# FRAMEWORK FOR THE EVALUATION OF CYBERSECURITY CURRICULUM EDUCATIONAL CONTENT

**Antti Hakkala, Anne-Maarit Majanoja, Ville Leppänen, Seppo Virtanen**

Department of Computing, University of Turku, Finland

## ABSTRACT

In this research, we define a framework for identifying the educational content of an existing university-level cybersecurity curriculum and aligning it with educational requirements distilled from the combination of the European cybersecurity taxonomy and European Cybersecurity Skills Framework, which identifies distinct role profiles with different educational requirements for cybersecurity professionals. We take the cybersecurity roles and skills frameworks and connect them with the knowledge areas defined in the European cybersecurity taxonomy. As a result, we can clearly identify the necessary knowledge areas for each individual role, and also align them with individual course contents in the cybersecurity curriculum. This makes it possible to identify gaps in existing curricula and ensure that educational content meets the requirements of expected knowledge areas. The developed framework is validated by using it to evaluate an existing university level cybersecurity curriculum at University of Turku, where engineering education curriculum follows the CDIO model. The results are used to identify the gaps in current educational content and to verify that the educational content sufficiently covers the desired role profiles. It is also used to provide input for board level decision-making on cybersecurity education. In addition, the assessment phase also provides important feedback for further development of the framework towards a tool that can be used to shape wider educational policy on cybersecurity education beyond individual universities.

## KEYWORDS

Cybersecurity, Course development, ECSF Framework, ECT Taxonomy, Standards: 3, 7, 8, 12

## INTRODUCTION

Cybersecurity plays a critical role in the fabric of modern society and industry. Recent research has identified a shortage of cybersecurity professionals both in the private and public sectors. In an attempt to accurately assess the current situation in Finland, a recent report by the University of Jyväskylä found that there is a need in Finland for between 6000 and 13000 new cybersecurity professionals in the next few years (Lehto, 2022). This creates and places great expectations on higher education institutions to provide high-quality education in cybersecurity that will lead to skilled cybersecurity professionals in the labour market. Cybersecurity, therefore, needs to be prioritized in education.

At the University of Turku (UTU), a previously identified shortage of cybersecurity professionals

through experience and partners served as an important motivator for developing the existing curriculum and the content of individual courses. The University of Turku's curriculum is largely built on the best understanding of what the course content should include, based on the best judgment of cybersecurity teachers and the industry network. The teaching of the Department of Computing includes CDIO-based approaches and the University of Turku's Information Technology education has been accredited on the basis of EUR-ACE accreditation (UTU, 2022), but accreditation does not include a systematic content review to allow further development of the courses. The curriculum of the University of Turku also meets the requirements of the EIT Digital Master School for Cybersecurity (EIT, 2022) and received the EIT Label in 2023 (EIT, 2023). Yet, there is a clear desire to improve existing courses and curricula in a more systematic way and to identify areas for prioritization or expansion.

Currently, there are no appropriate and effective tools to assess and design a university-level cybersecurity curriculum that also considers the wider societal and sectoral interests related to the role and educational profile of cybersecurity graduates. Such tools are needed to successfully design and implement a curriculum that both meets the societal needs of security professionals and ensures that cybersecurity-specific educational requirements are met. The University of Jyväskylä's report (Lehto, 2022) uses the NIST National Cybersecurity Workforce Framework (NIST, 2020b);(NIST, 2020a) to make a more granular assessment of the professional profile of the new professionals. While the report clearly identifies the need for new professionals and provides an assessment of the estimated numbers for each NIST NCWF category, it lacks the link between what is needed in the workforce and what universities should be teaching to meet this demand. More precise and robust definitions and categories are needed to help design and implement new cybersecurity curricula that are likely to deliver the desired outcomes. This paper provides the missing link between educational content, professional skills, and industry demand. Our approach is not limited to cybersecurity education, as the framework can be applied to other engineering fields with similar existing bodies of knowledge and well-defined professional profiles for industry practitioners. In this case, the general process is the same: extract essential knowledge and competence from the professional profile and map it to course content.

