9th International Conference on Higher Education Advances (HEAd'23)
Universitat Politècnica de València, València, 2023
DOI: http://dx.doi.org/10.4995/HEAd23.2023.16336

Cybersecurity education in European higher education institutions

Mirva Salminen, Niko Candelin, Kaisa Cullen, Sari Latvanen, Marianne Lindroth, Teemu Matilainen
Department of Information and Communications Engineering (DICE), Aalto University, Finland.

Abstract
This research paper presents some of the findings of an ongoing Cyber Citizen Initiative project (2022–24), which benchmarked civic cybersecurity education and training in all European Union (EU) member states. The research paper focuses on cybersecurity education in higher education. The study concluded that cybersecurity education varies across the EU. Whereas some countries have dozens of higher education institutes providing education in cybersecurity, some others have only a few institutions and educational programmes for the topic. In general, the educational programmes tend to be specific and focus on technical skills. A wider understanding of cybersecurity as a societal concern, civic cybersecurity skills, and discipline geared cybersecurity competence building may be lacking from the curricula.

Keywords: *Cybersecurity competence; cybersecurity skills; cybersecurity education; higher education; European Union.*

1. Introduction

The overarching digitalization of societies has made the strengthening of cybersecurity competence at all levels of society and across its sectors a priority in many countries. For a longer period, this has meant the build-up of cybersecurity focused educational programmes and curricula in universities and universities of applied sciences, as well as the integration of cybersecurity awareness and skills into basic and secondary education. More recently, the need of teaching civic cybersecurity skills to everyone in society has become emphasized.

This research paper presents some of the findings of an ongoing Cyber Security Initiative project lead by Aalto University, Finland. In its first phase (in 2022), the project benchmarked the 27 European Union (EU) member states regarding the teaching of civic cybersecurity skills. Civic cybersecurity competence is understood as "[t]he knowledge, skills and abilities required to operate in a cyber environment" (Limnéll et al., 2023, 2, 142). Everyone living in a digitalised society needs such competence. Data collection was implemented by extensive online research supplemented with interviews, conference and seminar attendance, and a scoping literature review.

This research paper focuses on findings regarding the teaching of cybersecurity skills in formal, higher education in selected member states. The countries in the sample provide a view to cybersecurity education across the union: Finland, Estonia, Germany, France, Romania, Spain, and Greece. Alongside providing geographical coverage, the selected countries rank relatively high in cybersecurity indices and/or host pivotal EU cybersecurity institutions. The research paper asks: How is cybersecurity competence currently built at universities and universities of applied sciences in the selected countries? The study includes both educational programmes in cybersecurity and civic cybersecurity training provided to all students in higher education.

2. Cybersecurity training in higher education in selected EU member states

There is no universally agreed practice of benchmarking (Chen et al., 2020). It can be understood as a process of improvement through adaptation and substitution of a process by another recognized as better (Maire et al., 2008, 765). In the Cyber Citizen Initiative project, benchmarking meant establishing the state of civic cybersecurity education across the EU to find out adoptable practices. This research paper focuses on higher education institutions providing cybersecurity education, the content of educational programmes, and the ways in which national cybersecurity strategies strive to improve cybersecurity education.

2.1. Finland

Finland's goal is to be a country of excellence in cybersecurity. One of its main strategic policies is the "[d]evelopment of cyber security competence – everyday skills and top skills

as cyber security safeguards" (The Security Committee, 2019, 8). National measures to enhance cybersecurity competence include, inter alia, the strengthening of cybersecurity and information security related education at all educational levels (The Security Committee, 2019, 4, 9). Higher education degrees focusing on cybersecurity are offered by both universities and universities of applied sciences. However, topics related to cybersecurity are part of several other higher education degree programmes as well (Limnéll et al., 2023).

Universities of applied sciences provide technical cybersecurity education. In terms of content, this education (eight bachelor's and four master's programmes, as well as specialisation, supplementary, and conversion training) is comprehensive and serves the needs of the industry. (Lehto, 2022, 9, 61-62.) There are three university degree programmes focused on cybersecurity, all master's programmes (provided by the universities of Jyväskylä and Turku and Aalto University) (Limnéll et al., 2023). In addition, cybersecurity is included in the structure of many degree programmes as optional or compulsory studies and many IT programs offer a possibility to study broader cybersecurity studies. Several free cybersecurity courses are also offered to everyone by the Finnish Institute of Technology (FITech), which is a network university. Its founding members include seven universities and technology industry associations. (Lehto, 2022, 10, 72, 76, 85, 92.)

