cyber commanders.

3.2. Technical Skills of Cyber Warriors

While more and more political statements require the improvement of offensive capabilities on a national level, NATO’s approach is considered. According to Shea [10]:

“… NATO will not develop offensive cyber capabilities and would therefore need to be able to rely upon voluntary national capabilities (subject to political approval by NATO overall) in instances where NATO military commanders believe that a cyber effect rather than the use of a conventional weapon is the best way of producing a desired military outcome [10].”

A majority of NATO members states will stay on the preventive or reactive measures in the forthcoming years, and offensive capabilities will be used only in military intelligence operations. Defence universities should understand this strategy and place more emphasis on cybersecurity operations from the preventive perspective, or as it has been called in U.S terminology in the past[1], Computer Network Defence (CND). For military intelligence agencies, the Computer Network Exploitation (CNE) skillset should be offered. Such knowledge is also useful in SOCs for threat hunting and malware analysis. Providing training for Computer Network Attack (CNA) is questionable, but as this kind of expertise can be used for setting up a red team[2], it is explainable.

We should also mention that NATO requires the setup of so called Cyber Rapid Reaction teams. Their task is to help member states deal with specific incidents and try to solve the issue jointly. This approach fits well to NATO’s operation, but raises several questions, such as sharing national secrets, giving access to dedicated systems for foreigners or simply the time needed to understand a special national system. In case of a well-known systems, RRTs might be doable, but in special systems, their practical

[1] CNA, CND and CNE were defined and used in United States Joint Publication 3-13: Information Operations but these terms have not been used since 2012.

[2] Red team in cybersecurity reflects to a group that works independently from the defence team and challenges the organization to improve its cybersecurity by assuming an offensive role.

operation needs further research. Due to the lack of publicly available information of NATO cyber RRTs, we do not analyse their function in more depth.

A good training program for milCERT personnel should consist of all elements and should go beyond the basics of cybersecurity. ENISA's survey also confirms the following statement: "the results from the survey indicated that training and education is considered the most important improvement made by the majority of the CERTs, indicating the significance of training activities for the CERT community [11]."

Tikk-Ringas, Kerttunen and Spirito [12] also advise a complex cybersecurity course for military personnel serving in cybersecurity units. In their research they highlight some key issues in current military cyber curricula. In smaller countries, cyber warriors are trained to be generalists and should perform functions up to more levels in their current rank. They also highlight the leadership challenge as mentioned above.

Based on the Baltic Defence College's model curriculum, they propose four levels of officer education: "Cyber defence and military cybersecurity need to be outlined in the context of the full spectrum of cybersecurity concerns reaching from basic cyber hygiene to civil-military cooperation and cyber diplomacy without overstretching the proportion of it [12]."

3.3. Role of Cyber Exercises

Both technical and leadership skills should be practised during complex exercises which simulate the real-world scenarios. This enables team members to apply the human and technical skills under high stress in real operational situations where less time is available for explicitly discussing what to do and how to do it. Cyber drills are frequently organized by NATO and national armed forces as well. Szabó [13] collected the most important exercises:

- Cyber Defence Exercise (CDX) is organized in the United States and involves responsible governmental institutes besides the military units. The red team in this case is the National Security Agency (NSA) whose major role in real life is to provide offensive capability in intelligence operations,
- Locked Shields has been the major cyber exercise of the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) since 2010. It mainly develops the defensive capabilities of the participating nations and aims to improve their communication and information sharing abilities,
- Cross Swords is also a NATO exercise, but it is open for other organizations besides military, including industry players. It is more technically-oriented and focuses on red and blue teaming[3]. This is an on-site exercise organized by the NATO Cooperative Cyber Defence Centre of Excellence,
- Cyber Coalition is the flagship cyber exercise of NATO. In 2017 more than 900 participants were involved into the three-days' long challenge,
- Cyber Perseu is a Portuguese event where the Spanish and Brazilian armed forces practise together with the national military experts,
- Panoptes is the Greek national event with more than 200 participants working on the challenge,

[3] Blue team is a team of defensive experts, IT security operators who perform an analysis of IT systems to ensure their cybersecurity and find potential security problems.

- Cyber Czech was initiated in 2015 and follows the NATO example. Its infrastructure, the KYPO, was developed by the CSIRT of Masaryk University (CSIRT-MU).