## PREVIOUS WORK

There is currently a high expectation and need to increase the number and skills of cybersecurity professionals. Due to the pressure on universities from different stakeholders, universities must find ways to develop and integrate course contents and curricula to fulfill the requirements on professionalism without increasing credit requirements (Harris & Patten, 2015); (Kans, 2016). Understanding different stakeholders and their demands on education and curriculum content is an important input for curriculum decisions. Previous research has highlighted the importance of teachers and other academic staff having a direct influence on education by defining content and format (Roberts, 2015). In addition, several different approaches have been used to develop course content and curricula. For example, development work has been started to be built through Bloom's taxonomy (Harris & Patten, 2015), accreditation requirements (Knapp, Maurer, & Plachkinova, 2017), program evaluation based on standards (Brink et al., 2020), and in-house development work, surveys for students, teachers, alumni, and companies (Kans, 2016). Knapp et al. (2017) also suggest that the cybersecurity curriculum should include an annual review of key professional certifications and the department

should enable professional certification of teaching personnel (Knapp et al., 2017).

Bloom's taxonomy, accreditations, and internal development activities are good starting points for the development of cybersecurity courses. But the challenge is that these approaches do not lead to a systematic review or development of course content. Other approaches are needed to achieve this. These approaches do not allow for a bridging of the transition from basic studies to working life, for example in the form of future job roles.

*The European Cybersecurity Skills Framework* (ECSF) (ENISA, 2022) is a framework developed by the European Union Agency for Cybersecurity (ENISA). Its purpose is to facilitate the identification of key tasks, skills, knowledge, and competencies for identified cybersecurity professional roles. The stated goals of the ECSF are, paraphrased, to ensure common terminology and shared understanding on cybersecurity between demand and supply sides, support the identification of critical skills from a workforce perspective, facilitate understanding of cybersecurity and essential skills for non-technical experts, harmonization in cybersecurity education, training and workforce development, and a standard structure on capacity building inside the European cybersecurity workforce. The ECSF provides the first European framework and definitions for cybersecurity professionals. There are 12 identified role profiles in the ECSF, and for each profile, the framework identifies required key skills, knowledge, tasks, and competencies. The ECSF Framework is strongly linked to *The European e-Competence Framework (e-CF)*, standard EN 16234-1 (European Committee for Standardization, 2019). The e-CF is is a common European framework for ICT Professional competences, knowledge and skills, which relates to competences needed and applied at the workplace (ENISA, 2022).

SPARTA project used a cybersecurity skills framework to create a free tool called Cybersecurity Curricula Designer (SPARTA, 2022a). The work roles and competencies used in the Curricula Designer reflect the requirements of the Workforce Framework for Cybersecurity (NICE Framework) (SPARTA, 2022b);(NIST, 2020b);(NIST, 2020a). The NICE Framework is developed by the National Institute of Standards and Technology (NIST) that can be used to provide a common lexicon for describing cybersecurity work, workers, and roles for employers. In NICE, cybersecurity is divided into high-level functions known as categories (7), which are further divided into specialty areas (33) and work roles (52). The Cybersecurity Curricula Designer is a web application that can help education providers to create new programs, and analyze existing study programs according to their content and their reflection of cybersecurity job requirements (SPARTA, 2022b). Hajny et al. (Hajny, Sikora, Grammatopoulos, & Di Franco, 2022) have examined the integration of the ECSF into a curriculum designer and thus it is possible to directly link knowledge and skills with the actual 12 professional profiles on the job market. Their work focuses on pairing knowledge and skills to profiles provided by the ECSF in the context of a curriculum designer tool for students. What their approach to the curriculum design tool lacks is the capability to verify that a curriculum covers all essential topic areas for a specified role profile in cybersecurity.