2.2. Estonia

The promotion of a cyber-literate society is one of the goals in Estonia's cybersecurity strategy. To achieve this goal, the academia must be involved in cooperation with the public sector and companies. Cybersecurity is taught at all educational levels as part of the development of digital skills. Lack of cybersecurity specialists and a small number of new talents in the field are recognised as challenges which must be solved, for example, by including cybersecurity in intensified IT studies. (Republic of Estonia, 2019, 7-8, 15, 17.)

Studying cybersecurity in higher education is possible in two master's programmes. Tallinn University of Technology (Tallinna Tehnikaülikool, TalTech) runs a master's programme "Cybersecurity" in cooperation with the University of Tartu (Tartu Ülikool). The students study under high-level cybersecurity practitioners from universities, industry, law enforcement, CERT, and the NATO Cooperative Cyber Defence Centre of Excellence (Taltech, 2023). The international master's programme "Cyberus Erasmus Mundus Master in Cybersecurity" is administered by the University of South Brittany in France (Université Bretagne Sud) and TalTech is responsible for a part of the training. Students can specialise either in software cybersecurity or IoT cybersecurity. (Université Bretagne Sud, 2023.)

2.3. Germany

According to the German cybersecurity strategy, responsible behaviour in cyberspace and the opportunities and risks brought by internet are an essential part of digital citizenship

skills. Therefore, digital education must be integrated into the country's entire education system. (BMI, 2016, 10.) The organization of and decision-making in the school system are delegated to the education ministries of the 16 states. Thus, each state has different regulations regarding the curriculum, the provision of study subjects and degrees, and the transition between school forms. The federal government's goal is that by graduation young people have sufficient knowledge and skills related to IT security. The aim is to increase and to expand course offerings in IT by establishing more study places at universities and supporting leading institutions, especially in computer science (BMI, 2016, 10).

IT studies are offered in almost all universities, which also include comprehensive information and cybersecurity study units. For example, University of Saarland provides a master's degree in cybersecurity, which offers students an opportunity to deepen their cybersecurity knowledge comprehensively and choose a specialization in the areas of cryptography, privacy, software security, systems and networks, formal methods, or legal aspects of cybersecurity (Universität Des Saarlandes, n/d). The Cybersecurity Higher Education Database (CyberHEAD) by the European Union Agency for Cybersecurity (ENISA) lists altogether five bachelor's and master's degrees related to cybersecurity.

2.4. France

The French white paper on defence and national security (2013) already highlighted the influence of increasing the number of trained information and cybersecurity experts on national security. In addition, it was to be ensured that information and cybersecurity were integrated into higher education in computer science, with the aim of preventing vulnerabilities in information systems and promoting vigilance and response against cyber threats (Poupard, 2016). To achieve these goals, The Agence nationale de la sécurité des systèmes d'information (ANSSI) created the CyberEdu programme, which purpose is to provide resources for cybersecurity training. This activity led to the creation of the CyberEdu association to develop and maintain the original programme and to grant approval to courses. In autumn 2019, CyberEdu published 78 certified training courses (Poupard, 2016).

The national cybersecurity strategy (2015) also highlights the importance of digital security as part of higher education. Higher education institutions should have a training unit dedicated to digital security. Contemporarily, French universities offer several programmes focused on digital and cybersecurity, such as MSc in Cybersecurity (CySec), MSc in Computer Science in Computer Security, and Master in Data & Security Science. According the CyberHEAD database (2023), France is offering 11 different master's degrees and postgraduate courses related to cybersecurity.

2.5. Romania

The Romanian cybersecurity strategy (2021) defines goals and identifies components that are relevant for the functionality of digital services and their safe utilization. The aim is to create a necessary framework for the future development of state administration, the business environment, the national economy, and the education and research sector. The government is investing in the development of education technology as part of the implementation of the Digital Education Action Plan of the European Commission for 2021–27. It has allocated resources for the improvement of digital pedagogical skills, educational resources, and physical and other resources. (Directoratul National de Securitate Cibernetica, n/d.)

In an EU funded Cyber_Education project, Romania's nine largest universities were invited to create common and modern curricula for cybersecurity and educational laboratories. The project was launched by the Bucharest University of Economics, which specialises in training cybersecurity experts. There are 54 public and 35 private universities. Universities specialising in cybersecurity education are Technical University of Cluj-Napoca (n/d) teaching Information and Computing System Security and University Politehnica of Bukharest (n/d) teaching Coding and Storage Theory of Information Master.

