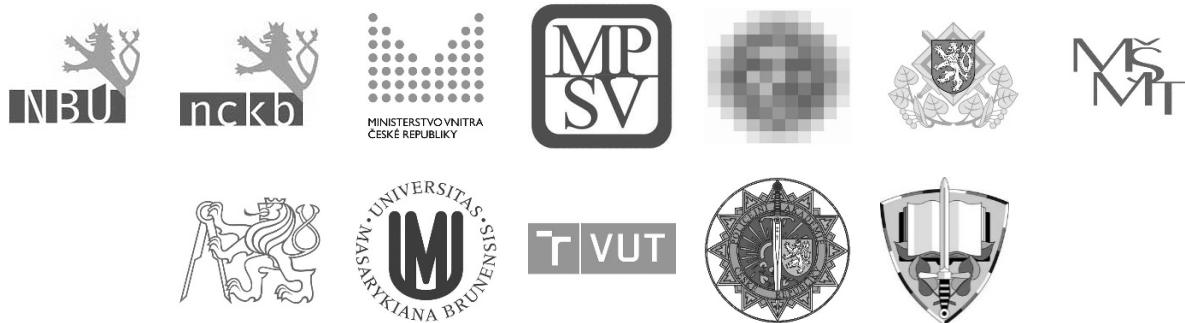# Executive Summary
CYBER SECURITY COMPETITION
SECONDARY SCHOOLS
CZECH REPUBLIC

The school year 2016 / 2017

Petr Jirásek et al

Praha © 2017

Executive Summary

Substantial growth in the use of information technologies in the current world leads towards a precipitous formation of the information society. On the one hand, the attendant acceleration of communications and the rapid development of digital services promote the growth of the whole society; however, on the other hand, we see a marked growing risk of abusing these technologies. Our society depends increasingly on digital data and communications, and thus successful attacks on the infrastructure or data result in extensive impacts on accessibility and trust and can potentially lead to large economic and material damage. In those cases when attacks, external or internal, are directed towards the critical infrastructure elements, this may ultimately result in putting the security or integrity of whole states in danger.

The response to this situation is a global effort for a quality protection of information and communication technologies against incidents that may jeopardize or change their operations, and this logically leads to a substantial increase in demands for the availability and education of new professionals in cyber security[1]. At the same time, we can see much stress being put on the dissemination and deepening of general public awareness, the public being the broadest potential source of mass proliferation of harmful codes (unsecured IoT, laxity towards identity protection, and similar).

The National strategy of cyber security of the Czech Republic and the Action plan of the National strategy of the Czech Republic for 2015-2020 was adopted by a government decree on 25 May 2015. This action plan includes several requirements for the education of experts, members of the public and students at all levels of education. The universities have been trying to respond to this state of affairs and step by step launch (albeit uncoordinated) educational programmes in the cyber security and defence. Secondary schools have not been involved yet in any focused way which explains the low interest of their students in continuing their studies in cyber security at the universities.

The Action plan of National strategy of cyber security of the Czech Republic contains, mostly in Part F, many objectives aimed at the students and teachers of secondary schools, for example: (a) increase the awareness and literacy in cyber security for secondary-school students; (b) contribute to the modernization of secondary-school educational programmes; (c) support the training of experts; (d) prepare methodological learning materials for the teachers; (e) promote talents among students in cyber security in cooperation with the universities.

AFCEA Czech Cyber Security Working Group (from now on „Working Group") **has been implementing awareness, educational and professional activities in cyber security and defence since as early as 2004.** The group organises, on a regular basis, security seminars for the employees and professionals from among the state sphere, the academia and the private sphere. It put together and has been updating (as required by the dynamic development of cyber security) the Cyber Security Glossary. The glossary has become an official publication and won several professional awards. The group has also organised many lectures, practical

---

[1] Cyber security is a collection of legal, organizational, technological, physical and educational means aimed at providing undisturbed and fault-free operation of the cyberspace. The cyberspace is a digital environment making possible the origin, processing and exchange of information created by information and communication technologies including access to a public network (internet). [Jirásek, Novák, Požár, Výkladový slovník kybernetické bezpečnosti, Praha, 2013. ISBN 978-80-7251-397-0]

workshops and exhibitions of modern security trends and technologies. The group has a close cooperation with the universities.

At the end of 2015, activities of the Working Group gave birth to the idea of a nation-wide cyber security competition aimed at secondary-school students. Preliminary efforts to implement the original idea were substantially accelerated in the spring of 2016 thanks to the offer of the European agency ENISA[2] to nominate the Czech national team, made up of secondary-school and university students, take part in the European Cyber Challenge (from now on „European finals").

Thanks to the rapid response and support on the part of selected state institutions, a decision was made in July 2016 to organise the first class of the Czech Secondary School Cyber Security Competition as early as the school year 2016/2017. The list of state institutions was headed by the National Security Authority, Ministry of the Interior of the Czech Republic, Ministry of Labour and Social Affairs, partner professional associations (in particular ICT unie, ČIMIB, NCBI) and there were also academic institutions headed by ČVUT (Czech Technical University), University of Defence, Police Academy, Masaryk University and Brno Technical University.


