CYBERSECURITY WORK FORCE SCARCITY – USE CASE CZECHIA: LESSONS LEARNED, LESSONS TO BE LEARNED

Pavel Loutocký / Miroslav Mareš / Jakub Drmola / František Kasl / Jakub Vostoupal

Pavel Loutocký, Ph.D., loutocky@muni.cz, postdoc researcher, CERIT – Faculty of Informatics and Institute of Law and Technology, Faculty of Law, Masaryk University, Botanická 554/68a, 602 00 Brno, Czechia, ORCID – 0000-0002-4965-1467;

Miroslav Mareš, prof., mmares@fss.muni.cz, professor, Department of Political Science, Faculty of Social Studies, Masaryk University, Joštova 218/10, 602 00 Brno, Czechia, ORCID – 0000-0002-7102-3205;

Jakub Drmola, Ph.D., jdrmola@mail.muni.cz, assistant professor, Department of Political Science, Faculty of Social Studies, Masaryk University, Joštova 218/10, 602 00 Brno, Czechia, ORCID – 0000-0003-4275-2115;

František Kasl, Ph.D., frantisek.kasl@muni.cz. postdoc researcher, CERIT – Faculty of Informatics and Institute of Law and Technology, Faculty of Law, Masaryk University, Botanická 554/68a, 602 00 Brno, Czechia, ORCID – 0000-0001-6675-9528;

Jakub Vostoupal, jakub.vostoupal@law.muni.cz, Ph.D. candidate and researcher, CERIT – Faculty of Informatics and Institute of Law and Technology, Faculty of Law, Masaryk University, Botanická 554/68a, 602 00 Brno, Czechia, ORCID – 0000-0002-1669-9931.

Keywords: ***Cybersecurity; qualifications framework; workforce; scarcity; use case***

Abstract: *In the long term, it is essential to ensure a sufficient number of well-educated and expert professionals for various positions in the field of cybersecurity with a high level of specific knowledge and skills. In this article, we present the situation and approach chosen in Czechia, which could serve as a potential inspiration abroad based on the experience gained. We analyse the current situation, problems and possibilities of mitigation by using cybersecurity qualification frameworks (specifically, the Czech one). Finally, we summarize specific recommendations that could serve as broader inspiration on how to mitigate the problem of expert workforce scarcity.*

1. Introduction[1]

The current evolution of cybersecurity threats requires an adequate response from the public, private and non-governmental sectors. It is essential to ensure a sufficient number of educated and qualified professionals in various cybersecurity positions with a high level of knowledge and skills in the long term. This high level needs to be guaranteed, thereby appropriate standards for cybersecurity jobs are needed. a similar level of knowledge and skills is desirable from the point of view of employers, who will be assured of the required level of security and the availability of cybersecurity experts, as well as of the European Union, as these standards allow for a harmonized approach to the cybersecurity workforce, its cross-border mobility and enable full use of the single market. This trend is expected to continue in the future. The existence and use of cybersecurity qualification frameworks, which provide the possibility of a suitable methodological approach to the issue and enable stakeholders to classify and identify their needs, is one of the tools that should substantially strengthen an adequate response to this problem.[2]

[1] This paper was created on the basis of the results from the project supported by the Ministry of the Interior, Czechia, "Národní kvalifikační rámec v kyberbezpečnosti" [National Qualifications Framework in Cybersecurity] with the identification code VI20192022161, which was concluded on 31st December 2022.

[2] Different approaches and types of cyber-qualification frameworks have been discussed, for example, in Drmola, J. et al. The Matter of Cybersecurity Expert Workforce Scarcity in the Czech Republic and Its Alleviation Through the Proposed Qualifications Framework. Vienna Austria: ACM, 2021. https://dl.acm.org/doi/10.1145/3465481.3469186.