2.6. Spain

Spain emphasizes the importance of national cybersecurity culture, which is one of the five main goals and materialized in two of the seven lines of action in Spain's National Cybersecurity Strategy (2019). Cooperation between public and private organizations and the media should be encouraged and strengthen human and technological skills promoting appropriate professional skills. Line of action 5 boosts research, development, and innovation support in digital and cybersecurity programmes, including universities and research centres. It also identifies needs for professional skills in cybersecurity and fostering collaboration between educational and training institutions by enhancing such elements as continuous training and university education. It also pays attention to identifying, encouraging, and retaining cybersecurity talents. Line of action 7 develops cybersecurity culture, such as digital literacy and quality and truthfulness of information. In schools, raising awareness and cybersecurity training are adapted to all levels, fields, and subjects. (Gobierno de Espãna, 2019, 38, 52-53, 56-57).

According to ENISA's CyberHEAD database (2023), cybersecurity is taught in 23 different higher education programmes (one bachelor's programme, while the rest are master's programmes). Spanish National Cybersecurity Institute INCIBE (2021) has listed 168 institutions that provide training in cybersecurity of which 49 are universities. As examples, Barcelona's Ramon Llull University's (2023) Master in Cybersecurity on-site study syllabus includes subjects such as ethical hacking, security analysis, and cyber intelligence. Mondragon University provides a master's degree in data analysis, cybersecurity, and cloud

computing. The studies include ethical hacking, internships in companies, and cybersecurity management. (Mondragon Unibertsitatea, 2018.)

2.7. Greece

Of the five strategic goals in Greece's cybersecurity strategy two (goals 4 and 5) address the ambitions for higher education. For instance, the state will offer support to research and development at the academic level. Such supportive actions include, for example, the reform of curricula to cover more cybersecurity issues and enhanced collaboration between academic and research institutions. One of the main flagship activities is the development of an Education and Awareness Action Plan, which will include an analysis of the current situation and an outline of targeted actions and activities for academic institutions. In relation to academic education, emphasis is given on the preparation of future cybersecurity executives. Suitable undergraduate and postgraduate study programmes are developed, and student attendance is incentivised. (National Cybersecurity Authority, 2020, 63-69.)

Several state universities and private colleges offer studies in cybersecurity. There are 24 universities which are all accredited by the state. Only education given at universities is considered higher education. (Study in Greece, 2023.) The CyberHEAD database lists four universities and five master's programmes (ENISA, 2023). For example, the International Hellenic University offers a master's degree in Cybersecurity, which main topics are digital forensics, intrusion detection and network security, and security audit and compliance (International Hellenic University, n/d). The University of the Aegean has a master's programme in Information and Communication Systems Security. Courses include network security, database security, cryptography, privacy, cybersecurity, and forensics. (University of the Aegean, 2022.)

3. Concluding remarks

Cybersecurity education varies significantly between the EU member states (for the full qualitative and quantitative benchmarking, see Limnéll et al., 2023). Whereas countries like Spain have dozens of higher education institutes teaching cybersecurity, others like Estonia have only a few institutions and educational programmes for the topic. The numbers ought to be contextualised, for example, with the size of the population and hence the estimated national need for expertise. In general, the educational programmes tend to be specific and focus on technical skills. A wider understanding of cybersecurity as a societal concern, civic cybersecurity skills, and discipline geared cybersecurity competence building may be lacking, even if some countries have also integrated these perspectives into curricula. Thus, the educational breadth and depth are to be considered as well. For strengthening civic cybersecurity competence, however, higher education is only a part of the puzzle. Alongside experts, a skilled general population is needed to support secured digitalisation of society.

References

Bundesministerium des Innern und für Heimat (BMI). (2016). Cyber security strategy for Germany. Retrieved February 10, 2023, from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany.

Chen, F., Lyu, J., & Wang, T. (2020). Benchmarking road safety development across OECD countries: An empirical analysis for a decade. *Accident Analysis and Prevention*, 147, 205752. Doi: 10.1016/j.aap.2020.105752.

Directoratul National De Securitate Cibernetică. (n/d). Directoratul National de Securitate Cibernetica. Retrieved November 26, 2022, from dnsc.ro.