Competition Committee was made up of cyber security professionals and faced no easy task. A quality competition had to be prepared in a relatively short time; the competition had one objective of verifying the knowledge of secondary-school students and selecting the best candidates for the European finals; the primary goal, however, was to address the young generation and arouse the interest in cyber security. In order to achieve these objectives, it was, of course, necessary to speak to the teaching staff and prepare for them the learning resources to teach cyber security as well as teach at least the fundamentals of how the cyber space operates.

---

[2] European Union Agency for Network and Information Security.

Despite minor technical issues in the initial phase and high time constraints of the whole process of preparations it was possible to issue a report in October 2016 that the competition was ready to start. This situation was made possible due to the efforts of many professional partners who took part there. Big thank-you is due to all; however, two companies must be singled out- Corpus Solutions, a.s., which put up a completely new competition portal for the first and second competition rounds using the Lime Survey technology- and DataSpring a.s., which provided hosting and technical support for this portal in their data centre. These events contributed substantially to the fault-free progress of the competition in the first year.

However, the greatest challenge and a chapter in its own right in the first year of the competition was using the appropriate communication methods to students themselves, arouse their interest and thus get them involved in active participation. The competition committee left nothing to chance and created a series of campaigns reaching out not only to students but also to the teachers and parents and not only in the secondary schools (and their controllers) but also to various associations which cooperate with the secondary schools on a long-term basis.

Participation by regions
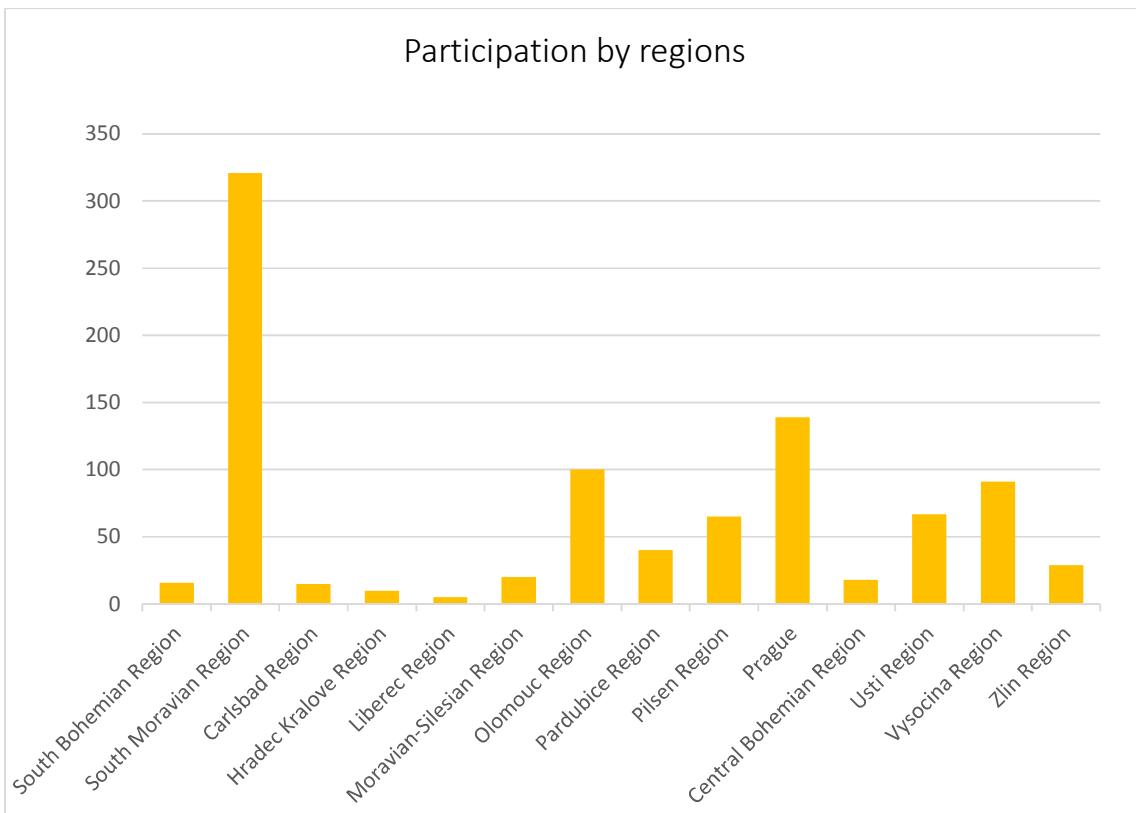
As a result, the participation was more than a thousand students from about 12 per cent of secondary schools organised in the Czech Republic. The greatest provable influence on getting the students´ participation was by the social media headed by Facebook. Direct communication with the schools resulted

in cooperation with the headmasters and headmistresses, and thus, among other things, representatives of the Competition Committee carried out more than sixty professional presentations at the secondary schools throughout the Czech Republic. Almost 2,500 students and about 150 of their teachers took part. This activity got a wide reception and created space for further cooperation and deeper involvement of the remaining secondary schools in the next years.