In this article, we present the benefits and opportunities within the cybersecurity qualification framework for Czechia based on our previous research[3], as well as recommendations on how to address the unsatisfactory situation using the framework we developed as part of this research. The presented observations are primarily based on our findings, individual consultations, and questioning, as a comprehensive view on this issue is not available both nationally and internationally. Therefore, the article should provide inspiration on how to approach the issue abroad and present potential options for improvement, among others, using the specific example of the qualification framework we developed for the Czech settings.[4]

In the second section, we present an overview of the available educational capacities and the available workforce in Czechia in the European context, including a basic definition of the current level of competencies. Subsequently, we identify the challenges of ensuring a sufficient number and quality of cybersecurity professionals in Czechia and propose tools and procedures to enhance the availability of a skilled workforce in the context of using the Czech cybersecurity qualification framework based on our own research in the Czechia (including interviews and surveys of experts from the private sector, security forces and academia), experience from abroad and relevant literature.

2. Analysis of the Available Workforce and Education in the Field of Cybersecurity in Czechia

The ICT sector, in which the issue of cybersecurity is included, is critical in terms of the needs of national security and other areas of the state and non-state spheres. Currently, the labour market in this field is highly attractive and is characterized by a significant prevalence of in-demand workers over the number of experts actually engaged. Therefore, ensuring sufficient qualified experts is a fundamental security interest of Czechia. The growing need for additional cybersecurity capacities also results from Czechia's membership in the EU and NATO. The need for new experts is expected to significantly increase due to the implementation of the NIS 2 Directive[5] and other forthcoming European legislation.[6] Another major factor increasing the need for cybersecurity is the degradation of the overall security situation related to the war in Ukraine[7] and the related impacts.[8]

According to material from the Czech Statistical Office (CSO), in 2020, almost 219.8 thousand people worked in the ICT sector,[9] which meant 4% of the employed population.[10] The numbers have been increasing compared to previous years, and at the time of the publication of this text, it is possible to expect a further increase by tens of thousands of workers. Despite this fact, there is a shortage of approximately 14,000 ICT workers

[3] Publication outputs describing the logic, design and grasp of the qualification framework in Czechia within specific publication outputs are available here: https://www.muni.cz/en/research/projects/48648.

[4] See more at https://platform.cyqual.cz/en.

[5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

[6] Cyber-security package, Legislative Train Schedule [online]. *European Parliament*. 20.3.2023 [accessed 28.9.2023]. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-cyber-security-package.

[7] *Monsees, Linda,* The Cybersecurity Implications Of Russia's War On Ukraine, Institute of International Relations Prague – Expertise to impact [online]. 21.3.2023 [accessed 29.9.2023]. https://www.iir.cz/en/the-cybersecurity-implications-of-russia-s-war-on-ukraine-1.

[8] International Information System Security Certification Consortium, (ISC)^2 . *Cybersecurity Workforce Study*. 2022, p. 42. https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.

[9] *Myšková Skarlandtová, Eva*, ICT odborníci [online]. *Český statistický úřad*. 2.2.2023 [accessed 20.10.2023]. https://www.czso.cz/csu/czso/ict-odbornici.

[10] Lidské zdroje v informačních technologiích – 2020 [online]. *Český statistický úřad*. 11. 6. 2023 [accessed 20.10.2023]. https://www.czso.cz/csu/czso/cri/lidske-zdroje-v-informacnich-technologiich-2020.

on the labour market, as shown by a survey of private entities Coding Bootcamp Praha and Techloop.[11] However, according to our findings, this number may be up to twice as high. In addition to the significant salary inequality between the public and private sectors, the situation is complicated because the relevant authorities often do not register vacancies for such specialized technical positions. This further complicates the effective balancing of supply and demand and the identification of needs.[12] The classification and description in the records of the Czech employment offices also no longer correspond to current needs, and the state sphere does not always have a clear idea of flexible adaptation to current requirements in the ICT field. These problems are, however, de facto similar across the European Union.[13] In the case of international comparison, Czechia belongs to the European average in terms of the percentage of the employed population, and the table below also shows a steadily increasing year-on-year trend.