Clearly, there is a need for further methods and/or frameworks to develop the content and to identify gaps in the courses. *The European Cybersecurity Taxonomy (ECT)* (European Commission Joint Research Centre (JRC), 2021) has been developed by the Joint Research Centre of the European Commission as a tool for categorizing institutions and expertise across Europe. It is based on four dimensions: technologies, domains, sectors, and use cases. This taxonomy provides clearer categorizations of topics that are necessary for cybersecurity skills, and can

be used in content design. The ECSF framework and the European Cybersecurity Taxonomy can be enriched by including external resources, e.g., the Cyber Security Body of Knowledge (CyBOK) (University of Bristol Cyber Security Group, 2021). In this paper, we have utilized the domains of the ECSF and the ECT as the set of different aspects and themes within the umbrella term of cybersecurity.

## PLANNING FRAMEWORK FOR CYBERSECURITY CURRICULUM DESIGN

The motivation for our Planning Framework is to help universities to design cybersecurity curricula that successfully delivers the necessary key knowledge and competences for each role profile based on a European standard, rather than NICE or the ACM curriculum guideline for cybersecurity (ACM, 2017), which are based on the US perspective and/or are lacking operational aspects that are rooted in industry. It also implements the key goals of the ECSF: to create an understanding between supply (universities) and demand (industry) in Europe on common terminology, key skills, knowledge and competences. Finally, it enables universities to educate future professionals for roles in proportion to industry demand.

### *Mapping course content and knowledge areas*

The overall process for curriculum evaluation and design is illustrated in Figure 1. Mapping the existing course contents to the ECT categories shows which topic areas are already covered, and also how well the courses cover the whole field of cybersecurity. For a more detailed assessment and overall process development, weights can be added to the mapping based on course level (e.g. basic, intermediate or advanced) and type (e.g. practical vs. theoretical). The assessment of the course content and matching to taxonomy categories is done based on

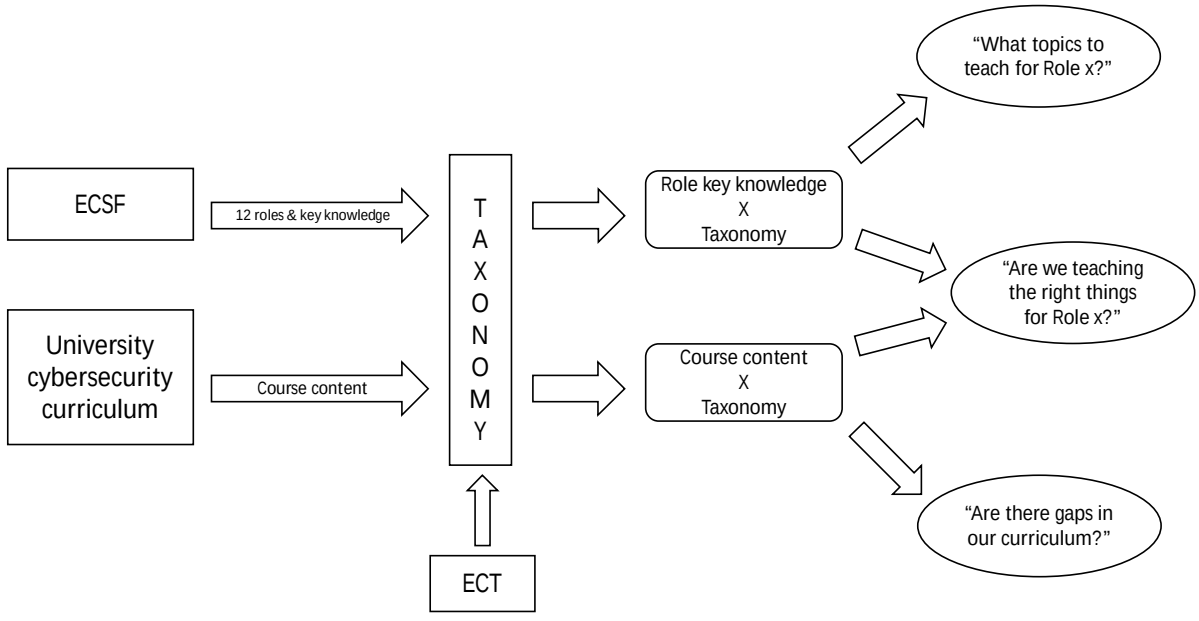


Figure 1. The overall process for incorporating the ECSF roles and key knowledge, ECT taxonomy and university cybersecurity curriculum.

course contents, learning objectives, and an estimation by the responsible teacher.

