TOOLS AND APPROACHES FOR THE PREPARATION OF CYBER DEFENCE SPECIALISTS

Miroslav Hrubý
University of Defence
Kounicova 65, 66210 Brno, the Czech Republic
miroslav.hruby@unob.cz

Abstract: *The paper deals with a problem of preparation of cyber defence specialists. Firstly, the necessary basic steps of the process are defined. Then some solution is offered. Finally, the future tasks are formulated. The main goal of the article is to contribute to the discussion about this problem area.*

Keywords: cyber defence, cyber safety, education, IT.

INTRODUCTION

The contemporary society is more and more dependent on cyber safety. Many countries are solving the problems connected with the upbringing and a suitable education of a number of highly needed and necessary new cyber defence specialists. The goal of the paper is to contribute to the discussion about this problem area. How to select a sufficient number of gifted students and what tools and approaches could be used are the main tasks of the preparation of cyber defence specialists, as well as of the paper. The author's point of view is based on the environment of the University of Defence, the Czech Republic. The research goals of the paper are: an analysis of open source data to the Czech National High School Cyber Security Competition, to suggest metrics for high school assessment in the cyber defence domain, to select the best Czech high schools in this domain, and to suggest a suitable approach to the cyber defence specialists' preparation. Available data sources analysis, knowledge synthesis, induction, deduction and comparison were used as the research methods. The author's own professional experience also played an important role in the formulation of the following text.

1. CYBER DEFENCE – BASIC INFORMATION

1.1 Cyber Defence in the Contemporary World

Cyber threats and attacks are becoming more common and sophisticated. Countries reinforce their capabilities for cyber education and training. They need to be prepared to defend its networks and operations against the growing sophistication

of cyber threats and attacks. Four different national approaches to cyber defence are discussed in Giles, Hartmann (2015). The authors compare the advantages and drawbacks of Norway, Estonia, Germany and Sweden's national approach.

In 2013 the European Union (EU) published its "Cyber Security Strategy – An Open, Safe and Secure Cyberspace" (Röhrig, Smeaton 2014). Information exchange, training and research in cyber defence have become a necessity. The process requires trust and various forms of cooperation.

The important questions for solving are:

- To estimate from where the next cyber attacks will originate;
- What will be the attackers' motivation;
- What will be their target(s);
- How they will probably realize the cyber attacks.

It is necessary to keep in mind that cyber attacks appear capable of having strategic consequences. At the national and organizational levels, a good starting point is methodical risk management, including objective threat evaluation and careful resource allocation.

The pertinent questions include (Geers 2011):

- What is our critical infrastructure?
- Is it dependent on information technology?
- Is it connected to the Internet?
- Would its loss constitute a national security threat?
- Can we secure it or, failing that, take it off-line?

The application of a Corporate Defence Methodology will enhance the organizational resilience and robustness in face of cyber-attacks (NCSA 2017).

1.2 Cyber Defence in the Czech Republic

Cyber security and cyber defence are seriously solved also in the Czech Republic. Cyber security includes, in particular, preventive measures and reactive measures against attacked subjects in the case of cyber security incidents. Cyber defence uses offensive capabilities towards the source of the attack. It includes tightly specialized activities aimed at defending the state against serious attacks, which can no longer be dealt with common cyber security. Cyber defence assets are therefore deployed only in cases of considerable importance, they may also have an offensive character, but can only be used for defensive reasons.

Citizens of the Czech Republic can use the website (CyberSecurity.cz 2018). Its main goal is general awareness of cyber security and cyber defence. A very useful tool for education seems to be Cyber Security Glossary (Jirásek, Novák, Požár 2015).

The legislative framework for cyber security consists especially of:

- Law No. 181/2014 Col., on cyber security and change of some laws (Cyber Security Law);
- Law No. 205/2017 Col.;
- National Cyber Security Strategy of the Czech Republic for 2015-2020;
- Action Plan for the Strategy.

On May 13, 2014 the National Security Authority of the Czech Republic opened the National Cyber Security Centre in Brno.

On August 1, 2017 the National Cyber and Information Security Agency (NCISA 2017) was established as a competent national authority for the issues of cyber and information security. The main areas of activity of NCISA include:

- operation of the Government Computer Emergency Response Team (CERT) (GovCERT.CZ);
- cooperation with other Czech CERT® teams and Computer Security Incident Response Teams (CSIRTs);
- cooperation with international CERT® teams and CSIRTs;
- drafting of security standards for different categories of entities in the Czech Republic;
- support of education in the field of cyber security;
- research and development in the area of cyber security.