State	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
EU27 total	**3,6**	**3,7**	**3,8**	**3,9**	**4,3**	**4,5**
Belgium	4,2	4,9	5,2	5,0	5,0	5,6
Bulgaria	3,0	3,1	3,3	3,1	3,3	3,5
Czechia	3,7	3,6	4,0	4,0	4,2	4,6
Denmark	5,0	5,1	5,1	5,2	5,5	5,6
Estonia	5,3	5,6	5,7	6,0	6,5	6,2
Finland	6,6	6,7	6,7	6,8	7,6	7,4
France	3,6	3,8	3,9	4,2	4,5	4,5
Croatia	3,3	3,3	3,5	3,2	3,7	3,6
Ireland	4,9	5,0	4,8	4,9	5,7	6,3
Italy	3,3	3,4	3,6	3,5	3,6	3,8
Cyprus	2,7	2,9	3,2	2,7	3,1	3,9
Lithuania	2,5	2,7	2,7	3,1	3,3	3,8
Latvia	2,8	2,8	2,6	3,1	3,7	3,8
Luxemburg	5,1	5,2	5,9	6,1	6,3	6,7
Hungary	3,6	3,6	3,7	3,4	3,8	3,9
Malta	3,9	4,3	4,8	4,6	4,4	4,9
Germany	3,7	3,8	3,9	4,0	4,7	4,9
Netherlands	5,1	5,1	5,3	5,6	5,9	6,7
Poland	2,7	2,8	3,0	3,1	3,4	3,5
Portugal	3,1	2,9	3,1	3,6	4,0	4,7
Austria	4,2	4,4	4,5	4,3	4,5	4,5
Romania	2,0	2,1	2,2	2,3	2,4	2,6

[11] Proč je tak těžké sehnat IT specialistu? Aktuální data z trhu práce [online]. *Strojirenstvi.cz*. 2.8.2021 [accessed 21.10.2023]. https://www.strojirenstvi.cz/proc-je-tak-tezke-sehnat-it-specialistu-aktualni-data-z-trhu-prace.

[12] *Drmola, Jakub/Kasl František/Loutocký Pavel/Mareš Miroslav/Pitner Tomáš/ Vostoupal Jakub,* The Matter of Cybersecurity Expert Workforce Scarcity in the Czech Republic and Its Alleviation through the Proposed Qualifications Framework. In: ACM International Conference Proceeding Series: ARES 2021: The 16th International Conference on Availability, Reliability and Security. New York: Association for Computing Machinery, p. 1–6 (2021), doi:10.1145/3465481.3469186.

[13] For more on this topic, see e.g., the individual outputs of the European H2020 Sparta project at: https://www.sparta.eu/deliverables/.

State	2016	2017	2018	2019	2020	2021
Greece	1,9	2,1	2,3	2,1	2,0	2,8
Slovakia	2,9	2,8	3,2	3,7	4,2	4,3
Slovenia	3,5	3,8	4,0	3,9	4,4	4,8
Spain	3,3	3,4	3,5	3,6	3,8	4,1
Sweden	6,3	6,6	6,8	7,0	7,5	8,0

Table 1: EU27 percentage of the employed population in the ICT sector[14]

Cybersecurity permeates the entire ICT sector, although selected specializations are more strongly or exclusively related to cybersecurity. Cybersecurity specialists are currently one of the most sought-after professions on the labour market, and it is generally crucial that other ICT sector workers have the relevant knowledge and skills in cybersecurity. As a result, the demand for professionals in this field is constantly growing.[15] This is also acknowledged and considered one of the most pressing issues in the field of cybersecurity, as shown in a study by the International Information System Security Certification Consortium. For comparison, below are five challenges that cybersecurity professionals will have to face in the near future.

Challenge	Percentage of states concerned[16]
Risks of emerging technologies like blockchain, AI, VR, quantum computing, intelligent automation, etc.	61 %
Keeping up with changing regulatory requirements (e.g. PCI v4.0, GPDR, AI regulations, breach disclosure requirements etc.)	60 %
Worker/skill shortages in the workforce	60 %
Adapting to risks from advances in employee computing technologies (e.g., increased prevalence of sensors, AI, etc.)	55 %
Cyber-attacks stemming from cyber operations as a precursor to military conflict, tactic of military operations, or tool of retaliation	53 %

Table 2: Top five challenges for cybersecurity experts[17]

However, it is impossible to obtain accurate and precise information about the level of qualification of experts in the field of cybersecurity in aggregate. This is due to the fact that there has not been a sufficiently representative common platform to identify the status nor clear benchmarks for the level of qualification so far. Cybersecurity qualification frameworks, including the Czech one, mitigate this problem.[18] It is also helpful to harmonize the descriptions of expert work roles in cybersecurity to provide a suitable methodological common ground of the policies and other approaches to tackle the issue of workforce scarcity, to allow for better monitoring of the current labour market situation and to target the specific measures and challenges better.