The mapping between role key knowledge and ECT taxonomy entries is performed next. This process is role dependent, as the perspective on cybersecurity of each role varies depending on the focus, e.g. (attack/defense) and/or abstraction level (hardware/software/architecture/legal).

Each key knowledge entry is matched to taxonomy items by relevance, taking into consideration the differences in focus mentioned above. The result is a nonempty set of matches between knowledge entries and taxonomy items. If the result set is empty, it implies no relevance between the key knowledge and *any* aspect of cybersecurity. This, in our opinion, should not happen when we are considering key knowledge for cybersecurity professionals. This assessment is based on academic and industry experience of the authors.

This process is illustrated in Figure 2. On the left is a general mapping between ECST CISO role's key knowledge areas and the taxonomy. On the right is a mapping between the security management and governance categories of the ECT and a subset of courses offered at the UTU's Department of Computing.

The mapping is challenging to perform due to the size of the resulting spreadsheet. There are twelve roles with between 4 and 15 key knowledge items, each of which need to be mapped to 154 taxonomy entries. We found the most practical way for this mapping to be printing the table on A3 paper and assembling it physically on a large whiteboard (see Figure 3). After the connections between courses and key knowledge areas have been formed via the taxonomy, we can cross-reference between course content and desired knowledge for a specific role through the taxonomy mapping.

| | | 3.1.10. Security management and governance | | | |
|---|---|---|---|---|---|
| | | Standards for Information Security | Governance aspects of incident management, disaster recovery, business continuity | Techniques to ensure business continuity/disaster recovery | Compliance with information security and privacy policies, procedures, and regulations |
| **Role** | **CISO** | | | | |
| CISO | Cybersecurity policies | X | X | X | X |
| | Cybersecurity standards, methodologies and frameworks | X | X | X | X |
| | Cybersecurity recommendations and best practices | | X | X | X |
| | Cybersecurity related laws, regulations and legislations | | X | X | X |
| | Cybersecurity-related certifications | | | | |
| | Ethical cybersecurity organisation requirements | | | | |
| | Cybersecurity maturity models | | | | X |
| | Cybersecurity procedures | | | | |
| | Resource management | | | | |
| | Management practices | | X | X | |
| | Risk management standards, methodologies and framework | | X | X | |

| | Course 1 | Course 2 | Course 3 | Course 4 |
|---|---|---|---|---|
| **3.1.9 Network and Distributed Systems** | | | | |
| Network security (principles, methods, protocols, algorithms and technologies) | | | X | X |
| Distributed systems security | | | | |
| Managerial, procedural and technical aspects of network security | | | | |
| Requirements for network security | | | X | X |
| Protocols and frameworks for secure distributed computing | | | | |
| Network layer attacks and mitigation techniques | | | X | X |
| Network attack propagation analysis | | | | X |
| Distributed systems security analysis and simulation | | | | |
| Distributed consensus techniques | | | | |
| Fault tolerant models | | | | |
| Secure distributed computations | | | | X |
| Network interoperability | | | | |
| Secure system interconnection | | | | |
| Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication) | | | | |
| Network steganography | | | | |
| **3.1.10 Security Management and Governance** | | | | |
| Risk management, including modelling, assessment, analysis and mitigations | X | X | X | X |
| Modelling of cross-sectoral interdependencies and cascading effects | X | | | |
| Threats and vulnerabilities modelling | X | X | | |
| Attack modelling, techniques, and countermeasures (e.g. adversary machine learning) | X | X | | |

Figure 2. Mapping of ECST role key knowledge (left) and existing course content (right) to the ECT taxonomy.

Figure 3. The mapping between ECSF role key knowledge and the ECT entries.

### *Evaluation*

Once the above mapping is complete, we can cross-reference between the key knowledge required in ECSF defined industry roles, and the content of a cybersecurity curriculum, as both are mapped to the ECT. Through this mapping, we can directly assess how well the educational content of the curriculum under evaluation corresponds to the key knowledge defined for a specific role, or a collection of roles, and to identify potential gaps or areas for improvement in course design.