The competition was divided into three rounds. The difficulties and complexities of the questions and tasks increased with each succeeding round. The first round was online at the turn of November and December 2016 and contained 15 more or less general questions from five areas of cyber security. The second round was also online in March 2017 and had ten practical tasks. The third round was held in Brno in the framework of the International Fair IDET 2017 and the finals, with a required registration, were held on 1 June 2017. There thirty best contestants had to solve six complex team tasks within a time limit. As the finals were held on the premises of the fair, there was an additional bonus for the students and the accompanying staff: they could get acquainted with modern technologies and new trends in cyber security and defence, and more.
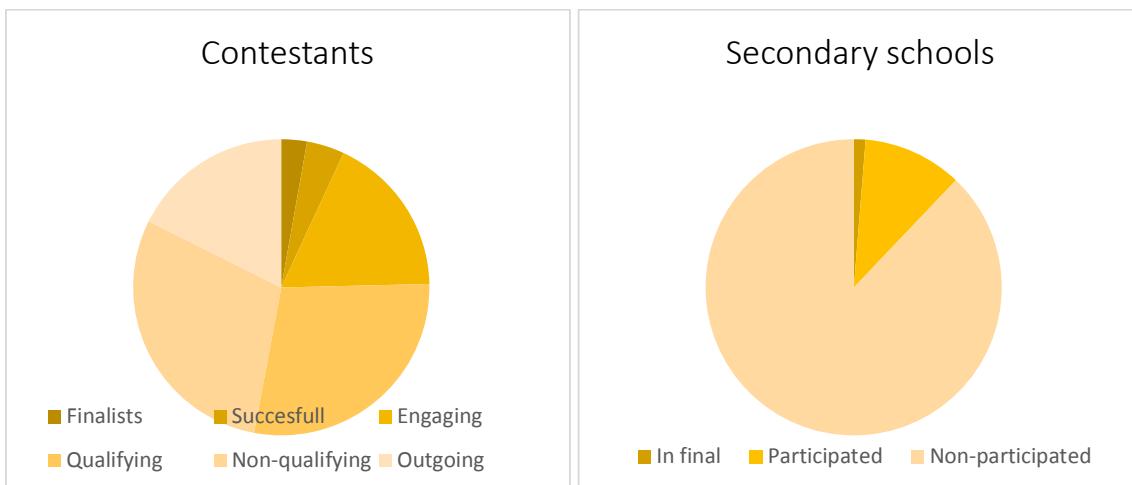
The final round provided the candidates for the participation in the Czech national team in the European Finals. Their qualification was confirmed during the summer camp in the Cyber polygon of the Masaryk University in Brno in July 2017.

The Competition Committee would like, on behalf of the members and organisers, to thank all partners and supporters of the first year of the competition for its smooth progress. The competition was organised as a non-profit, no-loss and low-cost event with the participation of volunteers. The volunteers have **spent more than 1,750 unpaid hours** during the preparation and course of the competition. There would be no competition without the help and active cooperation of all of the above subjects. Thank you ever so much.

The organizers and the Competition Committee, having used the experience from the first year, have decided to continue the work so well begun and organise the second year of the competition in 2017/2018, in order to increase the awareness among the secondary-school students in the cyber security issues, motivate the young people for a deeper (not only user-like) interest in modern technologies and, last but

not least, make them compare their knowledge with their peers in fair and open contests in their schools, regions, and the whole of the Czech Republic.

The complete report from the first year of the competition is available on https://www.kybersoutez.cz.

We are looking forward to your participation and support.

Competition Committee

7E0 CZ 2016
CYBER SECURITY COMPETITION

For more information, please contact:

Competition Committee
Czech Secondary School Cyber Competition
Cyber Security Working Group
AFCEA Czech Chapter
kybersoutez@kybersoutez.cz
www.kybersoutez.cz

Poskytovatel infrastruktury soutěžního portálu | Tvůrce soutěžní aplikace založené na LimeSurvey | Odborní partneři

DataSpring | CORPUS SOLUTIONS | AEC · ALEF · CISCO · CSIRT.CZ · CYBERGYM EUROPE · GORDIC · i-com-unity · ICZ · cz.nic · Microsoft · TOVEK · TREND MICRO · T.NET

Partner dopravy | Mediální partneři

České dráhy Národní dopravce | computer · ict network news · IDG · progres partners · BVV Veletrhy Brno · zive

Deloitte.

nckb · MPSV · úřad pro ochranu osobních údajů · KYPO · VUT · Provozně ekonomická fakulta · VŠKE · všrr

CSIRT.CZ · SSPŠ · cz.nic · European Cyber Security Excellence Center · NCBI · ict unie · JSI · AOBP · KYBEZ · ČIMIB

NBÚ
Národní bezpečnostní úřad

AFCEA

nckb
Národní centrum kybernetické bezpečnosti