PROGRESS TOWARDS CZECH NATIONAL CYBERSECURITY QUALIFICATIONS FRAMEWORK

Jan Hajný / František Kasl / Pavel Loutocký /
Miroslav Mareš / Tomáš Pitner

Jan Hajný, Ph.D., associate professor; Brno University of Technology, Faculty of Electrical Engineering and Communication, Department of Telecommunications; Technická 12, 61 600 Brno, CZ; e-mail: hajny@feec.vutbr.cz; http://crypto.utko.feec.vutbr.cz/

František Kasl, researcher; Masaryk University, Faculty of Informatics, CERIT and Faculty of Law, Institute of Law and Technology; Žerotínovo nám. 617/9, 601 77 Brno, CZ; e-mail: frantisek.kasl@mail.muni.cz; https://cyber.law.muni.cz/

Pavel Loutocký, Ph.D., postdoc researcher; Masaryk University, Faculty of Informatics, CERIT and Faculty of Law, Institute of Law and Technology; Žerotínovo nám. 617/9, 601 77 Brno, CZ; e-mail: loutocky@muni.cz; https://cyber.law.muni.cz/

Miroslav Mareš, Ph.D., professor, Masaryk University, Faculty of Social Studies, Department of Political Science; Joštova 10, 602 00 Brno, CZ; e-mail: mmares@fss.muni.cz; https://www.muni.cz/en/people/922-miroslav-mares

Tomáš Pitner, Ph.D., associate professor, Masaryk University, Faculty of Informatics, CERIT and Department of Computer Systems and Communications; e-mail: tomp@fi.muni.cz; https://www.muni.cz/en/people/94-tomas-pitner

Keywords: ***cybersecurity, qualifications, cybergovernance***

Abstract: *Cybersecurity is a crucial aspect of the progress towards cybergovernance. The coordinated and joined approach to ensure high level of cybersecurity throughout the country´s ICT infrastructures involves apart from the centralized cybersecurity activities and collaboration among CSIRTs also unified understanding of cybersecurity requirements, roles and activities among commercial entities, governmental agencies as well as individual cybersecurity experts. We present our current progress towards establishing such qualifications framework in the Czech Republic.*

1. Introduction on importance of the cybersecurity qualifications frameworks

The need and importance of comprehensive framework of qualifications in cybersecurity has been recently emphasised by various institutions and organizations. It is seen as foundation for unifying the often-diverging perspectives on cybersecurity requirements regarding work force qualification and education in particular.

For some time already, it is obvious that human resources in the field of cybersecurity are noticeably insufficient.[1] This situation affects security not only of private subjects but also the overall security situation of the state, which without available professional capacities is not able to effectively protect the cyberspace. This is a problem not only in the field of IT, but also with significant legal, security and management aspects, which solution requires specifically trained experts with adequate multidisciplinary knowledge.[2]

To promote and nurture the environment of high level of cybersecurity, it is necessary to uniformly define its key elements in order to be able to share information about cybersecurity capabilities comprehensively and transparently. Such is the aim of taxonomy, establishing unified terms, in particular in respect to qualification and necessary skills expected from various actors in the field of cybersecurity. With regard to work roles, such coherence of terminology is provided by cybersecurity qualifications frameworks, which should offer a „*taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for*

[1] Cf. Lusher, Present and Future Solutions for the Lack of Cybersecurity Professionals. Dissertation. https://search.proquest.com/openview/5efe4cf12de7323b4c5d840db2b9a498/1 (accessed on 14 November 2020), 2018.

