International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXV No 2 2019

ADJUSTING THE MILITARY EDUCATIONAL PROCESS TO THE CYBER DEFENCE DOMAIN

Mihaela BOSTAN-POP

Communications, Information Technology and Cyber Defence School, Sibiu, Romania
pop23miha@yahoo.com

Abstract: *Threats, challenges and attacks are becoming more frequent, sophisticated and damaging within the new and unique environment, known today as cyber domain. The article presents the importance of cyber defence as a field of study and the tremendous efforts that are being made to continuously adapt the military educational process to this field. Concerning the education process in this domain, we can identify a strong need for improving the way we approach it and a striving call to fill the knowledge gaps for generating a credible cyber workforce. The aim was to analyze and present a few new cyber defence courses and the curriculum developed for both content and methods of education for officer career courses at military academies worldwide. The conclusion I have reached is that there are numerous modern methods that prove to be highly efficient in teaching this new subject matter and military educational institutions are investing into the skills and competence of their personnel.*

Keywords: military education, training, cyber domain, cyber workforce

1. Introduction

Nowadays various cyber threats are becoming more prominent and there is a rising understanding of them by nations worldwide. In consequence the military domain needs an accelerated adaptation in dealing with the emerging cyber risks.

Considered the fifth domain of warfare, cyberspace, is proportionately important to military operations, alongside land, maritime, air and space operational domains.

Cyberspace domain influences the other physical domains that dependent upon its availability, therefore armed forces lean on the non-physical domain to obtain success and security during a mission.

The numerous challenges the digital environment inflicts on military domain have a massive impact upon all the branches and activities conducted in the military organization.

This unique environment can be analyzed from different points of view; we can take into consideration the physical and technological elements or the human resources that operate these elements.

Substantial efforts are being made for trying to define the concepts linked to cyber domain and spread awareness among the military organization and its personnel.

Within this context North Atlantic Treaty Organization and European Union member states must prepare to defend their networks and military operations against the continuously expanding cyber threats and attacks.

Regarding the human resource that needs to be qualified for this new environment it can pointed out the importance of cyber defence

DOI: 10.2478/kbo-2019-0083

as a brand-new field of study in the educational process. Military education makes no exception; clearly we can observe changes are being made to the structure of the curriculum and courses available at military schools and academies.

2. Cyber defence influence upon military education

There is a strong need to spread awareness and knowledge of cyber defence domain, among NATO and EU's Armed Forces, therefore the organizations are adopting proactive approaches in the education field.

NATO, EU and other partners are obliged to work together to strengthen cyber cooperation at the organization level and to eliminate the current vulnerabilities. To oust the risks that they are facing they need to consolidate a strong strategy for improving the ability to work together. The results are visible and quantified in the available specialized training courses, Military Erasmus Programm, cyber exercises, and other joint training activities.

Cyber defence evidently embodies military and civilian dimensions, and cyber challenges constitute a major threat to the security, defence and stability of the EU, its member states and its residents.

The Cyber Defence resolution adopted text, endorsed by the European Parliament, on 13 June 2018, highlights the significance of adequate education and training of military personnel.

The European Parliament strongly supports the Military Erasmus Programme and other common training and exchange initiatives aimed at enhancing the interoperability of the armed forces; stresses that there is a need for more experts in the cyber defence domain; calls on the Member States to facilitate cooperation between civil academic institutions and military academies to bridge this gap with a view to creating more possibilities in the field of cyber defence education; calls on the military academies to integrate cyber defence education into their curricula; believes that European armed forces can broaden their appeal by providing comprehensive cyber defence training to attract and retain cyber talent; also recognizes that human error is one of the most frequently identified weaknesses in cyber security systems, and calls, therefore, for regular training of both military and civilian personnel working for EU institutions [1].

From NATO's perspective the organization prepares to defend and enlarge resilience across its networks against cyber risks and attacks making cyber defence a core task for its collective defence.

Cyber education and training capabilities are reinforced within NATO, even a strengthen cooperation with industry is on progress through NATO Industry Cyber Partnership.

For developing and maintain competencies and skills in cyber defence domain NATO launched a Multinational Cyber Defence Education and Training Project - MN CD E&T - which has the main purpose to create a CD E&T Coordination Platform and to provide new initiatives that bring to completion NATO's CD E&T shortages.

United States Military Academy in West Point, New York, has a Cyber Research Centre incorporated within the Department of Electrical Engineering and Computer Science, dedicated to educate and inspire cadets and faculty in the acquisition, use, management, and protection of information through innovative teaching, curriculum development, research, and outreach to Army, Department of Defence, and federal agencies [2].

On the other hand the Defence Academy in Shrivenham, United Kingdom, incorporates a new Defence Cyber School with the mission to deliver skill sets and harmonize education with National Cyber Security Strategy objectives.

Cyber Network Fundamentals, Cyber Network Intermediate Practitioner and Cyber Network Security are the three operational cyber courses that are provided by Defence Cyber School helping the cyber workforce to understand networks and manage defence against future attacks.