In Figure 4 we assess how well the UTU cyber security curriculum covers the key areas of selected role profiles (Digital Forensics Investigators, Penetration testers, CISOs, and Cyber Incident Responders). The numerical values represent the sum of instances where an aspect of a key knowledge area is covered by courses in the UTU cybersecurity curriculum. The color coding is intended to illustrate the highest (green) and lowest (red) values within each role, while average values are coded as yellow. A key knowledge area that has several matches to different taxonomy entries potentially generates a higher score than one with a single match to

| Role | Key knowledge | |
|---|---|---|
| **Digital forensics investigator** | Digital forensics recommendations and best practices | 11 |
| | Digital forensics standards, methodologies and frameworks | 12 |
| | Digital forensics analysis procedures | 7 |
| | Testing procedures | 4 |
| | Criminal investigation procedures, standards, methodologies and frameworks | 15 |
| | Cybersecurity related laws, regulations and legislations | 10 |
| | Malware analysis tools | 7 |
| | Cyber threats | 4 |
| | Computer systems vulnerabilities | 4 |
| | Cybersecurity attack procedures | 12 |
| | Operating systems security | 37 |
| | Computer networks security | 36 |
| | Cybersecurity-related certifications | 4 |
| **Role** | **Key knowledge** | |
| **Penetration tester** | Cybersecurity attack procedures | 11 |
| | Information technology (IT) and operational technology (OT) appliances | 16 |
| | Offensive and defensive security procedures | 14 |
| | Operating systems security | 39 |
| | Computer networks security | 44 |
| | Penetration testing procedures | 9 |
| | Penetration testing standards, methodologies and frameworks | 10 |
| | Penetration testing tools | 7 |
| | Computer programming | 19 |
| | Computer systems vulnerabilities | 9 |
| | Cybersecurity recommendations and best practices | 17 |
| | Cybersecurity-related certifications | 4 |

| Role | Key knowledge | |
|---|---|---|
| **CISO** | Cybersecurity policies | 61 |
| | Cybersecurity standards, methodologies and frameworks | 55 |
| | Cybersecurity recommendations and best practices | 36 |
| | Cybersecurity related laws, regulations and legislations | 46 |
| | Cybersecurity-related certifications | 7 |
| | Ethical cybersecurity organisation requirements | 16 |
| | Cybersecurity maturity models | 30 |
| | Cybersecurity procedures | 13 |
| | Resource management | 30 |
| | Management practices | 33 |
| | Risk management standards, methodologies and framework | 34 |
| **Role** | **Key knowledge** | |
| **Cyber Incident Responder** | Incident handling standards, methodologies and frameworks | 22 |
| | Incident handling recommendations and best practices | 16 |
| | Incident handling tools | 13 |
| | Incident handling communication procedures | 16 |
| | Operating systems security | 74 |
| | Computer networks security | 66 |
| | Cyber threats | 17 |
| | Cybersecurity attack procedures | 10 |
| | Computer systems vulnerabilities | 13 |
| | Cybersecurity-related certifications | 4 |
| | Cybersecurity related laws, regulations and legislations | 5 |
| | Secure Operation Centres (SOCs) operation | 18 |
| | Computer Security Incident Response Teams (CSIRTs) operation | 18 |

Figure 4. Evaluation of UTU cybersecurity curriculum contents matching against four selected roles in the ECSF through matching key knowledge to course contents.

a taxonomy entry. Therefore, the scores are not comparable between roles, as the same key knowledge can have different meanings for different roles, due to the individual mapping of role key knowledge to taxonomy entries.

From the results we observe that our strengths are in computer network and operating system security, which are the strongest areas for three out of four roles. This is an expected result, as many of our existing courses focus on these areas. Similarly, for the more managerial CISO role, our courses provide a good knowledge of policy, standards and recommendations. This is also an expected result. On the weaker aspects, the evaluation confirms our initial assessment that the program lacks hands-on procedures for incident responders, forensics investigators and penetration testers. Observed knowledge gaps for these roles include cybersecurity procedures, vulnerabilities from the defensive perspective, use of tools, ethical issues, and cybersecurity certifications.