[14] *Myšková Skarlandtová, Eva*, ICT odborníci [online]. *Český statistický úřad*. 2.2.2023 [accessed 29.9.2023]. https://www.czso.cz/csu/czso/ict-odbornici.

[15] The Urgency of Tackling Europe’s Cybersecurity Skills Shortage [online]. *Microsoft: EU Policy Blog*. 23. 3. 2022 [accessed 17. 10. 2023]. https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/.

[16] This column indicates the percentage of countries that expressed concerns about stated issue in the survey.

[17] (ISC)^2. *Cybersecurity Workforce Study*. 2022, p. 42. https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx.

[18] The Czech framework classifies the individual qualifications and professional roles of cybersecurity workers, describes their required education, skills, and abilities, and serves as a unified basis for capacity development in this area in the Czech Republic. It is available in summary via an interactive platform here: https://platform.cyqual.cz/en.

The educational system and academic institutions in Czechia are also trying to respond to the shortage of ICT workers, including cybersecurity specialists. As can be seen from the aforementioned CSO analysis, there are fluctuations in the absolute number of ICT students over time. In 2020, the number of ICT students was 21 660, of whom 72% were studying for a bachelor‘s degree, 24% a master‘s degree and 4% a doctoral degree.[19] However, two-thirds of students were studying programmes focused on software development and analysis, i.e., not a programme predominantly focused on cybersecurity (although it does contain cybersecurity aspects). Furthermore, it should be noted and reminded that cybersecurity is not just an ICT issue (even though it is often mistakenly taken as such). This "hard" technical approach is somewhat limiting in creating complex and secure cyber environments. Apart from the ICT experts, there is also a number of other expert cybersecurity work roles based on legal, managerial, security and political approaches. The prime example is the cybersecurity manager (according to the Czech Act on Cybersecurity), the top cybersecurity managerial position responsible for the organisation‘s cybersecurity as a whole. However, ironically, at this time, there is no complex educational scheme throughout Czech higher education for the position of cybersecurity manager.

In Czechia, according to the CyberHEAD database (maintained by the European Union Agency for Cybersecurity – ENISA), it is possible to study two bachelor‘s programmes specializing in cybersecurity (at the Faculty of Informatics, Masaryk University and the Faculty of Electrical Engineering and Communication, Brno University of Technology) and four master‘s programmes (again at same faculties as previously stated, 'CYBERHEAD – Cybersecurity Higher Education Database' 2023)[20]. Furthermore, as of 28th November 2022, the database of newly accredited programmes of the Ministry of Education also lists a total of 46 study programmes/fields of study of Czech universities in the field of education „Cybernetics" and 279 study programmes/fields of study in the field of education „Informatics".[21] In addition, of course, Czechia also uses experts in the ICT field, including cybersecurity, who have come to Czechia after completing their education abroad, either from EU countries or from outside the EU.

The whole ICT area, especially cybersecurity, is potentially vulnerable to information leaks and internal security. At the same time, for all workers in critical positions, and especially for workers from countries where there is an increased risk of acting against the security interests of Czechia, increased requirements for their security clearance may play a role, which further negatively affects the supply in this specific labour market.

Previous analysis of the available workforce and available training in the field of cybersecurity in Czechia can therefore be summarised in the following main points:

- cybersecurity is one of the most in-demand specializations within the ICT sector;
- the sector, in general, and the specifics in the field of cybersecurity demand a large number of experts;
- so far, there are no clear criteria for cybersecurity qualifications nor a platform for comparison (this deficit should be addressed to some extent at the national level by the Czech cyber qualification framework);

there are several specialized cybersecurity programmes at universities in Czechia, but these are not able to cover the needs in terms of national security and broader public and private sector interests.

[19] Lidské zdroje v informačních technologiích – 2020 [online]. *Český statistický úřad*. 11. 6. 2023 [accessed 20. 10. 2023]. https://www.czso.cz/csu/czso/cri/lidske-zdroje-v-informacnich-technologiich-2020 *v informačních technologiích – 2020*, 2023.