Post-event reports following the exercises confirm our argument on the importance of teamwork in milCERTs. Kulich [14] collected the experiences of the Slovak team after the 2013 Locked Shields event. Besides the technical expertise in this team, he also highlights the challenges of the group:

"Individual players could be either a big contribution or danger for a team cohesion. Therefore, if the group is bigger, it is important to appoint a team leader who will be responsible for fulfilling the goals of the group. Next important aspect is the plan and its compliance, since the matter of course is the collaboration of all the groups together. Another important part is to define the way of how the members communicate, how they use collaboration tools, how they solve previous aims set, and how the experienced and well-informed individuals pass on their knowledge to the younger members of the team [14]."

Developers of KYPO platform reveal the specialties of cybersecurity experts and confirm that even in a military team, individuals should be managed on a non-conventional way. Traditional military leadership might be useless. They share the following experiences in KYPO [15]:

- users, especially experienced and advanced ones, do not read information, manuals, and texts in game. It is necessary to explicitly tell them the most important facts,
- advanced users can find unintentional vulnerabilities and try to use them to complete game levels,
- always group similarly advanced users into same groups. One advanced user in a group of beginners can finish too early and he will get bored. On the other hand, a beginner in a group of advanced people will be frustrated from his relatively slow progress.

This was further analysed by Ošlejšek et al. [16], using more in-depth data of the cyber defence exercise platform at Masaryk University. Their hypothesis was that the participants improve their skills while using the platform and being fully involved in the exercise. Based on the data they collected, a majority of the learners gained new knowledge, but objectively it is not confirmed that all participants of a team were involved in the solution during the practice, therefore teamwork was not satisfactory.

4. Training of Military Cybersecurity Experts in Hungary

The six-year-old National University of Public Service plays a key role in the education of the Hungarian public service. The military officer training, the law enforcement officer (police, correction officer, customs officer, etc.) training and many different types of public administration trainings are conducted in this unique university.

The University's educational structure consists of five faculties and three inter-faculty institutes. The five faculties are: Faculty of Military Sciences and Officer Training, Faculty of Science of Public Governance and Administration, Faculty of International and European Studies, Faculty of Law Enforcement and Faculty of Water Sciences. The three inter-faculty institutes are: Institute for Research and Development on State and Governance, Institute of Disaster Management, and Institute of National Security. The University offers four doctoral schools with numerous scientific research programs including many cyber related topics. NUPS has roughly 5 000 students and cadets. It has 600 instructors.

Act 132 of 2011 on the National University of Public Service and on the higher education of public administration, law enforcement and military summarize the University's operation and principles as follows: "As part of the Hungarian higher education the objective of the National University of Public Service with administrative, law enforcement and military courses is to train professionals carrying out administrative, defence and law enforcement activities, to provide the officer supply of the defence and law enforcement bodies, and to create the interoperability of the unifying public service careers. In the course of the officer supply training the duties of the Hungarian Defence Forces and law enforcement bodies, their unique service and life circumstances, as well as the knowledge gained previously in the education and training systems of certain corporations have to be taken into consideration."

In accordance with this Act the main missions of the University are the following:

- to provide harmonized and planned supply training for the personnel of civil administration, law enforcement, defence and national security services besides the strengthening of vocation and expertise while placing the academic public service professional training on single institutional foundations,
- to create the interoperability of public service careers through forming a training system that supports public service career model, and through the creation of the integration of educational fields to ensure graduates' efficient work for society instead of letting them leave their career,
- to make the quality development of public service personnel more efficient as the training centres of the corporations involved, thus opening the path for a more integrated educational structure in the fields of bachelor, masters, doctorate and specific trainings, higher vocational education and retraining.

In the past years, the University's faculties constructed many new ways and new possibilities towards an integrated structure of education in the field of undergraduate (bachelor) and graduate (master) and Ph.D. levels, as well as postgraduate and special education programs.

