



Consolidating cybersecurity in Europe: A case study on job profiles assessment[☆]



Carlos E. Budde^{a,1,*}, Anni Karinsalo^{b,1}, Silvia Vidor^{a,1}, Jarno Salonen^c, Fabio Massacci^{a,d}

^a University of Trento, Trento I-38121, Italy

^b VTT Technical Research Centre, Oulu FI-90571, Finland

^c VTT Technical Research Centre, Tampere FI-33101, Finland

^d Vrije Universiteit Amsterdam, Amsterdam, 1081 HV, The Netherlands

ARTICLE INFO

Article history:

Received 16 July 2022

Revised 22 November 2022

Accepted 24 December 2022

Available online 28 December 2022

Keywords:

Cybersecurity

Professional skills

Assessment framework

Education

ABSTRACT

To address the issue of educating and training new experts in cybersecurity, it is crucial to identify the specific educational needs of the various professions that exist in the field. We measure these needs by analysing six cybersecurity-related job profiles—each with its own specific skill requirements—that have been assessed by academic and industrial organisations from the cybersecurity community in 14 European countries. We find that it is possible to identify a series of “transversal” skills relevant to all job profiles, and thus of utmost importance in the cybersecurity curricula. However, we also observe that academic and industrial priorities differ substantially, and that skills related to the area of Human security do not rank particularly high, possibly exposing the difficulty of integrating such concepts in traditional education.

© 2023 The Author(s). Published by Elsevier Ltd.

This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>)

1. Introduction

Cybersecurity occupations have been facing a persistent shortage of staff for years (Nurse et al., 2021). It is thus crucial to educate and train new experts, which in turn requires to understand the specific educational needs of the various cybersecurity professions—since it is neither feasible nor realistic to require complete expertise in all the different areas of the field.

The European Union has already set in motion several initiatives to address the staff shortage, such as the Digital Europe programme for training SMEs and public administration (Bahrke and Grammenou, 2021; European Commission, 2021). But beyond training the current workforce, the selection of key skills is crucial to design a much-needed *educational curricula for cybersecurity careers*.

The need for professional cybersecurity education is almost a decade old, viz. since the US National Science Foundation asked

the ACM's Education Board to help reshape cybersecurity education (McGettrick, 2013). But while the professional needs in the US are well understood—from the seminal plans (McDuffie and Piotrowski, 2014) to the interview of professionals on their own needs (Armstrong et al., 2020), or the analysis of cybersecurity for non-technical majors (Nodeland et al., 2019)—the work in other countries is less discussed.

For example: the development in the Arabic regions is briefly reported in Alsmadi and Zarour (2018); cybersecurity education in Ecuador and South Africa is overviewed respectively in Catota et al. (2019) and Kortjan and von Solms (2013); and the role of Singapore in the ASEAN cybersecurity arena is described in Ang (2021). Most studies are surveys and/or comparisons against the state of the art in developed countries (usually just the US), with limited applicability to implement teaching curricula. Comparatively, Europe is even less well covered—with the exceptions of Crick et al. (2019) for the UK, and Dragoni et al. (2021) on formal cybersecurity education in Europe, which will be the basis for our study. Hence, *this work is focused on cybersecurity skills for professional needs*.

Research questions We carry out our studies to answer the main research question: *which skills should be covered by European curricula to satisfy the current and future needs in cybersecurity?* We split that question into the following sub-questions to better structure our research:

[☆] This work was funded by the European Union grant 830929 (H2020-CyberSec4Europe), and GA n° 101067199-ProSVED. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or The European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

* Corresponding author.

E-mail address: carloseteban.budde@unitn.it (C.E. Budde).

¹ First authors are alphabetically ordered on last names.

- RQ1 Which are the most relevant skills to teach and perform in cybersecurity-related jobs?
- RQ2 Is the (control of the) human factor regarded as a formal requirement in cybersecurity education and training?
- RQ3 Are there different perceptions in the relevance of skills:
- (a) from the perspective of professionals (in the industrial sector) vs. educators (in the academic sector)?
 - (b) that correlate to the job profile type, e.g. managerial vs. technical?

Methodology

Our focal contribution is on analysing educational needs of European organisations regarding cybersecurity. We approach this by selecting six cybersecurity-related job profiles, reviewed by experts to assess the specific skill requirements for each of them. From such assessments, we further compare the differences in priorities perceived by organisations representing academia and industry, and we study the different type of skills that are deemed necessary to perform in technical or managerial occupations.

To answer our questions, we designed and distributed surveys across different European stakeholders from the academic and industrial sectors, gathering $n = 60$ expert assessments. The surveys consisted of an evaluation of six cybersecurity job profiles, selected from material presented to the European Commission by special bodies dedicated to that task (European Commission, 2022; European Cyber Security Organisation, 2021). To evaluate the job profiles, the assessors had to choose the relevance of predefined cybersecurity skills to perform in each job. These skills—55 in total—come from standard frameworks for the assessment of cybersecurity capabilities (Karinsalo and Halunen, 2021; Dragoni et al., 2021; European Cyber Security Organisation, 2021; Joint Task Force on Cybersecurity Education, 2018; Nai-Fovino et al., 2019; Petersen et al., 2020; The National Cyber Security Centre, 2019). We briefly describe the chosen framework in Section 2 (Karinsalo and Halunen 2021; Dragoni et al. 2021).

Thus, in our surveys, each respondent assessed the relevance of each skill for the selected job profiles. For instance, to perform as Security Engineering, assess how relevant are the skills *Digital Forensics*, *System Testing*, *Cyber Policy*, etc. The results of these assessments are then analysed and used to answer our research questions. The detailed steps and sources that comprise and underpin the whole study are explained in Section 3.

Our surveys were conducted within the scope of *CyberSec4Europe* (CS4E Cyber Security for Europe, 2018), one of the four H2020 pilot projects that are paving the way to the European Cyber Competence Network (CCN European Cyber Competence Network, 2022). Besides using the network of CS4E, we resorted to the education focus group of the CCN² to extend the reach of our study.

Outline This work is structured as follows: Section 2 briefly reviews the cybersecurity frameworks and related work relevant to our study Section 3 presents our approach in detail, including the strategic choices of job profiles, the use case and scenario, and the technology and layout used for the surveys Section 4 presents the results of the study, and discusses their implications with respect to the research questions Section 5 concludes the work, and draws possible lines of improvement and future research.