[20] CYBERHEAD – Cybersecurity Higher Education Database [online]. ENISA – CYBERHEAD Map. 25. 4. 2023 [accessed 3. 10. 2023]. https://www.enisa.europa.eu/topics/education/cyberhead.

[21] Registr vysokých škol a uskutečňovaných studijních programů [online]. *Ministry of Education, Youth and Sports*. 9. 2. 2022 [accessed 19. 10. 2023]. https://regvssp.msmt.cz/registrvssp/csplist.aspx.

3. Identification of Problems in the Provision of Missing Labour Capacities and Uncovered Training Capacities

The main problems in ensuring cybersecurity stem from the overall lack of ICT experts, including cybersecurity specialists. This, in turn, leads to the problem of securing experts to work in positions of national security importance in the public sector in a situation where the private sector can offer significantly higher incomes. Another problem is the unclear requirements for the qualifications of these cybersecurity experts overall and in individual cybersecurity specializations (e.g., IT security system and interface administrators, IT system assessment and testing specialists or cybersecurity auditors) resulting, among other things, from the lack of a uniform taxonomy of cybersecurity professions.

It is essential to provide experts for both „normal ensuring" of cybersecurity as well as highly qualified experts for special issues and the identification and management of emerging threats. The need for specialized experts at all levels is also linked to the need for a sufficient number of scientists and researchers in cybersecurity, adequate support for research and its link with practice. While many departments strive to achieve these goals, there are still deficits overall. There is also a lack of understanding of cybersecurity by some government authorities and a failure to provide sufficient resources for development in this area. While the issue of various threats in cyberspace (disinformation, hate speech, child pornography, etc.) cannot be ignored, cybersecurity is largely a technological and information issue (albeit with overlap into other vital areas) and must be seen and supported as a priority. Overall, only a multidisciplinary approach (linking technical education with law, social sciences, forensic disciplines, etc.), promoted in the academic and partly in the business environment, can produce sufficiently well-equipped experts. Nevertheless, there is considerable potential for further development.

As already noted, there is a shortage of expert cybersecurity personnel in both the private and public spheres. In the public sphere, the trend towards a shortage of experts is further manifested in a high staff turnover, especially towards the private sphere, often motivated by significantly higher financial compensation. Specifically, for example, in the case of the Czech National Cyber and Information Security Agency for 2021, technical and non-technical staff turnover was 12%, and by 30th November 2022, 13% of technical staff and 9% of non-technical staff (these data were communicated to the authors' team by the Czech National Cyber and Information Security Agency staff on 24 November 2022). Despite current temporary improvement at this agency, it is still pressing to strengthen the expert staff in the military, as results from our consultations, for example, with the Cyber Forces Command or the National Cyber Operations Centre of the Military Intelligence.

A remarkably similar situation is also evident in the case of police forces, whether in the cybercrime section of the National Headquarters for Counterterrorism, Extremism and Cybercrime or in the cybercrime departments of individual regional directorates. Specialized needs in the field of cybersecurity also arise in other security forces, be it the Customs Administration, the Prison Service (among other things, because of the illegal penetration of digital devices among prisoners, as well as possible attacks on databases and electronic security at prison facilities), the General Inspectorate of Security Forces or the Fire Brigade (cyber protection of equipment serving the Integrated Rescue System, for which the Fire and Rescue Service is responsible, also plays a specific role). Cybersecurity experts are also needed and lacking in CERT/CSIRT teams at many levels.

4. Measures to Enhance the Availability of Skilled Workforce Needed to Ensure National Cybersecurity

As identified above, measures to strengthen the skilled workforce needed to ensure national cybersecurity can be defined on intersecting quantitative and qualitative parameters, whereas on the qualitative level, the national qualification framework is significantly beneficial and usable. This is also in line with the requirements of the European Union in this area, which have been developed primarily by ENISA.