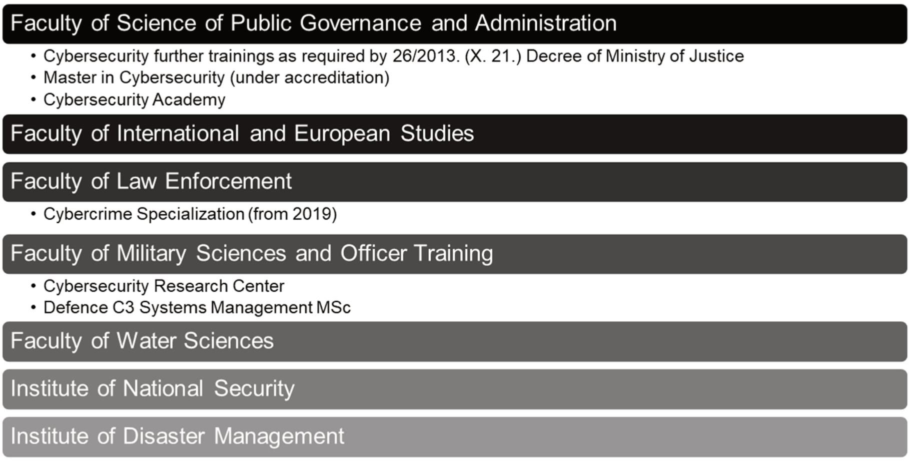
The cyber-related education and research activities have a relatively old history in the predecessors of NUPS, especially at the former Hungarian National Defence University. In the middle of the '90s, when the Information Warfare and later the Information Operations appeared, many research programs were conducted in those fields. Some years later cyber emerged and Cyber Warfare was examined parallel with Information Operations and its special parts, namely with the Computer Network Operations.

When the new University was established, a new Cyber Defence think-tank was created and as a result, a new Cybersecurity Research Centre was planned as a vision for the near- or mid-term future. The contributors of this think-tank conducted various research and development projects in the different fields of cybersecurity and cyber defence and critical information infrastructure protection. The scientific outcomes of those projects were transformed into special training and education programs at bachelor, master and Ph.D. levels. Many of those new results became part of curricula or training programs.

Today, the cyber-related research programs of NUPS focus on the following main dimensions:

- cyber strategies, in strong relation and collaboration with the public administration and Armed Forces of Hungary,
- cyber terrorism,
- methods and weapons of cyber warfare,
- cyber warfare and the international law on cyber operations,
- critical information infrastructure protection (CIIP), such as warnings and situational awareness, surveys for CIIP, trainings, research and development for different CII and CIIP stakeholders.

To reach the main research goals, there is a need for huge and wide cooperation at domestic as well as international levels which are detailed in Fig. 1.



Faculty of Science of Public Governance and Administration

- Cybersecurity further trainings as required by 26/2013. (X. 21.) Decree of Ministry of Justice
- Master in Cybersecurity (under accreditation)
- Cybersecurity Academy

Faculty of International and European Studies

Faculty of Law Enforcement

- Cybercrime Specialization (from 2019)

Faculty of Military Sciences and Officer Training

- Cybersecurity Research Center
- Defence C3 Systems Management MSc

Faculty of Water Sciences

Institute of National Security

Institute of Disaster Management

Fig. 1 Cybersecurity activities at NUPS

As we referred earlier, higher education in public service is greatly centralized in Hungary, and most tasks are carried out by the National University of Public Service. In addition to providing the public service succession planning in the institution's development plan and mission, the training system supporting the public service career model is also emphasized. Therefore, the University can be an excellent place for cybersecurity capacity-building. First of all, future cyber warriors and commanders learn in the Faculty of Military Sciences and Officer Training. Moreover, other future defence officers are also represented in different faculties, therefore successful exercises can be held with wide participations at university level. Meanwhile, based on the interviews conducted with responsible leaders and commanders of Hungary’s cyber defence organizations, there are some other capabilities that should be developed besides pure technical knowledge. In the following sections, we introduce the current education structure and propose new learning paths that aim at the improvement of teamwork in national defence in three main areas: cybersecurity awareness, incident management capabilities, and strategic or leadership skills.

4.1. Ability to Understand Cybersecurity in General (Cybersecurity Awareness)

The major requirement from the stakeholders was to improve cybersecurity awareness in the whole public service, including the military. We propose the following skill transfer for the students to learn the fundamentals in cybersecurity:

- at bachelor level: At this moment, only a few classes deal with the questions of cyber awareness. This needs to be improved, as it is essential to deal with the issues of cybersecurity in all bachelor's degrees, preferably during the first year, just because of the wide use of computers they will meet in their career in all professions. To do so, it is necessary to set up a practical laboratory class where students can experience computer-based attacks such as phishing, risks of incorrect password usage, or effects of a malicious code. On the other hand, during a theoretical lecture, the attacks that have been carried out need to be systematized, explaining that a user's mistake in the worst case could threaten the security of the whole country. At NUPS such lectures can be carried out within the Unified Common Module that is mandatory for all students, or it is possible to teach these classes within the faculties under subjects that are related to information technology,
- at bachelor and master levels: Considering that students are also interested in protecting their own digital existence, it is desirable to launch optional subjects that can demonstrate the practical questions of secure usage of computers and mobile devices in a semester. At the Faculty of Science of Public Governance and Administration, an Information Security Awareness course is currently available, and based on the annual feedback, students require some basic technical knowledge, so it is highly desirable to teach the subject with computer support. It is not needed to go deep into technical questions, but it can be taught how to harden devices, smart phones, configure home network devices, or understand social network privacy and security settings. This knowledge is necessary (but not yet enough) to dive deeper into cybersecurity,
- at post gradual level: The University's Institute of Executive Training and Continuing Education ensures the training of more than 70 000 civil servants annually, in many cases in the form of e-learning. Among these e-learning courses, more and more are dealing with cybersecurity and, specifically, increasing security awareness. As civil servants are required to take part in annual training courses, with the expansion of cybersecurity trainings, there is a chance that more and more people will choose these thematic courses, thus gaining an insight into the area.

4.2. To Build Incident Management Capability

As NUPS aims to provide a solid, interoperable base for all public service professions, not only the military faculty can serve as a source of milCERT personnel, but other faculties' students can also be hired for incident manager positions. To establish skills for incident management, the following courses should be offered:

- at bachelor level: based on a practical approach of security awareness, it is possible to gain a deeper understanding of the background and context of cybersecurity incidents in optional courses or in the case of more technically-oriented programs (for certain military and police programs) in mandatory courses. Such a course requires some network and IT skills, so it is also worth combining theoretical and practical knowledge. The aim is to provide a basic understanding of the operation of modern cyber defence systems, the technical bases of attacks and the features of security operation centres. Students who have completed the course can provide adequate labour force for both internal affairs and military security operation centres, which can be a solution to the shortage in human resources in the short term and can provide practical background for fresh graduates,

- at postgraduate level: Decree 26/2013. (21 October) of the Ministry of Public Administration and Justice on the training and further training of persons in charge of the electronic information security of state and local government bodies requires the University to prepare new e-learning training courses every year for the three target groups (persons responsible for the security of an electronic information system, persons involved in the security of an electronic information system, executives of the organization using an electronic information system). These trainings are available for the entire public service and provide a good basis for those who want to become specialists in cybersecurity. However, to build an incident management skill, laboratory practice is also necessary. For those who successfully complete the relevant e-learning training, i.e. acquire theoretical knowledge, it is possible to create a five-day (30-hour) course with the same practical base that the undergraduate students can get.

4.3. Strategic, Leadership Skills

A successful SOC requires a talented leader or leaders on multiple levels. As we discussed before, leadership is a key issue in the case of milCERTs. Furthermore, leading such teams has cybersecurity-specific requirements. To enable experts in national service to efficiently lead SOC teams, we propose the following training programs:

- at bachelor, master and doctoral levels: Based on the feedback provided by leaders and commanders, the Hungarian public service can absorb and integrate 30-50 non-technically-orientated specialists, experts and executives every year in the field of military and non-military cybersecurity. Therefore, we are not talking about mass education, but rather about individual talent management, in which deep understanding of one’s own specialization is as important as the ability to co-operate with other professions. One of the advantages of the University’s educational structure is that, under certain conditions, optional subjects are available to all professions, so it is desirable to start courses at each faculty which are also available for students of other faculties. This also helps to establish a good personal relationship between future leaders and commanders. However, in addition to the optional subjects, there is also an important responsibility for the special student groups, scientific circles and supervisors to develop individual skills in the niche areas, which is missing. At NUPS, we encourage the students to compete on national and international challenges like the National Cyber Challenge, Cyber 9/12 (organized by the Atlantic Council) or at Locked Shields,
- at postgraduate level: More and more public service professionals are looking for a new specialization within their profession and want to switch to cybersecurity. They already know their profession very well, so only cyber specialties must be taught to them. At NUPS, the post graduate course for persons responsible for the security of an electronic information system, launched on the basis of Act 50 of 2013 on cybersecurity is a good option. It consists of two semesters covering both theoretical and practical subjects. This postgraduate course is open not only for information security officers in organizations covered by the law, but for anyone. It is very popular, as 66 people attended the 2017/18 academic year, most

of them not due to the obligations by the law. Some of them came from the Hungarian Defence Forces as officers in charge. They can be cyber warriors or cyber commanders, depending on their personal abilities.