2. Assessment frameworks

This section briefly presents the theoretical background of the paper: what is meant by assessment framework for cybersecurity,

the related work and corresponding standards, and the details of the framework used in this work.

2.1. Standards, curricula, and frameworks

By *assessment framework* for job profiles we mean a reference curriculum used—e.g. by practitioners in the cybersecurity field—to define the professional skills needed to perform in specific work positions, as well as their required degree of expertise (Petersen et al., 2020). This builds on top of a taxonomy of skills or subjects on the field of interest, augmented with their relevance—for each work position considered—via an expert-driven assessment (Karinsalo and Halunen, 2021; Nai-Fovino et al., 2019).

There is more than one assessment framework for each domain or field of study, that classifies and assesses the skills for its intended context of application (Nai-Fovino et al., 2019). Each of these frameworks is usually linked to a major research, educational, or industrial environment, the priorities of which are expressed in the resulting classification. We have identified the following frameworks, taxonomies, and curricula for the general cybersecurity domain:

- CSEC** - the *Cybersecurity Curricular Guidelines*, by the ACM (Joint Task Force on Cybersecurity Education, 2018).
- CWF** - the *Cybersecurity Workforce Framework*, by the NIST (Petersen et al., 2020).
- ECT** - the *European Cybersecurity Taxonomy*, by the JRC (Nai-Fovino et al., 2019).
- CyBOK** - the *Cyber Security Body of Knowledge*, by the National Cyber Security Centre of the UK (The National Cyber Security Centre, 2019);
- MRC** - the *Minimum Reference Curriculum* for European Cybersecurity Education and Professional Training, by ECSO (European Cyber Security Organisation, 2021).

These cases stand out due to the broadness of their scope, and the well-established international institutions that produced them. Moreover, their different perspectives are complementary: CSEC is aimed at structuring academic curricula, while CWF and MRC focus on professional training and workforce skills. In turn, CyBOK structures mainly scientific knowledge—rather than pedagogical approaches—while ECT is mostly focused on research for technological development.

International standards Usually, one or several standards underpin the definition of the skills/subjects that appear in a framework. For example, various ISO standards were consulted in Nai-Fovino et al. (2019) to define the ECT, perhaps most notably ISO/IEC 27000 ISO/IEC 27000:2016 (2016). Similarly, CWF was originally released by the NICE partnership of NIST in 2017, in its Special Publication 800-181 (NIST.SP.800-181 Petersen et al., 2020). Several cases from the list above refer to NIST as a source for their own classifications, e.g. CSEC, CyBOK, ECT, MRC, and the Educational and Professional Framework developed by CS4E (Karinsalo and Halunen 2021; Dragoni et al. 2021). In turn, the ACM classification system is a source of its own—e.g. it was used by the MRC—also closely related to the Institute of Electrical and Electronics Engineers (IEEE) taxonomy. Thus, CSEC lists ACM/IEEE CS2013 and ACM/IEEE IT2017 among the sources used to define their curricula (Joint Task Force on Computing Curricula et al., 2013; Task Group on Information Technology Curricula et al., 2017).

2.2. The CSEC⁺ framework

Although complementary, the multiple perspectives of the frameworks, taxonomies, and curricula listed above result in a significant overlap of concepts and terminology. Furthermore, only

² <https://cybercompetencenetwork.eu/focus-groups/education-focus-group/>

Data Security (8) Cryptography Digital Forensics Data Integrity and Authentication Access Control Secure Communication Protocols Cryptanalysis Data Privacy Information Storage Security	Human Security (7) Identity Management Social Engineering Personal Compliance with Cybersecurity Rules/.../Policy/Ethical Norms Awareness and Understanding Social and Behavioral Privacy Personal Data Privacy and Security Usable Security and Privacy	System Security (7) System Thinking System Management System Access System Control System Retirement System Testing Common System Architectures
Software Security (7) Fundamental Principles Design Implementation Analysis and Testing Deployment and Maintenance Documentation Ethics	Connection Security (8) Physical Media Physical Interfaces and Connectors Hardware Architecture Distributed Systems Architecture Network Architecture Network Implementations Network Services Network Defense	Organizat. Security (9) Risk Management Security Governance and Policy Analytical Tools Systems Administration Cybersecurity Planning Business Continuity, Disaster Recovery, and Incident Management Security Program Management Personnel Security Security Operations
Component Security (4) Component Design Component Procurement Component Testing Component Reverse Engineering	Societal Security (4) Cybercrime Cyber Law Cyber Policy Privacy	Operate & Maintain (1) Customer Service and Technical Support

Fig. 1. Knowledge areas and units in the CSEC⁺ framework.

the MRC, which was published in November 2021, and partially based on the CSEC, describes subjects that connect education curricula to cybersecurity careers in Europe. Finally, all cases were designed as classification—as opposed to assessment—frameworks, i.e. without a scale to measure the degree of relevance of a subject or skill for a work position.

These are the main reasons why we conducted studies in 2020–2021 to define an *educational and professional assessment framework* focused on modern-day cybersecurity in Europe (Karinsalo and Halunen, 2021; Dragoni et al., 2020). The framework developed in that context—henceforth **CSEC⁺**—was designed for job profiles assessment, in connection to cybersecurity university curricula based on current world standards. The taxonomy adopted in CSEC⁺ to classify the skills is aligned with university curricula, more precisely the division in knowledge areas and units proposed in CSEC (Dragoni et al., 2021; Joint Task Force on Cybersecurity Education, 2018). Moreover, CSEC⁺ maps these subjects to the workforce classification presented in CWF by NIST, thus connecting the university output to the needs of the industrial sector (Karinsalo and Halunen, 2021; Dragoni et al., 2021).

The result is a broad classification in nine knowledge (security) areas: *Data*, *Software*, *Component*, *Connection*, *System*, *Human*, *Organizational*, *Societal*, and *Operate and Maintain*. Each area is then sub-divided into knowledge units, e.g. cybercrime, cyber law, cyber policy, and privacy are in the area of Societal security. We list all areas and units of CSEC⁺ in Fig. 1 and Appendix A—these were initially presented in Dragoni et al. (2021, 2020).