[2] Cf. Muncaster, Cybersecurity Skills Shortage Tops Four Million. Info Security Magazine. https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-tops/ (accessed on 14 November 2020), 2019.

whom the work is performed."[3] They are therefore applicable to all sectors whether it is governmental body, cybersecurity response unit (e.g. CSIRT) or private company.[4] This approach is in the European Union supported by broad activity to build European Cybersecurity Competence Network with emphasis on necessity to offer meaningful roadmap of cybersecurity skills and education.[5]

The core capabilities of the workforce in the field of cybersecurity concern abilities to propose, develop, manage, and secure computer networks (as well as all related communication and information technologies) in view of the growing number of threats. This mission however entails a myriad of specific skills, knowledge and task elements, which differ depending on the particular situation, threat and position. It is also a highly dynamic environment, on one hand due to high velocity of changes and spread of digitalisation throughout the society, on the other hand due to the depth and value of expertise in particular sub-areas. Not only the specialists, but generally employees with expertise in cybersecurity field are highly sought after due to above mentioned excess of demand over supply for such work force. This in turn makes cybersecurity an attractive and popular area for education, training and qualification. Due to crucial role of cybersecurity experts in ensuring functionality, privacy and safety of the increasingly omnipresent ICT infrastructures, there is also a general public interest in solving the expert capacity shortage in this field quickly and efficiently.

The core challenge related to that is to have in place a functional frame of reference that will allow clear and uniformly understood communication of requirements between the demand side (government in general and employers in particular) and the supply side (education in general and job candidates in particular).

It is through the references to the cybersecurity qualifications framework that these parties are then able to properly evaluate and determine the requirements for the specific function and work role. This further allows them not only to appropriately adjust processes and procedures for employee selection, but also optimization of his/her work tasks, further talent development and performance assessment.

The purpose of such framework is to provide clear and generally applicable set of requirements associated with a work role taking into account compatibility with the hierarchy and systematic structure of work roles in the cybersecurity field in general. This compatibility aspect is of high relevance when considering an area where in individual work teams deep and specific knowledge needs to be adequately supplemented by broad multidisciplinary understanding as well as military-like hierarchy of management in case of security incident scenarios. "*An integrated cybersecurity workforce can address the cybersecurity challenges inherent to preparing their organizations to successfully implement aspects of their missions and business processes connected to cyberspace.*"[6]

Properly defining the needs of the demand side is however only one side of the coin. As such, the availability of required professional capacity in the work force pool depends largely on existence of systematic education building up the sought-after expertise.[7] In this context, the exchange between governmental, private and aca-

---

3 Cf. NIST, Nice Framework Resource Center. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center (accessed on 15 November 2020), 2020.

4 Ryerse, The importance of a cybersecurity framework. Security. https://www.securitymagazine.com/articles/93509-the-importance-of-a-cybersecurity-framework (accessed on 15 November 2020), 2020.

5 Cf. European Commission. Four EU pilot projects launched to prepare the European Cybersecurity Competence Network. Shaping Europe's digital future. https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network (accessed on 15 November 2020), 2019; European Commision. Proposal for a European Cybersecurity Competence Network and Centre. Shaping Europe's digital future. https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre (accessed on 15 November 2020), 2018.

6 Newhouse/Keith/Scribner/Witte, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication 800-181. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf (accessed on 14 November 2020), 2017. P. IV.

7 Cf. Rowe/Lunt/Ekstrom, The Role of Cyber-Security in Information Technology Education. SIGITE ,11: Proceedings of the 2011 conference on Information technology education. https://www.researchgate.net/profile/Joseph_Ekstrom/publication/220707262_The_role_of_cyber-security_in_information_technology_education (accessed on 14 November 2020), 2011. P. 113 et seq.

demic sphere is an important challenge as well as the interconnection of cybersecurity research with various other scientific disciplines (a. o. with intelligence studies).

There are various paths of individuals to increase their knowledge and obtain necessary skills, in particular nowadays with broadening availability of online courses, training materials and various other inspirational or enlightening content. Nevertheless, these additional and supplementary educational channels are mostly merely substituting the role of systematic education programs with necessary accreditation (providing the often-elusive guarantee of quality), which (not only in Czech Republic) still did not adequately respond to the increasing demand for cybersecurity experts and remain for now insufficient.[8]