The school offers Cyber awareness courses that include Defence Strategic Cyber Awareness and Cyber Operational Awareness, two seminars dedicated to commanders, leaders and managers helping them to effectively manage, exploit and defend against cyber effects at the operational and strategic levels [3].

Singapore is another example in featuring the importance of cyber defence as a field of study. On 20th February 2019, Singapore Ministry of Defence announced the foundation of Cyber Defence School and he recognized that human resources and technology constitutes the essence of Singapore Armed Force cyber defence capability.

To develop a highly skilled cyber workforce, Ministry of Defence and Singapore Armed Force have created the uniformed Command, Control, Communications and Computers Expert - C4X vocation for military personnel, and Defence Cyber Expert - DCX job specialization for non-uniformed personnel. The C4X and DCX personnel will work together with cyber Full-time National Servicemen to defend the Ministry of Defence and the Singapore Armed Force [4].

Looking at these examples we can observe the efforts that are being made to introduce cyber defence as a study field in the military education programs. Many states are making considerable purposeful steps for developing new cyber defence study programs although there is plenty of room for improvement.

Aside from these additions to the educational programs there is a recommendation that all of NATO and EU armed forces must have a convergent overview upon the way future cyber workforce potential, competencies and skills will be enlightened. Merging their efforts to follow similar judgment and making fruitful exchanges of ideas, NATO, EU and other cyber communities will ensure potential synergies, interoperability in order to eliminate all possible duplication of teaching and training in cyber defence discipline.

3. Innovative methods for educating future cyber officers

Cyber is a rapidly moving environment and, in accordance, military academies, schools and institutions must develop innovative and appropriate processes to adapt to a new reality and keep-up-to-date.

European Union Military Training Group conducted a Cyber Defence Training Requirements Analysis and the conclusive result was a description of Education and Training activities embodied into courses, exercises and e-learning. The development of an integrated approach to Cyber Defence Education and Training is undergoing, first at national level, where France and Portugal are strongly engaged and second at international level, where NATO and EU as organizations are involved.

Through opening up the curriculum to the full Cyber Defence discipline spectrum all of the cyber competences can be arranged under the form of a matrix containing the courses military personnel will attend in order to gain knowledge and develop proficiency.

Expositive classes followed by a debate and then some of the issues discussed may be used as a case study approach would be a good teaching method, but when it comes to cyber courses there are other ways to deliver the information and engross students interest.

One example of innovative forms of delivering education is online learning, a method that offers additional flexibility, can be used for cyber courses, and if developed correctly it may be used in a joint environment too. If students were to use online learning platforms then the collaboration between countries would enhance, and the knowledge would be significantly available to all platform users.

Another method to transfer effortless information to students that attend a cyber defence course would be to let them put into practice their knowledge in a cyber range. As cyber range operators, they can create an authentic duplicate of the real system, learn how to defend the network, use the right tools and follow the valid protocols to remove all simulated hacker attacks.

Cyber ranges can be seen as an environment where military students can practice competences such as penetration testing, defending networks, hardening critical infrastructure and responding to attacks [5]. More over these cyber ranges can easily be linked, forming Cyber Ranges Federations, thus generating a host of new exploitation possibilities.

4. Conclusions

Each and every education method can be treated like an innovative one as long as the educational objective has been accomplished. There are numerous modern education methods, but two of them draw my attention and I consider them to be highly efficient in teaching the cyber defence subject matter. Allowing students the possibility to enroll on an e-learning platform offers them the possibility to gain access and integrate information in a large spectrum of knowledge.

To make matters even more precisely by using cyber ranges and cyber labs the possibility to put into practice all the theory in a special artificial environment that replicates reality emerges making this method even more appealing.

Adequate education and training are the keys to succeed in eliminating cyber attacks that withstand and transform into evident challenges to our society and security.

Facing uphill challenge military academies, military schools and institutions introduce a forward-thinking approach in their curriculum and invest into the skills and competence of their cadets and personnel.

To conclude I would like to stress out again the importance that cyber defence could be looked upon as a field of study and, therefore, is an increasing need to appreciate correctly the great efforts that are being made to adjust the military education process with the cyber defence domain.

References

[1] *European Parliament resolution on cyber defence* (2018/2004(INI)), adopted text available at http://www.europarl.europa.eu

[2] https://westpoint.edu/centers-and-research/cyber-research-center

[3] https://www.da.mod.uk/colleges-and-schools/technology-school/defence-cyber-school

[4] https://www.opengovasia.com/singapore-ministry-of-defence-opens-new-cyber-defence-school

[5] Jon Davis, Shane Magrath, *A Survey of Cyber Ranges and Testbeds*, Cyber and Electronic Warfare Division, Defence Science and Technology Organisation, p. 2, Edinburgh South Australia, Australia, October, 2013, available at https://pdfs.semanticscholar.org/687f/f7737f9e32b85cf885db88341b73892aa8ae.pdf