In this sense, CSEC⁺ follows quite closely the classifications of CSEC and CWF. In the following, when referring to the CSEC⁺ framework, we use the terms *skill* to indicate (any) one of its knowledge units, and *area* to indicate a knowledge area.

2.3. Job profiles assessment

A distinguishing feature between CSEC⁺ and all previous frameworks is its definition of a scale, used to indicate the degree to which each skill is relevant for a specific job profile. This allows CSEC⁺ to be used for assessment: for each knowledge unit, assessors of a work position can select the degree to which that unit is relevant for the job.

The Likert scale defined in CSEC⁺ consists of four steps that go from irrelevant to essential as follows:

0. **Irrelevant:** The skill or knowledge is not necessary to perform in the given specialization.
1. **Basic Knowledge:** Understanding the basic principles of the skill or knowledge is needed in the specialization. Application of these is not necessary to perform in the specialisation.
2. **Intermediate Knowledge:** Applying the skill or knowledge is needed to perform in the specialization. Such application is only needed up to the point of well-known (possibly de facto) standard procedures.
3. **Advanced Knowledge:** Applying the skill or knowledge is essential to perform in the specialization. The application of the skill or knowledge is necessary on an advanced level and beyond well defined standard procedures.

Using this scale, independent subjects—known as assessors—can evaluate the needs and requirements of a job profile in terms of abilities and knowledge. To do so, the assessors are presented with a description of the profile and a list of skills, and they must determine the relevance of each skill to perform the job. The list of skills is generally determined relative to the topic of interest for the assessment. These skills are evaluated for relevance on a scale from some minimum (skill not necessary for the considered job) to some maximum value (essential skill for the considered job), as in the Likert scale of CSEC⁺.

In order to help the assessors understand the nature of the job profile under assessment, e.g. avoiding any possible ambiguity due to the existence of similar job titles, it is useful to provide context in the form of a use case. A *use case* is a textual description of a situation or company in which the job is exercised: for example, the operations of a European bank in compliance to the Revised Payment Services Directive (PSD2) (Council of the European Union and European Parliament, 2015), or migration control in an international airport.

With the intention to mirror real-life scenarios, each use case typically covers several job profiles that interact with each other in the given context. Several interaction scenarios can be defined within a single use case: for instance, opening a private customer account in a bank, or performing international payment transactions. The goal of these descriptions is to better define the situations in which the job profile is expected to operate.

Thus, use case and scenarios help assessors to interpret the skills that the worker should possess, by providing them with a concrete situation in which skills are needed. However, this may also constrain the scope of the assessments—Section 5 discusses the issue.

Finally, and although the exception rather than the rule, we note that the definition of some job profiles is already narrow enough to permit its assessment outside of any use case. For example, cybersecurity auditors (European Cyber Security Organisation, 2021) may be expected to have basically the same tasks independently from the specific company they work in.

Assessment example Four skills from CSEC⁺ are *Information Storage Security*, *Cryptography* (these correspond to the Data security area), *Identity Management* (corresponding to Human security), and *Customer Service and Technical Support* (corresponding to Operate and maintain). An assessment based on these skills for the position of Technical Cybersecurity Auditor could be:

1. *Information Storage Security*: advanced knowledge (3).
2. *Cryptography*: intermediate knowledge (2).
3. *Identity Management*: basic knowledge (1).
4. *Customer Service*: irrelevant (0).

3. Approach and use case

For the assessment in our study we use CSEC⁺, which includes the skills shown in Fig. 1, and whose discrete assessment scale goes from level zero (irrelevant) to level three (advanced) as described above. More in detail, we gathered expert knowledge from the European cybersecurity community to give representative answers to our research questions. For this, we designed surveys in which the respondents employed the CSEC⁺ framework to assess the skills needed to perform in six job profiles. The profiles were selected in merit of their relevance for the current and future needs of cybersecurity in Europe.

This section provides detailed information about the target groups and dissemination of the survey (Section 3.1), its structure and the technology used to gather the responses (Section 3.2), the six job profiles distributed for the expert assessment (Section 3.3), and the categorical division that guided the profiles selection (Section 3.4).

3.1. Target groups and dissemination of the surveys

Our survey data was collected in three phases. The first phase was used partly as a pilot, intended to collect initial data while at the same time determine the steps to make a larger-scale dissemination feasible.

This phase took place between October 2021 and January 2022, and it targeted partners from the CS4E project. The dissemination methodology was semi-formal, consisting in intra-CS4E announcements and subsequent communication via private e-mails. In these e-mails the survey was provided to the respondents as a worksheet, with descriptions and detailed instructions about the CSEC⁺ framework and the job profiles to assess.

The results of the first phase—provided by 13 respondents from Finland, Italy, Slovenia, and Denmark Fig. 2—showed that using CSEC⁺ to assess the skills for all job profiles in this way takes between 20 and 35 min. Since this is a significant effort required from respondents, we decided to make the instructions more suc-

cinct, including only minimal data about the already-verbose (and reportedly self-explanatory) CSEC⁺ framework.

Therefore, the second phase of our data collection was prepared as an online service, designed to be anonymous and easy to broadcast. This second phase took place between March and April 2022. With the help of the CCN education focus group, we extended the target groups beyond the CS4E project, to reach also:

- Members from the European Cyber Security Organisation (ECSO, <https://ecs-org.eu>)³.
- The three EC pilot projects besides CS4E, namely CONCORDIA, SPARTA, and ECHO.
- Other potential respondents suggested by members from the aforementioned target groups.

Unlike ECSO, the four EC pilot projects—SPARTA, CS4E, CONCORDIA, and ECHO—were selected from the Horizon 2020 Cybersecurity call. As such, they intend to develop technological and industrial capacities within the EU that are necessary to secure its Digital Single Market (Penchev and Shalamanova, 2020). These projects are part of the CCN (Network (2022) <https://cybercompetencenetwork.eu/>), sharing its goal of “establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap”.

With input from these target groups, the second phase of our survey gathered 15 new responses from cybersecurity experts in the Czech Republic, Estonia, Germany, Greece, Hungary, Italy, Norway, and Spain.

Feedback on the clarity and ease of use of the new interface was positive. However, the response time remained high (in all cases above 15 min), limiting the amount of respondents. This was mainly due to the sheer amount of input requested per respondent—assessing 55 skills independently for six job profiles—and was also related to the use of an internal spreadsheet, which had to be filled-in and submitted. Since further input was required, we addressed these limiting factors in the third phase of our study, by designing a fully-online survey service.