European Union Agency for Cybersecurity (ENISA). (2023). Cybersecurity Higher Education Database CYBERHEAD. Retrieved January 31, 2023, from https://www.enisa.europa.eu/topics/education/cyberhead#/.

Gobierno de Espãna, Presidencia del Gobierno. (2019). National Cybersecurity Strategy 2019, 38, 52-53, 56-57. Retrieved January 31, 2023, fromhttps://www.dsn.gob.es/eu/file/2989/download?token=EuVy2lNr.

International Hellenic University. (n/d). MSc in Cybersecurity. Retrieved January 31, 2023, from https://www.ihu.gr/ucips/postgraduate-programmes/cybersecurity.

Lehto, M. (ed.). (2022). Development Needs in Cybersecurity Education: Final report of the project. University of Jyväskylä. Retrieved January 31, 2023, from http://urn.fi/URN:ISBN:978-951-39-9469-3.

Limnéll, J., Alasuutari, M., Candelin, N., Cullen, K., Halonen, O., Helenius, M., Hermunen, T., Lappalainen, J., Latvanen, S., Lindroth, M., Matilainen, T., Palonen, O.-P., Riiheläinen, J., Salminen, M., & Virkkunen, P. (2023). Cyber citizen skills and their development in the European Union. Aalto University. Retrieved April 24, 2023, from https://cyber-citizen.eu/en/materials/.

Maire, J.-L., Bronet, V., & Pillet, M. (2008). Benchmarking: methods and tools for SME. *Benchmarking: An international journal*, 15(6), 765-781. Doi: 10.1108/14635770810915931.

Mondragon Unibertsitatea. (2018). Data Analysis, Cybersecurity and Cloud Compting. Retrieved February 2, 2023, from https://www.mondragon.edu/en/master-degree-data-analysis-cybersecurity-cloud-computing.

National Cybersecurity Authority. (2020). National Cybersecurity Strategy 2020-2025. Ministry of Digital Governance, Hellenic Republic, 63-69.

Poupard, G. (2016). Processus pour l'obtention du label secnumedu. Peremier Ministre. Retrieved February 10, 2023, from https://www.ssi.gouv.fr/uploads/2016/05/anssi-secnumedu-p-01_v2_processus.pdf.

Premier Ministre. (2015). French National Digital Security Strategy. Retrieved February 10, 2023, from https://www.ssi.gouv.fr/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/.

Ramon Llull University. (n/d). Master in Cybersecurity. Retrieved February 1, 2023, from https://www.salleurl.edu/en/education/master-cybersecurity.

Republic of Estonia. Ministry of Economic Affairs and Communications. (2019). Cybersecurity strategy 2019-2022. Retrieved February 10, 2023, from https://ccdcoe.org/library/strategy-and-governance/?category=cyber-security-strategies.

The Security Committee. (2019). Finland's Cyber Security Strategy 2019. Government Resolution 3.10.2019. Retrieved February 6, 2023, from https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/.

Spanish National Cybersecurity Institute (INCIBE). (2021). Instituciones que imparten formación en ciberseguridad en España. Retrieved January 31, 2023, from https://www.incibe.es/sites/default/files/paginas/talento/catalogos-formacion/catalogo-instituciones.pdf.

Study in Greece. (2023). Bachelor's/Master's/PhDs. Retrieved February 1, 2023, from https://studyingreece.edu.gr/studying/studies-taught-gr/bachelors-masters-phds/.

Taltech. (n/d). Cybersecurity (MSc). Retrieved February 2, 2023, from https://taltech.ee/en/cyber-msc.

Technical University of Cluj-Napoca. (n/d). Information and Computing System Security (SISC) – Cybersecurity Master Program at Technical University of Cluj-Napoca. Retrieved November 26, 2022, from utcluj.ro.

Université Bretagne Sud. (n/d). Cyberus Erasmus Mundus Joint Master in Cybersecurity. Retrieved February 2, 2023, from https://master-cyberus.eu/.

University of the Aegean. (2022). Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων. Retrieved January 31, 2023, from https://msc.icsd.aegean.gr/masters/security/.

University Politehnica of Bukharest, Faculty of Applied Sciences. (n/d). Coding and Storage Theory of Information Master, Prezentare. Retrived November 26, 2022, from tcsi.ro.

Universität Des Saarlandes. (2023). Cybersecurity Master of Science, Solving the challenges of today and providing security for tomorrow. Retrieved February 8, 2023, from https://cysec.uni-saarland.de/master/cybersecurity/.