These contain recommendations and comparisons between EU countries on cybersecurity skills in higher education.[22] In addition, ENISA is developing a common framework for cybersecurity in the EU, which addresses qualification requirements in the European Cybersecurity Skills Framework.[23] It emphasizes, among other things, a greater diversity (in the sense of plurality) of educational disciplines, support for under-represented groups of people in cybersecurity and cooperation between Member States and the European Union in this area. ENISA also runs the CyberHEAD project, which contains data on cybersecurity training programmes in the EU and is being further developed and refined.[24] Nevertheless, it turns out that in accordance with the inspiration from abroad e.g., in the USA, UK or Italy,[25] it is highly beneficial to have a framework providing a detailed overview of individual work roles and skills, which is what localized qualification frameworks contribute to (as is the case with our CyQUAL framework, which was the result of a project successfully concluded at the end of 2022 and along with an action plan that served as a basis for this article approved and adopted by the Czech National Cyber and Information Security Agency for further use).

This top-down approach should strengthen not only national interests but also the security of cyberspace in the EU in general, which also emerged from the programme of the Czech Presidency in 2022.[26]

In particular, it is necessary to integrate the criteria contained in the qualification framework into the training and recruitment needs in the first step and with the assistance of the cyber qualification framework and to unify the terminology in defining roles and work positions at different levels of cybersecurity assurance. In addition, beyond staffing, a scientific understanding of cybersecurity needs to be developed in various applied and basic research dimensions.[27]

In order to strengthen security personnel from an organizational point of view, it is also necessary to provide special salary tariffs for cybersecurity experts in clearly defined state units (armed forces, security forces, intelligence services, selected central state administration bodies) and to promote general benefits of these units (retirement benefits, special health care, etc.) and to motivate them with training assistance and potentially specific certification for positions resulting from at least some of the roles included in the Czech qualification framework.

The recommendations for the Czech context that we arrived at include in particular:

- to support university programmes in Czechia that will be primarily focused on cybersecurity or will include this issue significantly (it is crucial to include cybersecurity in programmes of other orientations, e.g., law, management, social science security studies, etc.). These programmes should be designed in such a way that they are relevant to the roles and requirements of the qualification framework;
- to support an increase in the number of professionally oriented university degree programmes in cybersecurity;

[22] *Nurse, Jason R. C./Adamos, Konstantinos/Grammatopoulos, Athanasios/Di Franco, Fabio*, Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education, Report number: 10.2824/033355. European Union Agency for Cybersecurity (ENISA) (2021), doi:10.2824/033355 https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education[accessed 3.10.2023].

[23] Ibid.; European Cybersecurity Skills Framework (ECSF) [online]. *ENISA*. 2023 [accessed 3.10.2023]. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework.

[24] Nurse et al. *Addressing Skills Shortage and Gap Through Higher Education.*; CYBERHEAD – Cybersecurity Higher Education Database [online]. *ENISA – CYBERHEAD Map*. 25. 4. 2023 [accessed 3.10.2023]. https://www.enisa.europa.eu/topics/education/cyberhead.

[25] Respectively Hack the Gap [online]. *Cyber Seek*. 2023 [accessed 20. 10. 2023]. https://www.cyberseek.org/; The Cyber Security Body of Knowledge [online]. *CyBOK*. 27. 4. 2023 [accessed 20. 10. 2023]. https://www.cybok.org/; Schede delle professioni ICT [online]. *Osservatorio delle Competenze Digitali*. 27. 4. 2023 [accessed 20. 10. 2023]. https://competenzedigitali.org/osservatorio-delle-competenze-digitali/schede-delle-professioni-ict/.

[26] *Program českého předsednictví v Radě Evropské unie*. 2022. https://czech-presidency.consilium.europa.eu/media/edkb5w41/program-cz-pres.pdf.

[27] Základní pojmy výzkumu a vývoje v OECD a EU [online]. *Výzkum a vývoj v ČR* [accessed 20. 10. 2023]. https://www.vyzkum.cz/FrontClanek.aspx?idsekce=932.

- to support retraining and specialization programmes for already graduated experts in IT technologies and/or other programmes and disciplines related to cybersecurity, taking into account the roles defined in the qualification framework;
- to increase the budget that can be spent on retraining a jobseeker;
- to send experts from Czechia with public support or with support from specialized private entities to complete specialized university studies in cybersecurity abroad (prestigious universities in the field), while the selection of study programmes would also take into account the roles and requirements contained in the qualification framework; or similarly apply to specialized cybersecurity courses and internships at prestigious foreign and international cybersecurity workplaces;
- to encourage the arrival of foreign cybersecurity experts to the country to cover shortage positions identified by the cyber qualification framework;
- to encourage the arrival of prospective international students to study cybersecurity in Czechia;
- to promote cooperation, networking and information exchange between actors, experts, and stakeholders in cybersecurity, especially between educational institutions, academic experts, private sector representatives, public administration, and security forces.