This final phase was implemented in the Qualtrics online platform <https://vuass.eu.qualtrics.com>, which provides support for PCs as well as mobile devices, see Fig. 3. The main changes with respect to the second phase were an interactive interface to perform the assessments—without spreadsheets, see Fig. 3b—and the possibility to choose the number of job profiles to assess. Further technical details are given next in Section 3.2.

This survey was distributed in three channels: mailing lists and word-of-mouth, as before, and also via the official newfeed of CS4E⁴. Data was recorded during four weeks, between mid-September and the first week of October 2022. The result were 32 new respondents, from industry and academia, coming from Denmark, Estonia, Finland, Germany, Greece, Italy, The Netherlands, Portugal, Slovenia, and Sweden.

In total, the three phases resulted in 60 independent responses from 14 European countries, provided by experts in the cybersecurity community from industry and academia. We now give the technical details of the structure and content of the surveys used to gather this data.

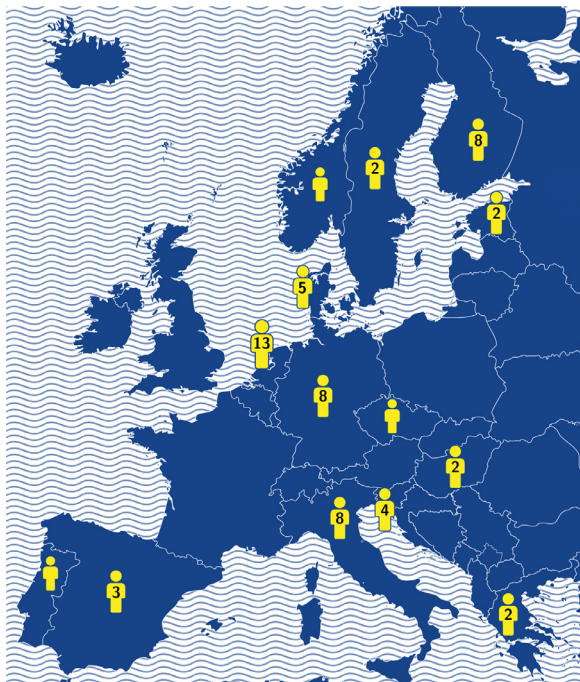


Fig. 2. Geographical distribution of respondents in Europe.

³ ECSO is a self-financed not-for-profit organisation established in 2016 to implement the cybersecurity Public-Private Partnership for the European Commission. It functions as a cross-sectorial partnership organisation, working towards a cyber-resilient and strategically autonomous digital Europe. ECSO hosts over 200 members in 6 working groups, ranging from standardization and certification to education, training and awareness European Cyber Security Organisation (2022).

⁴ <https://cybersec4europe.eu/the-eu-cybersecurity-skill-gap-is-bleeding-but-you-can-help-heal-it/>

Fig. 3. Survey - Third phase, mobile version.

3.2. Structure of the surveys

The second-phase survey, disseminated to the EC pilot projects and ECSO, was designed with the QuestBack online platform <https://www.questback.com>. It consisted of a first part with demographic questions, and a second part that contained the data and framework for the assessment. Questions in the first part were kept to a minimum, to preserve anonymity but still gather useful data to answer RQ3.a), and overview the representativeness of the data collected. The third-phase survey in Qualtrics also requested this information—see Fig. 3a.

The first demographic question asked the base country of the respondent: it opened as a drop-down menu listing European countries first, and the rest afterwards.

The second demographic question concerned the type of organisation of the respondent. It consisted of a single-choice question with the following possibilities:

1. Large company.
2. Small- or medium-sized company.
3. Academia/Research.
4. Public administration.
5. Other (please specify).

In our analyses, respondents who choose options 1 or 2 clearly belong to the *industrial sector*. Moreover, option 4 (present only in the Qualtrics survey) was chosen by two respondents: just like options 1 and 2, these represent *consumers of education*—as opposed to researchers who *produce education*—thus we placed them as part of the industrial sector. Contrarily, respondents who choose option 3 are said to belong to the *academic sector*. The last option opened a free-text box to write the respondent's organisation type. Only one respondent chose this option, indicating "self-employed": we also counted this as part of the industrial sector, for the same reason as option 4.

The second part of the surveys consisted of the job profiles skills assessment. For the QuestBack survey (second phase) this was a spreadsheet that contained the description of the profiles

INSTRUCTIONS

To carry out this study, we ask you to fill in the SURVEY sheet of this Excel file, with the evaluation of the knowledge units necessary for each of the six selected job profiles.

First of all please read the SKILLS sheet, which describes the six job profiles and the expected set of skills they should cover.

The SURVEY contains the so-called knowledge units of our cybersecurity assessment framework, e.g. cryptography, software design, risk management, etc. To fill in the SURVEY, for each job profile you must choose the degree to which you understand that each knowledge unit is relevant, in a scale from 0 (irrelevant) to 3 (extremely important for the job).

For instance, a "cybersecurity analyst" could need a degree of 3 in cryptography, a 1 in software design, and a 0 in risk management.

The scale of evaluation is the four step scale given below:

LEVEL	DESCRIPTION
Irrelevant (0)	The skill or knowledge is not necessary to perform in the given specialization.
Basic Knowledge / Skill (1)	Understanding the basic principles of the skill or knowledge is needed in the specialization. Application of these is not necessary to perform in the specialisation.
Intermediate Knowledge / Skill (2)	Applying the skill or knowledge is needed to perform in the specialization. The application of the skill or knowledge is not needed beyond standard procedures.
Advanced Knowledge / Skill (3)	Applying the skill or knowledge is essential to perform in the specialization. The application of the skill or knowledge is necessary on an advanced level and beyond well defined standard procedures.

Fig. 4. Survey - Second phase, spreadsheet instructions.

and of the CSEC⁺ framework. This spreadsheet was organised in three tabs:

- INSTRUCTIONS: the opening tab showed the instructions on how to carry out the assessment, curated and minimised with the experience of the first (pilot) phase of our approach—see Fig. 4.
- SKILLS: the second tab contained the detailed descriptions of the six job profiles, together with the use case and the scenario in which they interact. We discuss this in detail next, in Section 3.3.
- SURVEY: the third tab contained the CSEC⁺ framework prepared to assess the six job profiles. We show an excerpt of an assessment in Fig. 5.