5. Concept of the Cybersecurity Academy

As mentioned above, educational and research activities of the National University of Public Service are conducted in five faculties and three inter-faculty institutes. All of these address certain aspects of cybersecurity in their way. However, due to the organizational autonomy and differences, a university-level coordination of cybersecurity education and research was required. On most of the faculties, one or two professors taught and researched cybersecurity, typically within the scope of optional courses, so they did not have the opportunity to run more courses or had only a specific knowledge set to be transferred to the interested students. Due to the differing timetables of the faculties and the distance between campuses, there was no opportunity to exploit the existing synergies.

The university management understood this challenge in time and found that cybersecurity is a horizontal topic that requires professional coordination between education and research actors. To accomplish this coordinating activity, on 1 March 2017 the Cybersecurity Academy was founded by the Rector of NUPS. It is led by the program director, with the support of a professional governing body. Its main goal is to integrate and organize the synergies of the cybersecurity work of faculties, institutes and research units, and to organize training and research programs to increase their effectiveness and efficiency.

Under the guidance of the Professional Governing Body and under the direction of the Program Director, the Cybersecurity Academy's primary task is to organize training programs, professional events and publications for international and domestic target groups, which:

- are based on the synergies of current training and research resources of NUPS,
- react flexibly and quickly to government development needs,
- effectively integrate NUPS's IT resources to reach a common goal,
- also apply a "comprehensive approach" to different roles of profession,
- generate developments that are in line with state-of-the-art IT technology.

From NUPS, professors involved in cybersecurity from the five faculties and institutes are members of Professional Governing Body, and external organizations that play a decisive role in the Hungarian cyber defence system are also invited. The members of this body are from the following organizations:

- National Authority for Data Protection and Freedom of Information, its president is the chairperson of the Body,
- Ministry of the Interior,
- National Directorate General for Disaster Management, Ministry of the Interior,
- Constitutional Office,
- Special Service for National Security,
- Military National Security Service,
- Ministry of Justice,
- Ministry of Defence,
- National Police Headquarters, National Bureau of Investigation, Anti-Cybercrime Division,

- Hungary's Cyber Coordinator,
- Ministry of Foreign Affairs and Trade,
- Prime Minister's Office.

This coordination enables the different entities to have a common understanding of what is really required for the national cyber defence and how the governmental university can provide the background. In the last two years, some significant results have been achieved in the field of skill improvement and intra- and inter-organizational teamwork. Among others, a two-day cybersecurity exercise was organized with the participation of almost 1 000 students. With the simulation of a full-scale cyberattack against the Hungarian electricity system, not just the future cyber warriors, but all other young public servants understood the importance of cybersecurity. The next major milestone is a master program in cybersecurity that is under accreditation and aims to reflect all needs of public service in the protection of Hungarian cyberspace.

6. Conclusions

Teamwork in cybersecurity practice is as important as the technical skills the employees are required to have. There is increasingly growing literature from multiple fields which now describes the cooperation, leadership, and other human aspects in cybersecurity and which we have summarized in this paper. Built on that and on our previous research we are now focused on milCERTs. This aims to synthetize other industry knowledge and private sector/corporate security operation centres. As NATO and national defence initiatives have shown, there is a growing need for milCERTs to secure cyberspace besides physical defence. Compared to the civil field, the milCERTs have special needs and require a special source of personnel: military and public service experts.

As a result, the NUPS in Hungary is practising and continuously developing a joint educational program for multiple experts to provide future milCERT staff. This special curriculum to develop skills focuses on: technical skills, awareness, incident management, and leadership or strategy. To train a diverse set of experts in public service, a coordinating institution has been founded: The Cybersecurity Academy. This enables systematic training programs and co-training of different students in the fields of public service to prepare for security teamwork.

It is important to highlight that a multidisciplinary approach is required to prepare public service employees to be trained to be part of a milCERT team. Experiences from private CERTs and SOCs, and research on other high-risk fields where team work is crucial, and cybersecurity expertise is required to be synthetized.

Further down the road in the future we aim to develop and assess the training program at NUPS and continue the exchange of knowledge between cybersecurity technology and humanities fields.

Acknowledgement

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the Ludovika Workshop.