Despite high quality of some online education currently available (in particular introductory or specialized courses provided by major world universities), most non-accredited educational channels provide murky and unreliable quality of expertise, which may lead to significant mismatch between employer expectation and employee capabilities. If only for this reason, there is high need for specialized cybersecurity study programs that will sufficiently build up the ranks of sought-after experts.[9] For this to be achieved through the provided curriculum, there needs to be a sufficient level of common understanding between the demand and supply side regarding the content of particular expertise. Therefore, it is necessary to align the development of study programs in the field of cybersecurity with the present and expected future requirements on qualification of the work force capable to cover the spectrum of roles increasingly demanded in the job market. This shows another crucial role of the cybersecurity qualifications framework, which should provide a point of common reference for this challenge, on the basis of which the study programs can be better adjusted to the needs of the job market, providing the graduate with better job prospects on one hand and fully contributing to solving the broader issue of insufficient availability of cybersecurity work force on the other. Currently, the Czech Republic is missing any such qualification framework or even a coordinated approach to cybersecurity study programs with unified criteria for identification of educational needs in this field of expertise.

2. Relevant experience with qualifications frameworks from abroad

Our work on Czech national cybersecurity qualifications framework was strongly influenced and facilitated due to availability of previous progress and suitable existing frameworks abroad. We have drawn on experience from EU as well as US environment.

The first framework considered is offered by American National Institute of Standards and Technology (NIST) and labelled National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.[10] We found this framework highly relevant for our purposes, in particular due to the high level of granularity, distinguishing elaborate groups (competencies) of elements (abilities, knowledge, skills and tasks), which are described in detail. These are used to define requirements associated with particular work roles. The work roles are systematically sorted in hierarchical structure of categories and specialty areas (e.g. Target Network Analyst falls under the category Analyze (AN) and specialty area Targets (TGT)). Each work role is then qua-

[8] For the overview of currently available higher and university level education in the cybersecurity field in the EU see ENISA. List of selected courses. https://www.enisa.europa.eu/topics/cybersecurity-education/education-map/education-courses (accessed on 14 November 2020), 2020.

[9] Surveys in the cybersecurity industry indicate that most companies expect from new employees at least bachelor level of education. Cf. EC-Council University, A Degree in Cybersecurity or a Certification Course: Which is Better for Your Future?. EC-Council University Blogs. https://blog.eccu.edu/a-degree-in-cybersecurity-or-a-certification-course-which-is-better-for-your-future/ (accessed 15 November 2020), 2019. In Czech Republic, such cybersecurity study programs are currently provided by Masaryk University, Faculty of Informatics (https://www.muni.cz/en/bachelors-and-masters-study-programmes/26540-kyberbezpecnost (accessed 15 November 2020)) as well as Brno University of Technology (https://www.vutbr.cz/en/students/programmes/branch/13264 (accessed 15 November 2020)).

[10] Newhouse/Keith/Scribner/Witte, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication 800-181. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf (accessed on 14 November 2020), 2017.

lified by description (e.g. Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave) and a specific set of qualification elements (e.g. Cyber Intel Planner is associated with 17 ability, 89 knowledge, 33 skill and 45 task elements). The NICE framework offers the richest material for cybersecurity qualifications framework we came upon, offers transparent taxonomy and is generally one of the most respected in the area of cybersecurity curricula. It therefore presented highly valuable input into our efforts. However, using it to its full potential was hindered by two drawbacks. Firstly, it was published in 2017, which means that in such dynamic area as cybersecurity, some elements or work roles were already becoming outdated and some newly emergent trends were not covered. This was clearly acknowledged by NIST, as the NICE framework is currently under revision and new version should be available early in 2021. This then transforms this drawback into significant benefit, as it shall make it into the most up-to-date cybersecurity qualifications framework available. The second drawback is the partial misalignment between the US and EU perspective, in particular with regard to legal, organisational and cyber-defence aspects of the framework. Drawing from the example of this framework thereby unavoidably required adjustment of the elements to Czech (EU) setting.