For all of the above-mentioned groups of cybersecurity experts needed, not only do we need to identify those who are interested, but we need an active approach to motivate them to study or retrain, including support for under-represented groups. It is also possible to consider a stable national educational platform, for example the Greek Digital Citizen Academy.[28]

As mentioned, to ensure national security, it is also necessary to create an adequate research base that will enable an adequate response to new threats in cybersecurity, including adaptation to emerging technologies (including the expected arrival of quantum computers). Multidisciplinarity in research is also highly desirable, inter alia, in the link between ICT sciences and legal or social sciences, including their internationalization. In general, cybersecurity research must be one of the main priorities of national science and research policy. These should also consider improving experts‘ knowledge in the individual job positions defined by the qualification framework.

To this end, it is necessary to support stable research centres in the long term, which on the one hand, will be able to conduct research on their own initiative, and on the other hand, will be able to communicate permanently with the state and private cybersecurity forces about national security needs. Such centres can also be created by cooperation between several universities or research organizations (an example is the CyberSecurity Hub z.s., in which Masaryk University, Brno University of Technology and the Czech Technical University participate[29]), even internationally.[30] Of course, cybersecurity research can be developed at less prestigious institutions, but centres and teams of excellence should be preferred. Close cooperation with interested state institutions and private bodies, and thus support for applied research, must also be an integral part of the research. However, this should not only be through support from a single source (typically the government in the context of security research) but also through specialized agencies, international project frameworks or specific users from the public (especially intelligence services and specialized police forces) and the private sector.

[28] *Jākobsone/Māra*, Greece – Citizen's Digital Academy [online]. *Digital Skills and Jobs Platform*. 10. 5. 2021 [accessed 20.10.2023]. https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/greece-citizens-digital-academy.

[29] See more at: https://www.cybersecurityhub.cz/.

[30] For more on the sub-activity of setting up European digital hubs, see: https://digital-strategy.ec.europa.eu/en/activities/edihs.

5. Conclusion

In this article, we have presented the current experience and recommendations obtained during our research activities related to the problem of the lack of cybersecurity experts. One of the essential tools mitigating said state should be a cybersecurity qualification framework, which allows the classifying and categorizing of individual needs that can be further reflected. As an example of such a framework and related recommendations, we have presented an approach discussed and agreed upon by the Czech National Cyber and Information Security Agency.

In conclusion, the areas of action to strengthen the availability of the skilled workforce needed to ensure national cybersecurity can be summarised as follows.

It is essential to:

- provide special salary conditions and other benefits for cybersecurity experts in positions critical to national security (especially within the public sector);
- support specialized cybersecurity programmes, especially at universities and colleges of higher education, cybersecurity curricula for secondary schools and other educational activities (reskilling and upskilling);
- appropriately stimulate labour migration to Czechia to strengthen cybersecurity;
- provide appropriate research facilities in the field of cybersecurity.

In all these points, it is also necessary to consider alignment with EU-level initiatives (especially ones led by ENISA) and to emphasize that the cybersecurity work-roles need to be constantly reviewed and updated to reflect the current state of cybersecurity challenges (whether through a change of policy, education or regulatory ecosystem). That means the used qualification framework needs to be efficient, flexible, user-friendly, and capable of easy revisions and feedback collection. Only through this can it sufficiently react and serve its role to the highest potential.