The current cyber defence tasks of the Ministry of Defence of the Czech Republic are discussed in Feix, Procházka (2017).

2. DEFINITION OF BASIC STEPS IN PREPARATION OF HUMAN SOURCES

2.1 Suitable Start of Preparation

When, how and what methods should be used is a difficult task which should be solved together with experts in the developmental psychology. The core basic preparation should be realized at the high schools, students and their teachers should be strongly motivated. The author believes that one of the excellent ways to raise high school students' motivation is a Cyber Security Competition.

2.2 Cyber Security Competition

The Czech National High School Cyber Security Competition could serve as a very good example of human resources suitable motivation. This competition is organized annually. In the school year 2018/2019 the AFCEA (Armed Forces Communication & Electronics Association) cyber security working group organizes the third competition of this type in the Czech Republic. The role of the main guarantor is played by NCISA.

The competition is divided into three rounds. The first round is done electronically in September and October, the second round electronically in January and February, and the third attendance final round in April. The competition can be attended only by students of high schools whose age is between 14 and 20 years at the time of the start of the competition in September. They must be registered on the portal of the competition.

The competitive test consists of questions divided into several categories. A certain number of points is assigned to each correct answer. A bad answer in the first round means a negative assessment of -0.25 to -1 point depending on the type of question. The aim is to get as many points as possible. The second round is only for competitors who win at least 20 % of the maximum number of points in the first round. A wrong answer in the second round means a negative assessment of -1 to -5 points depending on the type of question.

The third final round is a one day competition. It is for the best 6 boys and best 6 girls and next best competitors from the second round to the total number of 30 to 60 competitors. Among other things, the winners can be invited to the European final, where they can compete with other young people from 20 countries (European Cyber Security Challenge 2018).

Table 1.

Basic data to the first two years of the Czech National High School Cyber Security Competition

	Competition I 2016/2017	**Competition II 2017/2018**
The first round:		
– total number of students	1,067	3,061
– number of successful students	565	1,852
– number of high schools	162	86
The second round:		
– total number of students	286	588
– number of students with a good knowledge	74	81
The third round:		
– venue	Brno Masaryk University	Prague Police Academy
– total number of students	29	36
– number of high schools	17	26
– points: 1st place / 15th place	118.0 / 41.2	447 / 220
European final:		

– venue	Malaga, Spain	London, U.K.
	September 2017	October 2018
– total number of Czech students	10	not known yet

Source: Own work based on data from the Czech National High School Cyber Security Competition

2.3 Selection of gifted high school students in the field of cyber security and cyber defence

The Czech National High School Cyber Security Competition could serve as a starting point for searching new required human sources for the cyber security and cyber defence.

Suggested metrics for high school assessment in the cyber defence domain could be based on

- Participation in the first round of the competition – total number of students from every participating school;
- Successful participation in the first round (students who win at least 20 % points);
- Successful participation in the second round (e.g. students who win at least 1 point);
- Successful participation in the third round (e.g. students who win at least 1 point);
- Winners of the Czech final (e.g. best 15 students);
- Successful participation in the international competition (a special care and education should be prepared for these gifted students in the next years).

Table 2.

The best high schools in cyber security education in the Czech Republic according to the first two years of the Czech National High School Cyber Security Competition

High school	Winners I 2016/2017	Winners II 2017/2018
Církevní gymnázium Německého řádu, Olomouc		1
Gymnázium Boskovice Palackého náměstí 1	1	
Gymnázium Boženy Němcové, Hradec Králové		2
Gymnázium, Český Brod		1
Gymnázium Jihlava	1	1
Gymnázium Jiřího Ortena, Kutná Hora		1
Gymnázium Jiřího z Poděbrad, Poděbrady, Studentská 166	1	
Gymnázium J. S. Machara, Brandýs nad Labem - Stará		1

Boleslav		
Gymnázium J.Š.Baara, Domažlice		1
Gymnázium Otokara Březiny a Střední odborná škola Telč	**1**	
Hotelová škola, Obchodní akademie a Střední průmyslová škola, Teplice		1
Jazykové gymnázium Pavla Tigrida, Ostrava-Poruba, příspěvková organizace	1	
Smíchovská střední průmyslová škola, Praha 5		2
SPŠE a VOŠ Pardubice	2	1
Střední odborné učiliště elektrotechnické, Plzeň		1
Střední průmyslová škola na Proseku, Praha	**3**	**1**
Střední škola informatiky poštovnictví a finančnictví Brno, Čichnova 106	**4**	**1**
Vyšší odborná škola a Střední průmyslová škola Žďár nad Sázavou	1	
Total	**15**	**15**

Source: Own work based on data from the Czech National High School Cyber Security Competition

Table 2 gives information about the Czech high schools and their best 15 students in the first two the Czech National High School Cyber Security Competitions. From the author's point of view the best education in cyber security is provided especially at high schools written in bold.