The European Union Agency for Cybersecurity (ENISA) has chosen different approach focused purely on education standards in European Union. This framework is predominantly identifying available courses and study programs oriented on cybersecurity, mapping available materials, databases, educational information and exposing gaps in available education.[11] As described above, we perceive this aspect as crucial for the purpose and benefit of the qualifications framework, as the study programs ought to develop skills and knowledge that is needed in the practice. Comprehensive EU taxonomy in this regard is currently lacking. This should be resolved for the education area by the initiative Sector Skills Alliances 2020[12] and through relevant EU taxonomy and capacity building in connection with education in the major projects SPARTA,[13] CONCORDIA[14] and CyberSec4Europe[15].

The third major source of experience for us was the initiative of American Joint Task Force on Cybersecurity Education[16], which created Cybersecurity Curricular Guideline[17]. The main task of this material is to offer structured taxonomy in order to help develop educational materials and programmes, but also to identify missing skills by the employees. We perceive it thereby as a sort of link between the NICE framework and ENISA activities. This guideline is based on eight knowledge areas (e.g. data security, system security, human security or organizational security), which are then divided into more detailed units. Each knowledge area

[11] ENISA, Roadmap for NIS education programmes in Europe. https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe (accessed on 15 November 2020), 2014. Most recently (November 2020) the ENISA Ad Hoc Working Group on the European Cybersecurity Skills Framework was established. See ENISA, Ad Hoc Working Group on the European Cybersecurity Skills Framework. Cybersecurity Education. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls (accessed on 15 November 2020), 2020.

[12] EACEA, Sector Skills Alliances 2020. Erasmus+. https://eacea.ec.europa.eu/erasmus-plus/actions/key-action-2-cooperation-for-innovation-and-exchange-good-practices/sector-skills_en (accessed on 15 November 2020), 2020.

[13] The SPARTA Cybersecurity Skills Framework links knowledge, abilities and skills (KAS) with predefined work roles and education topics. See SPARTA, Cybersecurity Training and Awareness. https://www.sparta.eu/training/ (accessed on 15 November 2020), 2020. An example of outcomes from the SPARTA project is the Cybersecurity Curricula Designer (https://informacni-bezpecnost.cz/curricula-designer/ (accessed on 15 November 2020)).

[14] CONCORDIA, Towards a European Education Ecosystem for Cybersecurity. https://www.concordia-h2020.eu/news/towards-a-european-education-ecosystem-for-cybersecurity/ (accessed on 15 November 2020), 2019.

[15] Cf. Cyber Security for Europe, Cybersecurity Skills and Capability Building (WP6). https://cybersec4europe.eu/work-packages/work-package-6-cybersecurity-skills-and-capability-building/ (accessed on 14 November 2020), 2020.

[16] The members of this task force are Association for Computing Machinery, IEEE Computer Society, Association for Information Systems Special Interest Group on Security and International Federation for Information Processing Technical Committee on Information Security Education. See Joint Task Force on Cybersecurity Education, ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline. https://cybered.hosting.acm.org/wp/ (accessed on 15 November 2020), 2017.

[17] Joint Task Force on Cybersecurity Education, Cybersecurity Curricula 2017. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf (accessed on 15 November 2020), 2017.

then contains description of what is needed for a specific position (either as working position or as educational needs) with interdisciplinary overlaps being explicitly emphasized.

3. Building Czech national cybersecurity qualifications framework

Structured upon the above described example of NICE framework, in alignment with the current ENISA activities and ongoing projects under initiative Sector Skills Alliances 2020 and with inspiration taken from inter alia the Cybersecurity Curricular Guideline, our multidisciplinary research team currently develops a Czech national cybersecurity qualifications framework. The aim of the project is creating a universal and holistic framework of cybersecurity qualifications applicable to Czech Republic. The framework shall classify individual professional roles, describe their required knowledge, skills and abilities and will serve as a single basis for capacity development in this area in the Czech Republic. It shall further include dynamic platform representation that will allow its use in the training and recruitment of workforce by all interested stakeholders. The members of the research team span a multitude of expertise areas concerning cybersecurity (technical aspects of cybersecurity, general IT expertise, security studies, legal background, organisational and business insight) and the project is set to develop the framework in close cooperation with a broad spectrum of stakeholders on all levels. The project is financed under the auspices of the Ministry of Interior, which ought to further contribute to broad dissemination and adoption of the result as a primary source of common reference. The research project started in 2019 and is set to conclude by 2022. It is systematically organised into four stages.