Thus, the core data used for our analyses comes from the SURVEY tab of those spreadsheets. To provide this information, the respondents had to use the CSEC⁺ framework—as described in Section 2.3—to assess the skills required to perform in six job profiles. The choice of these profiles, and the use case in which they are given context, is described next in Section 3.3.

In contrast, the Qualtrics survey (third phase) embedded all questions into a user-friendly interface available for PCs and mobile devices, where the latter was used by 12 out of 32 respondents. In this survey, after the demographics questions, respondents were asked to choose the first job profile to assess; when that was completed, it was possible (but not mandatory) to continue on to assess the remaining profiles, which was done by six respondents.

The Qualtrics interface provides drop-down and single- or multiple-choice selectors—see Fig. 3. This survey offered area-wide choices: assessments are presented per area as in Fig. 3b, allowing respondents to choose the same assessment for all skills in the area. Alternatively, selecting "Detailed answer" permits individual responses per skill as in the second phase. Moreover, minimal information (and a reference link) about the area, skills, and evaluation scale appeared in the same page where the assessment was being done—see Fig. 3b. These modifications resulted in completion times of around 5 min per job profile.

3.3. Use case, scenario, and job profiles

Our main RQ—which skills should be covered by European curricula to satisfy the current and future needs in cybersecurity?—puts

Profile / Description	Knowledge area:	Data Security					
		Cryptography	Digital Forensics	Data Integrity And Authentication	Access Control	Secure Communication Protocols	Cryptanalysis
General Cybersec Auditor	Conducts external/internal audit of security controls and information systems, with particular attention to EES (Entry/Exit Systems); executes cybersecurity audits and composes technical reports on audit findings; maintains cybersecurity policies and standards.	2	1	2	2	3	1
Technical Cybersec Auditor	A specialisation of the general cybersec auditor, the technical cybersec auditor provides in-depth analysis of whether the cybersecurity systems are adequate and operating well; this person is also typically responsible for responding and assessing relevant cybersecurity measures, such as which technology to use for person identification (e.g. fingerprint readers vs. webcams).	2	2	2	3	3	1
Threat Modelling Engineer	Focuses on establishing security requirements, locating security risks and potential vulnerabilities, calculating threat and vulnerability criticality, and prioritizing remedial options.	2	3	3	3	2	2
Security Engineer	Creates and enforces security strategies and standards; the majority of the tasks entail predicting network or computer vulnerabilities and determining how to address them.	2	3	3	3	3	1
Enterprise Cybersecurity Practitioner	Manages cybersecurity risk at the company level, focusing on security operations and architecture; he/she identifies threats, vulnerabilities and risks in the enterprise network, outlines common attack techniques and security controls against common threats.	3	2	3	3	3	1
Cybersecurity Analyst	Deals with the network aspects of cybersecurity, focusing especially on reconnaissance, threat identification and mitigation, vulnerabilities' analysis and security incidents investigation.	2	3	3	2	2	1

Fig. 5. Survey – First and second phases, excerpt of an assessment.

emphasis on identifying skills whose relevance can transcend the present European needs, also projecting into the future.

In our approach, this can be done by selecting job profiles that can be expected to remain in demand for the next 10–20 years. To that aim, we chose occupations related to the regulatory system for people transit in the EU—since Schengen is one of the largest travelling areas in the world, for which the EU is mandating the implementation of new IT solutions such as Entry/Exit Systems (EES [European Commission, 2022](#)).

More in detail, our exemplary use case and related scenario depict a border control process in the context of travelling inside the European Union. Within this scenario, we define four relevant job profiles that interoperate to provide the necessary services.

We also describe two additional job profiles that appear in the MRC framework of ECSO ([European Cyber Security Organisation, 2021](#)). Strictly speaking, MRC does not describe occupations but rather teaching subjects. However, these descriptions include “suitable job roles” for people undertaking such courses. We based our choices on that, selecting *Enterprise Cybersecurity Practitioner* and *Cybersecurity Analyst*. Besides being relevant to the European cybersecurity panorama—as identified by ECSO in its MRC—these job profiles are in clear articulation with the use case defined for our study, e.g. as positions in the company deploying the passport-control software.

We now describe in detail the use case, scenario, and job profiles that comprise the basis of our survey.

Use case: border control post Border control posts typically utilise threat models to reduce risk. These models affect how and what kind of threats the security personnel—and IT solutions such as EES—are looking for in the system. In addition to detection mechanisms such as biometric identification and automated passport control readers, the access of unauthorised passengers is dependent on the threat model that is designed, i.e. how the border control personnel and technology are prepared to identify the unauthorised passengers. False positives in the system might be hard to notice without a proper indicator. Therefore, the threat model employed to detect unauthorised passengers affects the probability of them being allowed access mistakenly.

Scenario: threat model implementation The use case defines an environment where different interactions can take place. We refine this via a specific *scenario* of interaction, namely involving the application of a threat model to the border crossing checkpoints in airports. Border controls are carried out by agents (guards) in the crossing checkpoint. This threat model should be validated and enforced: the job profiles described next are essential for these activities.

Job profiles The following four job profiles were selected with regards to the use case and scenario defined above:

JP1 General cybersec auditor;

JP2 Technical cybersec auditor;

JP3 Threat modelling engineer;

JP4 Security engineer.

Additionally, the following two job profiles are also applicable to the use case in a broader scope. These occupations were taken from the minimal reference curriculum, first published by ECSO in 2021 ([European Cyber Security Organisation, 2021](#)):

JP5 Enterprise Cybersecurity Practitioner;

JP6 Cybersecurity Analyst.

We now describe the roles and main tasks that these job profiles entail in the use case and scenario selected.

JP1: General cybersec auditor This job profile is central to the adoption and audition of Entry/Exit Systems, currently being implemented in EU countries to ease manual border control checks. EES are European automated IT systems to register third-country visitors, whenever they cross an EU-external border. The visitor's name, type of travel document, biometric data, and the date and location of entry and exit are recorded by the system. This job profile executes audits on the implementation of such systems, to ensure that the required cybersecurity policies and standards are respected.