3. POSSIBLE TOOLS AND APPROACHES

Possible tools and approaches which could lead to stated learning objectives in the field of cyber security and cyber defence, should be especially set according to the age and level of contemporary general knowledge of target groups. The most suitable tools could be a mixture of lectures and practical tasks solving with the use of modern technologies prepared in compliance with the age and current knowledge of listeners. The author thinks that it is possible to recognize four main target groups with specific focus as follows.

3.1 Primary Schools

The main focus should be on mathematics, physics, IT and communication basic terms.

3.2 High Schools

Mathematics and physics knowledge should be deepened. The focus should be on IT and communication technology, programming, computer and communication networks and memory devices.

3.3 Universities

Beside top-level hardware and software, the focus should also be on law framework for use of top-level IT and communication technology.

3.4 Life-long Learning

Seminars and lectures, professional courses on IT, communication, sharing information, cooperation of expert groups and recent technology trends should be permanently provided.

CONCLUSION

Cyber security and cyber defence is based not only on sophisticated technical devices and methods but especially on top-level educated human resources, who are capable of performing demanding tasks in the field of IT, communication and law. Acquired data from the first two years of the Czech National High School Cyber Security Competition enable to select required human sources, who could be raised to strong needed cyber security professionals. An analysis of the steps and methods used for the preparation of winners of the competitions can bring valuable information which can play an important role of an irreplaceable source of knowledge which should be carefully used and improved in the future education of cyber security and cyber defence specialists.

The research goals of the paper specified in the introduction part were fulfilled but they can be developed deeper in the future. The future main tasks seem to be:

- Improve the education in mathematics and physics at primary and secondary schools as a basis for successful education of future experts in cyber security and cyber defence.
- Motivate contemporary experts in cyber security and cyber defence for their contribution in education of new generation of professionals in this field.
- Support especially English language education as the main communication language in the field of cyber security and cyber defence.

Acknowledgements

This paper was supported by the Ministry of Defence of the Czech Republic via institutional support for research organization development KYBERBEZ (DZRO K-209).

REFERENCES

AFCEA (2018). Armed Forces Communication & Electronics Association website. Retrieved from https://www.cybersecurity.cz/main_en.html (accessed 23 July 2018).

CyberSecurity.cz (2018). Kybernetická bezpečnost a obrana. Retrieved from https://www.cybersecurity.cz/main_en.html (accessed 23 July 2018).

Czech National High School Cyber Security Competition (2018). Středoškolská soutěž v kybernetické bezpečnosti. Retrieved from https://www.kybersoutez.cz/kybersoutez.html (accessed 23 July 2018).

European Cyber Security Challenge (2018). Website, London 2018. Retrieved from https://www.europeancybersecuritychallenge.eu/ (accessed 23 July 2018).

Feix, M., & Procházka, D. (2017). Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany. *Vojenské rozhledy, 26*(3), 31–50. doi:10.3849/2336-2995.26.2017.03.031-050.

Geers, K. (2011). *Strategic Cyber Security.* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.pdf (accessed 23 July 2018).

Giles, K., & Hartmann, K. (2015). Cyber Defense: an International View. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press. Retrieved from https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1286 (accessed 23 July 2018).

Jirásek, P., Novák, L., & Požár, J. (2015). *Cyber Security Glossary.* The third updated edition. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA. Retrieved from https://www.cybersecurity.cz/data/slovnik_v310.pdf (accessed 23 July 2018).

Law No. 181/2014 Col., on cyber security and change of some laws (Cyber Security Law). Retrieved from http://www.zakony.cz/zakon-SB2014181 (accessed 23 July 2018).

National Cyber and Information Security Agency (NCISA) – Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) (2017). Retrieved from https://www.nukib.cz/en/ (accessed 23 July 2018).

Röhrig, W., & Smeaton, V. (2014). Cyber Security and Cyber Defence in the EU. *Cyber Security Review,* Summer 2014, pp. 23-27. Retrieved from https://www.eda.europa.eu/docs/default-source/documents/23-27-wolfgang-r%C3%B6hrig-and-j-p-r-smeaton-article.pdf (accessed 23 July 2018).

The National Cyber Security Authority (NCSA) (2017). *Cyber Defense Methodology for an Organization.* June 2017. Retrieved from https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4_0.pdf (accessed 23 July 2018).