CYBERSECURITY EDUCATION

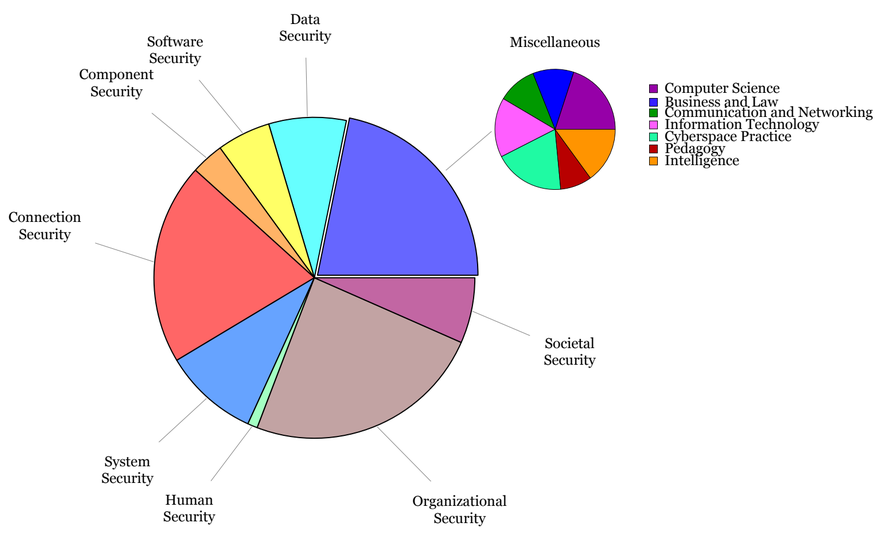
Harri Kähkönen
harri.kahkonen@helsinki.fi
Valtteri Niemi
valtteri.niemi@helsinki.fi
Department of Computer Science,
University of Helsinki, Finland

b

CYBERSECURITY EDUCATION DEVELOPMENT

Prior work: Ramezanian and Niemi [4] demonstrated how their measurement system can be used to develop a cybersecurity curriculum that aligns with workforce needs and supports lifelong learning for professionals.

Lehto et al. [2] determined weights for the 7 Job Categories defined in the NICE Framework [3]. Based on these weights, Ramezanian and Niemi [4] derived the relative importance of Knowledge Areas (KAs) and Knowledge Units within the curriculum as defined in Cybersecurity Curricula 2017 (CSEC) [1]. Using this structure, they mapped Knowledge Descriptions from the NICE Framework to the corresponding Knowledge Units.



Weight distribution of the Knowledge Areas based on their importance to cybersecurity work role competences.

In March 2025, the NICE Framework was updated with revised Knowledge Descriptions. To map the new descriptions to Knowledge Areas, we utilized the `gpt-4o-mini` large language model via an OpenAI API. Together with University of Lund, we are currently comparing the language model's mappings with those made by human participants to evaluate consistency and potential differences.

PARTICIPATE IN OUR STUDY!

Please help us. For each of the three randomly chosen specific knowledge descriptions from the NICE framework, decide which broader knowledge area(s) of the CSEC curriculum it belongs to. You may select more than one area if applicable.

Please allocate each of the below three **specific** descriptions of knowledge to the **wide** knowledge areas (0–8) listed in the bottom part.

C	Knowledge of reverse engineering tools and techniques	
D	Knowledge of data encryption practices and principles	
N	Knowledge of data concealment tools and techniques	

Knowledge Areas

1. DATA SECURITY
Basic cryptography concepts, Digital forensics, End-to-end secure communications, Data integrity and authentication, Information storage security.

2. SOFTWARE SECURITY
Fundamental design principles, Security requirements, Implementation issues, Static and dynamic testing, Configuring and patching, Ethics.

3. COMPONENT SECURITY
Vulnerabilities of system components, Component lifecycle, Secure component design principles, Supply chain management security, Security testing, Reverse engineering.

4. CONNECTION SECURITY
Systems, architecture, models, standards, Physical component interfaces, Software component interfaces, Connection attacks, Transmission attacks.

5. SYSTEM SECURITY
Holistic approach, Security policy, Authentication, Access control, Monitoring, Recovery, Testing, Documentation.

6. HUMAN SECURITY
Identity management, Social engineering, Awareness and understanding, Social behavioral privacy and security, Personal data privacy and security.

7. ORGANIZATIONAL SECURITY
Risk management, Governance and policy, Laws, ethics, and compliance, Strategy and planning.

8. SOCIETAL SECURITY
Cybercrime, Cyber law, Cyber ethics, Cyber policy, Privacy.

0. MISCELLANEOUS
Includes: Computer Science, Business and Law, Communication and Networking, Information Technology, Cyberspace Practice, Pedagogy, Intelligence.

Participant form for mapping NICE Knowledge Descriptions to CSEC Knowledge Areas. Ask for a form and a pen to participate in the study.

NATIONAL CYBERSECURITY EDUCATION NETWORK PROJECT

The project enhances collaboration between Finnish universities to develop research-based cybersecurity education and broaden study opportunities. It is coordinated by the University of Jyväskylä, with Turku, Helsinki, Vaasa, Oulu, Åbo, Tampere, Aalto, and LUT as partners. It is funded by the Ministry of Education and Culture, Finland.

[1] Joint Task Force on Cybersecurity Education (JTF). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. `https://cybered.hosting.acm.org/wp/`. 2017.

[2] M. Lehto, ed. *Development Needs in Cybersecurity Education: Final Report of the Project*. Informaatioteknologian tiedekunnan julkaisuja 96. URN:ISBN:978-951-39-9469-3. Jyväskylän yliopisto, Informaatioteknologian tiedekunta, 2022.

[3] R. Petersen et al. *Workforce framework for cybersecurity (NICE framework)*. Tech. Rep. National Institute of Standards and Technology, 2020.

[4] Sara Ramezanian and Valtteri Niemi. "Cybersecurity Education in Universities : A Comprehensive Guide to Curriculum Development". English. In: *IEEE Access* 12 (May 2024). Publisher Copyright: © 2013 IEEE., pp. 61741–61766. ISSN: 2169-3536. DOI: `10.1109/ACCESS.2024.3392970`.

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI
MATEMAATTIS-LUONNONTIETEELLINEN TIEDEKUNTA
MATEMATISK-NATURVETENSKAPLIGA FAKULTETEN
FACULTY OF SCIENCE