6. Bibliography

(ISC)^2. *Cybersecurity Workforce Study*. 2022, p. 42. https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

CYBERHEAD – Cybersecurity Higher Education Database [online]. *ENISA – CYBERHEAD Map*. 25. 4. 2023 [accessed 3. 10. 2023]. https://www.enisa.europa.eu/topics/education/cyberhead

Cyber-security package | Legislative Train Schedule [online]. *European Parliament*. 20.3.2023 [accessed 28.9.2023]. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-cyber-security-package

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

Drmola, Jakub/Kasl František/Loutocký Pavel/Mareš Miroslav/Pitner Tomáš/ Vostoupal Jakub, The Matter of Cybersecurity Expert Workforce Scarcity in the Czech Republic and Its Alleviation through the Proposed Qualifications Framework. In: ACM International Conference Proceeding Series: ARES 2021: The 16th International Conference on Availability, Reliability and Security. New York: Association for Computing Machinery, p. 1–6 (2021), doi:10.1145/3465481.3469186.

European Cybersecurity Skills Framework (ECSF) [online]. *ENISA*. 2023 [accessed 3. 10. 2023]. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

International Information System Security Certification Consortium, (ISC)^2 . *Cybersecurity Workforce Study*. 2022, p. 42. https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

Jākobsone/Māra, Greece – Citizen's Digital Academy [online]. *Digital Skills and Jobs Platform*. 10. 5. 2021 [accessed 20. 10. 2023]. https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/greece-citizens-digital-academy

Lidské zdroje v informačních technologiích – 2020 [online]. *Český statistický úřad*. 11. 6. 2023 [accessed 20. 10. 2023]. https://www.czso.cz/csu/czso/cri/lidske-zdroje-v-informacnich-technologiich-2020 *v informačních technologiích – 2020*, 2023.

Monsees, Linda, The Cybersecurity Implications Of Russia's War On Ukraine | Institute of International Relations Prague – Expertise to impact [online]. 21.3.2023 [accessed 29.9.2023]. https://www.iir.cz/en/the-cybersecurity-implications-of-russia-s-war-on-ukraine-1

Myšková Skarlandtová, Eva, ICT odborníci [online]. Český statistický úřad. 2.2.2023 [accessed 29.9.2023]. https://www.czso.cz/csu/czso/ict-odbornici

Nurse et al. *Addressing Skills Shortage and Gap Through Higher Education*.; CYBERHEAD – Cybersecurity Higher Education Database [online]. *ENISA – CYBERHEAD Map*. 25. 4. 2023 [accessed 3.10.2023]. https://www.enisa.europa.eu/topics/education/cyberhead

Nurse, Jason R. C./Adamos, Konstantinos/Grammatopoulos, Athanasios/Di Franco, Fabio, Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education, Report number: 10.2824/033355. European Union Agency for Cybersecurity (ENISA) (2021), doi:10.2824/033355 https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education[accessed 3. 10. 2023].

Proč je tak těžké sehnat IT specialistu? Aktuální data z trhu práce [online]. *Strojirenstvi.cz*. 2. 8. 2021 [accessed 21. 10. 2023]. https://www.strojirenstvi.cz/proc-je-tak-tezke-sehnat-it-specialistu-aktualni-data-z-trhu-prace

Program českého předsednictví v Radě Evropské unie. 2022. https://czech-presidency.consilium.europa.eu/media/edkb5w41/program-cz-pres.pdf

Registr vysokých škol a uskutečňovaných studijních programů [online]. *Ministry of Education, Youth and Sports*. 9. 2. 2022 [accessed 19. 10. 2023]. https://regvssp.msmt.cz/registrvssp/csplist.aspx

Respectively Hack the Gap [online]. *Cyber Seek*. 2023 [accessed 20. 10. 2023]. https://www.cyberseek.org/

Schede delle professioni ICT [online]. *Osservatorio delle Competenze Digitali*. 27. 4. 2023 [accessed 20. 10. 2023]. https://competenzedigitali.org/osservatorio-delle-competenze-digitali/schede-delle-professioni-ict/

The Cyber Security Body of Knowledge [online]. *CyBOK*. 27. 4. 2023 [accessed 20. 10. 2023]. https://www.cybok.org/

The Urgency of Tackling Europe's Cybersecurity Skills Shortage [online]. *Microsoft: EU Policy Blog*. 23. 3. 2022 [accessed 17. 10. 2023]. https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/

Základní pojmy výzkumu a vývoje v OECD a EU [online]. *Výzkum a vývoj v ČR* [accessed 20. 10. 2023]. https://www.vyzkum.cz/FrontClanek.aspx?idsekce=932