References

[1] KOVÁCS, L. The National University of Public Service and the Training System of Faculty of Military Science and Officer Training. In: KULCZYCKI, M. (ed.) *Better Cooperation for Better Operation of the Future Visegrad EU Battle Group.* Wrocław: CHROMA Drukarnia, 2013. p. 21-34. ISBN 978-83-61315-68-1.

[2] SHEA, J. How Is NATO Meeting the Challenge of Cyberspace? *PRISM,* 2017, vol. 7, no. 2, p. 18-29. ISSN 2157-0663.

[3] DESHPANDE, S. *Security Operations Centers and Their Role in Cybersecurity.* [online] October 2017. [cited 2019-02-16]. Available from: https://www.gartner.com/en/newsroom/press-releases/2017-10-12-security-operations-centers-and-their-role-in-cybersecurity.

[4] MUNIZ, J., MCINTYRE, G. and ALFARDAN, N. *Security Operations Center: Building, Operating, and Maintaining Your SOC.* Indianapolis: Cisco Press, 2015. 448 p. ISBN 978-0-13-405201-4.

[5] HÁMORNIK B.P. and KRASZNAY, C. Prerequisites of Virtual Teamwork in Security Operations Centers: Knowledge, Skills, Abilities and Other Characteristics. *Academic and Applied Research in Military and Public Management Science,* 2017, vol. 16, no. 3, p. 73-92. ISSN 1788-0017.

[6] KASKINA B., TAURINS E. and DUFKOVA, A. *CSIRT Capabilities – How to Assess Maturity? Guidelines for National and Governmental Csirts.* Heraklion: European Union Agency for Network and Information Security (ENISA), 2015, 59 p. ISBN 978-92-9204-164-9.

[7] STEINKE, J., BOLUNMEZ, B., FLETCHER, L., WANG, V., TOMASSETTI, A.J., REPCHICK, K.M., ZACCARO, S.J., DALAL, R.S. and TETRICK L.E. Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. *IEEE Security & Privacy,* 2015, vol. 13, no. 4, p. 20-29. DOI 10.1109/MSP.2015.71.

[8] CONTI, G. and RAYMOND, D. *Leadership of Cyber Warriors: Enduring Principles and New Directions.* [online] July 2011. [cited 2019-02-16]. Available from: http://smallwarsjournal.com/blog/journal/docs-temp/811-contiraymond.pdf.

[9] NEVES, P.J.B. das. *Ability to Respond to Information Security Incidents in Cyberspace: an Approach* (in Portuguese). DOTMLPI-I Lisbon: Técnico Lisboa, 2016. 123 p.

[10] SHEA, J. Stepping Up Its Game in Cyber Defence. *Cyber Security: A Peer-Reviewed Journal,* 2017, vol. 1, no. 2, p. 165-174. ISSN 2398-5100.

[11] BELASOVS, A. *CERT Operational Gaps and Overlaps.* [online] Heraklion: European Union Agency for Network and Information Security (ENISA), 2011. 73 p. [cited 2019-02-16]. Available from: https://www.enisa.europa.eu/publications/operational-gaps-overlaps.

[12] TIKK-RINGAS, E., KERTTUNEN, M. and SPIRITO, C. Cyber Security as a Field of Military Education and Study. *Joint Force Quarterly*, 2014, vol. 75, no. 4, p. 57-60. ISSN 0030-1299.

[13] SZABÓ, A. Technical Cyber Security Exercises – International Overview (in Hungarian). *Hadmérnök*, 2018, vol. 13, no. 1, p. 286-301. ISSN 1788-1919.

[14] KULICH, B. Lessons Learned from Military Cyber Defence Exercises. *Science & Military Journal*, 2014, vol. 9, no. 1, p. 47-53. DOI 10.1109/FIE.2017.8190713.

[15] ČEGAN, J. and VIZVÁRY, M. Lessons Learned from KYPO – Cyber Exercise & Research Platform Project. In JIRSA, M., KADERKA, J., HAGARA, L. and DOČKAL, J. *Security and Protection of Information*. Brno: University of Defence, 2015, p. 15-26. ISSN 2336-5587.

[16] OŠLEJŠEK, R. VYKOPAL, J., BURSKÁ, K. and RUSÁK, V. Evaluation of Cyber Defense Exercises Using Visual Analytics Process. In *Proceedings of the 48th IEEE Frontiers in Education Conference*. San Jose: IEEE, 2018, p. 1-9. ISBN 978-1-5386-1173-9.