JP2: Technical cybersec auditor This job profile is similar to JP1, but with special focus on the technological deployment of the implementation. The work includes providing in-depth analysis of where the cybersecurity systems are adequate and operating well, as well as where there is room for improvement. If enhancements are required, the security auditor may also be responsible for providing an analysis of recommended security measures.

JP3: Threat modelling engineer This job profile focuses on establishing security requirements, locating security risks and potential vulnerabilities, calculating threat and vulnerability criticality, and prioritising remedial options. Creating well-documented threat models gives assurances that may be used to explain and defend the security posture of an application system. As opposed to the previous profiles, it is possible that a modelling engineer operates directly on the implementation of the EES.

JP4: Security engineer A security engineer's main job is to create and enforce security strategies and standards. The majority of the tasks involve predicting network or computer vulnerabilities and determining how to address them. This job profile is also expected to operate directly on the implementation.

JP5: Enterprise Cybersecurity Practitioner A person in this position must be able to master risk management specifically from a cybersecurity perspective. The job profile should understand at least superficially network architecture and security vulnerabilities of the company, including storage and computation facilities. They can assess the risks and choose measures to mitigate them, e.g. advising on the best solutions for the company: for mobile devices, cloud storage and computation, cryptographic techniques, response team size and composition, etc.

JP6: Cybersecurity Analyst This profile is proficient with network administration (including security), e.g. for architecture and vul-

nerability analysis as well as threat identification and mitigation. A cybersecurity analyst should be at least moderately proficient in cyber incidents response, such as performing a penetration analysis using professional tools.

3.4. Categorisation of the job profiles

From the six job profiles described above, the tasks carried out by the engineers and analyst—i.e. the Security engineer, Threat modelling engineer, and Cybersecurity Analyst—will likely involve direct implementation and deployment of policies and decisions in general. For that reason, we call these *technical job profiles*.

In contrast, the other three—Enterprise Cybersecurity Practitioner, General cybersec auditor, and Technical cybersec auditor—represent hierarchical positions, either within a company or across different bodies, e.g. the auditors may be assigned by a government department. These roles are expected to operate at a high level, possibly without participating into the implementation of policies or standards. We call these *managerial job profiles*.

This division between technical and managerial job profiles pursues two objectives:

- First and foremost, it is instrumental to interpret the survey results under the light of RQ3.b).
- On top of that, we exploit it as indicator of the quality of the communication with our respondents.

This secondary objective is based on a priori expectations: in principle, technical skills—e.g. from the Data security area in the CSEC⁺ framework—should be assessed higher values for the technical job profiles, while strategic skills—e.g. from the Organizational security area—should be given higher values for the managerial job profiles.

Note that these expectations are coarse, in the sense that we cannot foretell the exact skills that will be chosen as primordial for the job profiles. We only expect to see the following correlations between the job categories and the security areas of CSEC⁺: (a) technical job profiles should have high values assessed to skills from Data security, Software security, Connection security, or Operate and Maintain; (b) managerial job profiles should have high values assessed to skills from Societal security, System security, or Organizational security. We do not have specific expectations with respect to skills from the areas of Human security or Component security.

Technically, to interpret the survey results for this secondary (validation) objective, we study the degree to which our expectations are fulfilled. That is, if we can make a cut of skills that separates managerial from technical occupations in the expected way, it is taken as evidence that the interpretation of the profiles by our respondents was conveyed to them as desired.

3.5. Representativeness of the profiles

As discussed in Sections 3.3 and 3.4, the job profiles used in this study are relevant to areas on-demand in the European market, currently and for the foreseeable future. Moreover, the specific choice of profiles covers technical as well as managerial positions.

To achieve the above in a representative way (in terms of European cybersecurity needs), we partially guided our choices by ongoing studies of the European Union Agency for Cybersecurity, recently published in [European Union Agency for Cybersecurity \(2022\)](#). That document “describes the most important requirements of a professional cybersecurity workplace by defining a set of 12 typical cybersecurity professional role profiles”⁵.

More specifically, by virtue of the summary statement, mission, and main tasks of those twelve role profiles, we establish the following relations between our six job profiles and six roles listed in [European Union Agency for Cybersecurity \(2022\)](#):

- JP1 and JP2 cover the *Cybersecurity Auditor* role.
- JP3 covers the *Cyber Threat Intelligence Specialist* role (alternative title: *Cyber Threat Modeller*).
- JP4 covers the *Cybersecurity Implementer* role (alternative title: *Cybersecurity Engineer*).
- JP5 covers partially two roles: *Chief Information Security Officer* and *Cybersecurity Risk Management*.
- JP6 covers the *Cyber Incident Responder* role (alternative title: *Security Operation Analyst*).

This concerns the relevance of job profiles JP1–JP6 in the European Union. [Table 1](#) extends this analysis to compare against profiles published by the British Computer Society⁶, to give a notion of representativeness of our profiles in Europe but outside the EU. Our intentions in the long run are to extend our surveys to these cases—we discuss this as future work in [Section 5](#).

4. Results

Our survey gathered responses from 60 experts from the EU cybersecurity community—see [Table 2](#) and [Fig. 2](#). These responses cover 14 European countries, where two countries (Estonia and Portugal) had respondents solely from the industrial sector, eight had respondents solely from academic institutions, and the remaining four countries had respondents from both sectors.

The raw numeric assessments gathered by this study are presented in full in [Appendix A](#) on pages 16 and 17—a graphical representation of these is given by [Fig. B1](#) of [Appendix B](#), on page 18. To interpret this data and answer the research questions, we now present:

- The general aggregated information (transversal skills and top rankings), in [Section 4.1](#).
- An analysis of the data divided between academic and industrial respondents, in [Section 4.2](#).
- A further division depending on the job profile type (managerial vs. technical), in [Section 4.3](#).

In each section we discuss the implications of the results with respect to our research questions.

4.1. General analysis

Transversal skills We call a skill *transversal* if it requires above-average knowledge across many different job profiles. Such skills are very useful in many jobs, and therefore constitute the main educational targets in the curricula of academic and training institutions.

In our study, we identify a skill as transversal when its mean value is above intermediate—in the CSEC⁺ scale—for at least four profiles. That is, the mean value of a transversal skill is strictly greater than 2.0 for four or more of the six job profiles.