For example, we can observe that for forensic investigators, the category "Cyber threats" receives a score of 4, while for incident responders the score is 17. This does not mean that the curriculum does not cover cyber threats, but rather that the specific aspects of forensic investigators are not covered. Given the strong signal from previous research that more cyber incident responders are needed, improving the educational content in this category would be worthwile.

## DISCUSSION

The global shortage in cybersecurity professionals that has been identified by many researchers and analysts can be further pigeonholed into more precise demand for new talent in specific roles. The ECSF roles provide the connection between industry needs and cybersecurity education planning. By leveraging the ECSF it is possible to design cybersecurity education with the desired impact on the level of an individual programme, a single university, or a group of universities seeking to coordinate their educational profiles. The reason for incorporating the ECT in the process is to use a common European foundation and understanding of cybersecurity domains at the core of the framework.

Curriculum design is not an exact science, and we do not advocate that it should only follow mechanical procedures and constraints. The expertise and intuition of the teacher designing the curriculum and the capability to leverage limited resources for the best possible outcome remain vital to a successful cybersecurity education programme. However, we do advocate the use of well-defined processes and frameworks to both help with the design of new a curriculum, and to act as a sanity check for existing ones. Our framework provides a systematic approach to verify and control that an existing curriculum contains the necessary topics at the necessary depth for graduates to operate in industry.

A key finding from the curriculum analysis is that cybersecurity certification is a core knowledge and competence in many roles, but current curricula are not sufficient to provide certifications to university students. University-industry cooperation can help to provide technology or vendor-specific certifications to students (Hakkala & Virtanen, 2012), but given the importance of certifications in the field and the emphasis on certifications in life-long learning in cybersecurity, universities should be able to provide both more information on certifications to students, and

perhaps even early career certifications (Majanoja, Hakkala, Virtanen, & Leppänen, 2023).

We also observed that in our opinion, certain roles lacked key knowledge areas: those working in a CISO or cybersecurity risk manager role can benefit from the legal aspects of cybersecurity, but this was not included as a key knowledge area. Another observation we made was that some role profiles can benefit from multidisciplinary degree programmes or even complete second degrees, as for example cyber legal, policy and compliance officers are more likely than not to be lawyers rather than engineers or computer scientists. This provides multidisciplinary universities an edge in providing education that can meet the demands of today's world.

*Future work.* For each key knowledge area within a role, the ECSF also defines a competency level based on the e-Competency standard. In this version of our framework, the effects of these levels is not yet considered. It is also open to debate how universities can provide deeper competences (up to e-4 and e-5), which in practice requires extensive work experience and practice to attain. The perception of industry on what the competence level of fresh graduates should be, and what is realistically attainable in higher education do not necessarily match. There is existing research on industry expectations based on job advertisements, but as the nature of the job market varies between countries, a holistic view is difficult to form. A mapping of industry actor expectations and requirements to the framework established in this paper will be explored in future research.

Through our framework is is possible to integrate the CDIO standards and practices into the core of curriculum development. Through the integration of e-CF we can identify key competences in cybersecurity and map them to course content. Similarly we can identify core CDIO skills and principles from these competences and integrate them to the curriculum already at the design phase, thus fulfilling the goals of standard 3. After we have identified these skills and principles, the framework facilitates synergies between industry and universities by integrating industry partners into teaching those skills to students in the necessary context.

When implementing the curriculum in the form of courses, active learning methods can be conveniently mapped to individual topics, competences and themes from the framework. The advantage of our approach is that when there is a clear mapping between competences, topics and roles, the learning methods for conveying subject information according to CDIO principles are easier to determine.

The integration of CDIO standards into the framework provides the opportunity to thoroughly analyze each educational topic and determine the best way to arrange the teaching for each course. Having such a structured tool for curriculum design also provides a tool for communicating to stakeholders and implementing forms of continuous follow-up and improvement of the curriculum.