The first stage was focused on initial research and identification of available sources of inspiration and experience regarding taxonomy of work roles and qualifications in the field of cybersecurity. It involved survey of the current job market and the available educational channels and study programs concerning cybersecurity, as well as desk research aimed at determination of suitable sources for definition of the requirements for qualification of the various roles and positions. It was followed by in-depth analysis of the collected source materials and development of methodology for creating taxonomy. Given that the taxonomy was from the onset designed with the structure of a dynamic database in mind, in order to allow for its representation in a form of well-arranged interactive platform, the technological approach for this result was also discussed at this stage. The resulting taxonomy is a set of tree structures connecting the relevant elements in complex framework that allows insight from several perspectives (the perspective of the work roles for job market purposes, the perspective of competencies for educational purposes and the perspective of keywords identifying the qualification elements in order to allow better management and update of the framework).

The second stage is focused on default assignment of description and qualification elements (e.g. required skills and knowledge) to individual work roles and adjustment of the work role structure in order to indicate the complementary nature of specific sets of work roles. This default setting shall be further adjusted and updated based on cooperation and consultation with stakeholders. At this stage, the dynamic online platform representation of the framework shall be developed and its initial design shall be tested in order to verify that it is suitable to serve the defined needs.

The third stage shall be aimed at promoting the adoption and maximising the practical benefits of the developed framework and its platform representation. This shall include an action plan proposing systematic steps to be taken at the state, organisational and academic levels in order to achieve optimal development of the work force in the field of cybersecurity. It shall include a suggestion of mechanisms for support and incentives by the state to motivate educational institutions in development of systematic education and study programs concerning cybersecurity. Further considerations shall aim at improving the process of recruitment of qualified work force in public as well as private sphere in order to achieve higher level of cybersecurity in general. Part of this shall be a suggestion of further avenues for utilisation of the project results in practice for education, recruitment and assessment purposes.

The final fourth stage of the project shall concern finalisation of the online platform for dynamic representation and management of the created taxonomy and qualifications framework. This ought to involve and additional user-friendly layer on top of the previously developed administrative level, which will be freely accessible and should allow all interested parties as well as broader public to use the framework as well as link the database to broader set of applications or European level frame of reference, allowing for maximised benefits of its existence to be reaped. It is expected that at this stage the particular needs of main stakeholders shall be aligned with structure and functionalities of the framework and transition of administration onto respective authority (National Cyber and Information Security Agency) shall be possible.

The project is currently in the second stage, which is the core step in creating the main result of the project and it therefore also the longest and most challenging stage of the project. We have established the systematic structure of the qualifications framework and are currently developing an interactive online representation in a form of a platform that would allow transparent and user-friendly management of the default database of work roles and associated qualification elements. The adjustment and update of links between work roles and qualification elements shall be undertaken already on the platform, allowing on one hand a proper testing of the core functionalities and also implementing from the onset the processes for authorised administrative updates that are prerequisite for the framework to reflect new developments in the area of cybersecurity and retain high level of relevance over time.

4. Conclusions

The need of comprehensive framework of qualifications in cybersecurity is recently increasingly understood as beneficial on EU as well as national level by various institutions and organizations. It is seen as fundamental element of common reference that allows for describing the work needs in the field of cybersecurity and alignment between the demand on the job market and supply through specialised education and study programs. In the first part of the contribution, we described the underlying need and advantages of developing cybersecurity qualifications frameworks. The second part provided a brief overview of the three most relevant sources of experience and insight from abroad, which we identified and analysed in-depth in the first stage our research project. In the third part we provide an introduction to our research, its objective, structure and current progress.

5. Acknowledgments

This article was created on the basis of the project support of the Ministry of the Interior, Czech Republic within the project "*Národní kvalifikační rámec v kyberbezpečnosti*" [National Qualifications Framework in Cybersecurity] with the identification code VI20192022161.