Out of the 55 skills in the CSEC⁺ framework, only seven satisfied this strong criteria, namely Network Defense, Fundamental Principles, Secure Communication Protocols, Incidents & Continuity,⁷ Network Architecture, System Control, and System Access. We show them in [Table 3](#), where the rightmost column indicates the

⁶ www.bcs.org

⁷ “Incidents & Continuity” is short for the skill *Business Continuity, Disaster Recovery, and Incident Management* from the knowledge area Organizational security—see [Fig. 1](#) and [Table A.1](#).

⁵ <https://bit.ly/3U9bela>















Table 1

Comparison of JP1–JP6 against other EU and non-EU frameworks. Double checkmarks (✓✓) indicate that the job profile requires knowledge in the corresponding competence; a single checkmark (✓) indicates that knowledge is advantageous but not essential.

Reference	Job profile	Requires skills with these competences:				
		Business implemen.	Technical implemen.	Incidents response	Research & develop.	Legal aspects
CS4E (CSEC ⁺ Dragoni et al., 2021)	JP1: General Cybersecurity Auditor	✓✓				✓✓
	JP2: Technical Cybersecurity Auditor			✓	✓✓	✓✓
	JP3: Threat Modelling Engineer	✓	✓✓	✓✓		✓
	JP4: Security Engineer		✓✓	✓✓	✓	
ECISO (MRC European Cyber Security Organisation, 2021)	JP5: Enterprise Cybersecurity Practitioner	✓✓	✓	✓		✓✓
	JP6: Cybersecurity Analyst		✓	✓✓	✓✓	
	Security Architect	✓	✓✓	✓✓		✓
	Chief Information Security Officer	✓✓		✓✓		✓✓
ENISA (ECSEF European Union Agency for Cybersecurity, 2022)	Penetration tester		✓✓	✓✓	✓	
	Cyber Legal, Policy and Compliance Officer	✓✓		✓	✓	✓✓
BCS (CCP specialisms British Computer Society, 2022)	Security and information risk advisor	✓✓	✓✓	✓		✓
	Cyber security / IA architect	✓	✓✓	✓✓		✓
	Cyber security / IA auditor	✓✓		✓	✓✓	✓✓
	IT security officer	✓✓		✓✓		✓✓

Table 2

Distribution and sector of respondents to our survey. The middle column indicates the number of responses that were received from the corresponding country.

Country	#	Sector
Czech Republic	1 	Academia
Denmark	5 	Academia
Estonia	2 	Industry
Finland	8 	Academia
Germany	8 	Industry & academia
Greece	2 	Academia
Hungary	2 	Industry & academia
Italy	8 	Industry & academia
The Netherlands	13 	Academia
Norway	1 	Academia
Portugal	1 	Industry
Slovenia	4 	Academia
Spain	3 	Industry & academia
Sweden	2 	Academia

number of job profiles for which the above-average criterion was satisfied.

Top-10 ranking of skills Table 4 shows the ten highest-ranked skills (on average) by the assessors in this study. We report the

standard deviation alongside the mean, to give an indication of the spread in the assessments, and also to disambiguate: in cases when the mean values coincide, we sort the skills in ascending order of the standard deviation values, prioritising the skills for which there was a higher coincidence of its relevance.

Discussion

Five transversal skills appear in the top-10 ranking—both transversal skills from System Sec. fall out, appearing in positions 11 and 13 of the total ranking. Conversely, only five skills from the top-10 are classified as transversal, at the ranking positions 1 (Network Defense), 3 (Fundamental Principles), 4 (Secure Communication Protocols), 5 (Network Architecture), and 6 (Incidents & Continuity). This shows how the criterion of transversal skills, that requires their high assessment in many different job profiles, produces a different cut than the simpler top-10 ranking.

These rankings give a nuanced answer to RQ1—Which are the most relevant skills to teach and perform in cybersecurity-related jobs?—where the cut of transversal skills gives a minimal shortlist. Such shortlists are helpful to prioritise the curricula of teaching institutes, whose intention is to cover the most essential and widely useful cybersecurity topics. More in general and unsurprisingly, many of the highly-relevant skills—e.g. Risk Management, Access Control, Common System Architectures, etc.—are very useful only to specific occupations. This suggests that teaching institutes with a strong interest in cybersecurity education might need to

Table 3

Transversal skills in our study: mean value of the assessments, and amount of job profiles with an assessment above 2 on the Likert scale from 0 (irrelevant) to 3 (advanced) of Section 2.2.

Skill	Area	Mean	#>2
Network Defense	Connection Sec.	2.28	5
Fundamental Principles	Software Sec.	2.12	4
Secure Comm. Protocols	Data Sec.	2.11	4
Network Architecture	Connection Sec.	2.09	4
Incidents & Continuity ⁷	Organizational Sec.	2.09	4
System Control	System Sec.	2.01	4
System Access	System Sec.	1.99	4

Table 4

Top-10 skills in our study: mean value and standard deviation of the assessments, following the Likert scale of [Section 2.2](#) that ranges from 0 (irrelevant) to 3 (advanced).

	Skill	Area	Mean	Stdev
1	Network Defense	Connection Sec.	2.28	0.85
2	Access Control	Data Sec.	2.13	0.76
3	Fundamental Principles	Software Sec.	2.12	0.89
4	Secure Comm. Protocols	Data Sec.	2.11	0.76
5	Network Architecture	Connection Sec.	2.09	0.81
6	Risk Management	Organizational Sec.	2.09	0.85
7	Incidents & Continuity ⁷	Organizational Sec.	2.09	0.88
8	Information Storage Sec.	Data Sec.	2.07	0.78
9	Data Integrity & Authen.	Data Sec.	2.05	0.78
10	Common System Archit.	System Sec.	2.02	0.80

prioritise their educational offer on the basis of their intended output market sector—a task for which studies like this one are instrumental.

In that sense it is useful to compare the transversal skills from [Table 3](#) against the cybersecurity curricula of current careers across different European countries ([Dragoni et al., 2021](#)). We observe that the two skills from Connection security, i.e. Network Defense and Network Architecture, are relatively well covered by mandatory or optional courses in most countries. In contrast and despite its high general relevance (even across occupations), Incidents & Continuity is taught much more sparsely, e.g. it is absent from MSC programmes in Hungary, Romania, Poland, and Ireland.