The accumulation of competences is also influenced by the organization of the teaching: how much is hands-on practice with industry standard tools and programs, and how much is purely theoretical? In Finland, universities of applied sciences have traditionally focused more on tool-specific hands-on exercises and problem-based learning, while university teaching is more grounded in theory, complemented by more generic practical exercises. However, the issues identified in cybersecurity higher education are present in both. More research is needed in this area.

When discussing higher education policy at national level, the level of abstraction is above individual courses or even curricula. In public discussion, the focus is on "cybersecurity professionals" and their perpetual shortage. Our aim is to use this framework in a national development project on cybersecurity capabilities and the division of responsibilities between different universities in Finland. A project for this purpose, funded by the Ministry of Education and Culture, has started in late 2022. Our contribution to this project will be based on the framework presented in this paper, enhanced with the aspects of the e-Competency standard.

## CONCLUSION

The goal of the curriculum design framework is twofold. First, it facilitates the design of better cybersecurity curricula by providing a tool with which we can verify that an existing curriculum indeed is focused on the desired aspects, technologies and topics that correspond to the desired professional profile of graduates from the degree programme. Second, it facilitates a systematic approach to building a new cybersecurity education programme at university level that provides graduates with a professional profile desirable to the wider industry.

The framework presented in this paper serves as a starting point for defining education profiles for universities. Once the desired education profiles have been selected, the framework can be used to analyze an existing curriculum to see how well it meets the requirements of each professional role profile, and to identify potential gaps in content that need to be addressed. The content, structure, and organization of studies can vary considerably between universities and degree programmes. This framework makes it possible to benchmark cybersecurity degree programmes against those of other universities.

## FINANCIAL SUPPORT ACKNOWLEDGEMENTS

The author(s) received no financial support for this work.

## REFERENCES

ACM. (2017). *Curriculum guidelines for post-secondary degree programs in cybersecurity.* Available onilne at https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf, Accessed 14.04.2023.

Brink, S., Carlsson, C. J., Enelund, M., Georgsson, F., Keller, E., Lyng, R., & McCartan, C. (2020). *ASSESSING CURRICULUM AGILITY IN A CDIO ENGINEERING EDUCATION | Worldwide CDIO Initiative.* Retrieved 2023-01-26, from http://cdio.org/knowledge-library/documents/assessing-curriculum-agility-cdio-engineering-education

EIT. (2022). *EIT Digital Master School - Cyber Security // EIT Digital Master School.* Retrieved 2023-01-27, from https://masterschool.eitdigital.eu/cyber-security

EIT. (2023). *Decision 02/2023 of the Director of the European Institute of Innovation and Technology on awarding the EIT Label to masters and doctoral programmes.* Ref.Ares(2023)321702 - 16/01/2023.

ENISA. (2022). *European Cybersecurity Skills Framework.* Available online at https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework, Accessed 18.01.2023.

European Commission Joint Research Centre (JRC). (2021). *European Cybersecurity Taxonomy.* Available online at https://cybersecurity-atlas.ec.europa.eu/cybersecurity-taxonomy, Accessed 18.01.2023.

European Committee for Standardization. (2019). SFS-EN 16234-1 : 2019 : en ( e-CF ). A common European Framework for ICT Professionals e-Competence Framework ( e-CF ). A common European Framework.

Hajny, J., Sikora, M., Grammatopoulos, A. V., & Di Franco, F. (2022). Adding european cybersecurity skills framework into curricula designer. In *Proceedings of the 17th international conference on availability, reliability and security.* New York, NY, USA: Association for Computing Machinery. Retrieved from https://doi.org/10.1145/3538969.3543799 doi: 10.1145/3538969.3543799

Hakkala, A., & Virtanen, S. (2012). University-industry collaboration in network security education for engineering students. In *Proceedings of the International Conference on Engineering Education ICEE 2012, University of Turku, Turku, Finland, 30.7.–3.8.2012,.*

Harris, M., & Patten, K. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computic Curriculum. *Journal of Information Systems Education*, *26*(3). Retrieved from https://aisel.aisnet.org/jise/vol26/iss3/4

Kans, M. (2016). *What Should we Teach? A Study of Stakeholders' Perceptions on Curriculum Content | Worldwide CDIO Initiative.* Retrieved 2023-01-26, from http://www.cdio.org/knowledge-library/documents/what-should-we-teach-study-stakeholders-perceptions-curriculum-content

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education*, *28*(2), 101.

Lehto, M. (Ed.). (2022). Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti. *Informaatioteknologian tiedekunnan julkaisuja*(93). Retrieved from https://jyx.jyu.fi/handle/123456789/82709

Majanoja, A.-M., Hakkala, A., Virtanen, S., & Leppänen, V. (2023). Motivation for continuous software engineering expertise development through lifelong learning. In *Submitted to the 19th International CDIO Conference, hosted by NTNU, Trondheim, Norway, June 26—29, 2023.*

NIST. (2020a). *NICE Framework Supplemental Material.* Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-supplemental-material.

NIST. (2020b). *NIST Special Publication 800-181 Revision 1: Workforce Frame-work for Cybersecurity (NICE Framework). ht.* Retrieved 2023-01-26, from https://nlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Roberts, P. (2015). Higher education curriculum orientations and the implications for institutional curriculum change. *http://dx.doi.org/10.1080/13562517.2015.1036731*, *20*(5), 542–555. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/13562517.2015.1036731

SPARTA. (2022a). *Curricula Designer.* Retrieved 2023-01-26, from https://www.sparta.eu/curricula-designer/

SPARTA. (2022b). *SPARTA - Cybersecurity Training and Awareness.* Retrieved 2023-01-26, from https://www.sparta.eu/training/

University of Bristol Cyber Security Group. (2021). *CyBOK – The Cyber Security Body of Knowledge.* Retrieved 2023-01-26, from https://www.cybok.org/

UTU. (2022). *Tietotekniikan tutkinto-ohjelmille EUR-ACE -akkreditointi | Turun yliopisto.* Retrieved 2023-01-27, from https://www.utu.fi/fi/ajankohtaista/uutinen/tietotekniikan-tutkinto-ohjelmille-eur-ace-akkreditointi

## BIOGRAPHICAL INFORMATION

**Antti Hakkala** is a University Teacher (D.Sc (Tech.)) in Communication Systems and Cyber Security at Department of Computing, University of Turku, Finland. Hakkala has over 10 years' experience in teaching engineering students on cyber security and communication systems engineering, and he has supervised over 100 Bachelor's and Master's theses. His reserach interests are centered around various cyber security topics, security and privacy in the networked information society, biometrics and biometric passports, cryptography, and security design in hardware, software and networks.

**Anne-Maarit Majanoja** is a University Teacher (PhD) in software engineering at the Department of Computing, University of Turku, Finland. Majanoja has more than a decade of work experience in the industry and her work experience has equipped her with an in-depth knowledge of global IT development and services, quality management, leadership, and logistics and supply chain environments. Majanoja has also worked for several years in the development and implementation of lifelong learning courses and content at the University of Turku. Her current research interests include: quality management, process development, global IT outsourcing, leadership and change management, and IT education and lifelong learning.

**Ville Leppänen** is a Professor in software engineering and software security at the Department of Computing, University of Turku, Finland. At the moment, he is also vice dean of Faculty of Technology. He has now over 230 international conference and journal publications. His research interests are related broadly to software engineering and security, ranging from software engineering methodologies, practices, and tools to security and quality issues, as well as to programming languages, parallelism, and architectural design topics. Leppänen is a member in several boards and working groups in University of Turku and outside the university.

**Seppo Virtanen** is a Professor in Cyber Security Engineering and Vice Head of Department of Computing, the University of Turku, Finland. He is a Senior Member of the IEEE. He has taught more than 70 instances of 23 different university courses to engineering students as principal instructor. His current research interests are on cyber security in smart environments, secure network and communication technology and security technologies for IoT.

***Corresponding author***

Antti Hakkala
University of Turku
Dept. of Computing
20014 UNIVERSITY OF TURKU
Finland antti.hakkala@utu.fi