Another important observation from [Tables 3](#) and [4](#) is that none of the highest ranked skills pertain to the area of Human security, which includes skills such as Social Engineering, Identity Management, and Personal Compliance.⁸ Extending the ranking from [Table 4](#), the highest-valued human skills—Identity Management (mean=1.95) and Social Engineering (mean=1.86)—appear respectively in positions 17 and 25, see [Table A.1](#). This gives a mostly negative answer to RQ2—*Is the human factor regarded as a formal requirement in cybersecurity education and training?*—suggesting that trainers and educators still do not consider the human aspect of cybersecurity as a main topic requiring formal teaching, validation, and certification.

The absence of Human security skills in [Tables 3](#) and [4](#) could have its roots in the traditional forms of teaching, that favour theoretical and technical contents such as network architecture, fundamental principles of software, cyber law, etc. Instead, skills like Social and Behavioural Privacy (from the Human security area) are harder to fit as subjects into existing curricula.

Notwithstanding such explanation, it is crucial to take into account the importance of developing and maintaining cybersecurity awareness, in terms of not only “what to learn” but also “how to learn it”. Human security is greatly affected by this, where studies show that training and education will be more effective when the emphasis is not only on what is important (knowledge), but also by motivating why it is important (attitude) ([Parsons et al., 2017; 2014](#)). Within this scope, it should also be acknowledged that cybersecurity knowledge is often spread tacitly within organizations ([Ahrend et al., 2016](#)), which may serve as another information source from the educative point of view, such as utilizing this institutional source as a part of the education plan.

There is, moreover, abundant evidence on the importance of mitigating attacks targeted at individuals. These range from attack

vectors of human security—targeted by information operations or as part of hybrid operations—implemented by larger scale organizational or national actors, all the way down to the low-complexity phishing, shoulder surfing, and the like. The fact remains that a successful attack to a single individual can compromise an entire organisation, and this could be initially addressed in a comprehensive cybersecurity education plan.

However, and despite its criticality, our results above suggests that Human security skills may still not be given sufficient attention in formal education and training. This can be based on limitations—psychological and technical—of the traditional forms of education ([Furnell and Clarke 2012; Parsons et al. 2014](#)). A possible solution can be to resort to alternative approaches, better suited to train individual and social behaviour, such as Security Serious Games that can be taught at medium, academic, and professional levels.

Finally, we note that the choice of Network Defense as the most relevant skill—even across different job profiles—can be argued to be consistent with the under-appreciation of Human security skills, showing a tendency to consider cybersecurity as concerning remote (i.e. network-based) attacks. Albeit undoubtedly important, we believe that this should be balanced by education on personal security hygiene, teaching early on how to protect oneself from the most common—and usually most successful—human attacks. Interestingly, the assessment of Network Defense as one of the most relevant skills is a point of agreement between academia and industry, as we show next.

4.2. Industry vs. academia

From the fourteen countries that participated in this study, six included respondents from the industrial sector⁹, and twelve included respondents from the academic sector. We analyse how this division impacts the assessment values, to better understand the degree to which industrial and academic priorities are aligned. For that, [Tables 5](#) and [6](#) show respectively the areas ranking and top-10 skills as assessed by respondents from these two sectors.

Before comparing the rankings in our discussion below, we note that the assessment values chosen by industrial respondents are higher than those of academic respondents. Since this is uniform for all rankings, *any meaningful comparison for RQ3.a) must consider the positions of an area or skill within a particular ranking, and not only the exact (mean) assessment value chosen.*

⁸ “Personal Compliance” is short for the skill *Personal Compliance with Cybersecurity Rules / Policy / Ethical Norms* from the knowledge area Human security—see [Fig. 1](#) and [Table A.1](#).

⁹ This includes two respondents from public administration, who are also consumer of education—see the discussion in [Section 3.2](#).

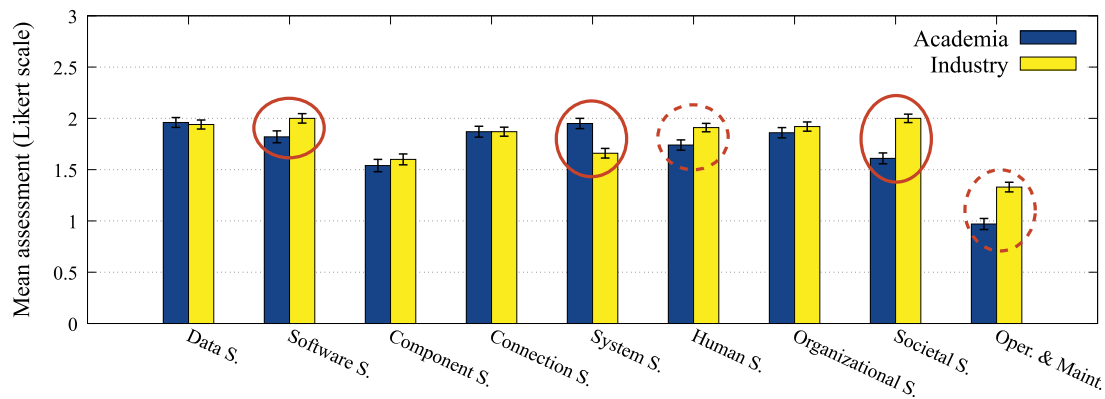


Fig. 6. Areas assessment: academic vs. industrial respondents. The value for an area is the average value of its skills, in the Likert scale from 0 (irrelevant) to 3 (advanced). The whiskers on top of the bars represents Student's *t* confidence intervals (95%) with 59 degrees of freedom. Red rings highlight the areas for which there are statistically significant differences, but these must be interpreted in conjunction with the ranking positions of Table 5, as explained in Section 4.2.

Discussion

Clear coincidences between academic and industrial respondents are the positions of Organizational security (4), Component security (8), and Operate & Maintain (9) in Table 5. Two further points in common are the relatively high position of Data security, and the middle position of Human security. Although this comparison of areas is coarse, it helps to see that the general priorities between academia and industry are not entirely misaligned.

Notwithstanding such coincidences, the table also helps to spot notorious differences, e.g. the second place of Software security in responses from industry. In contrast, the second place is occupied by System security in the academic ranking, mainly by the high value observed for its skills System Control, System Access, and Common System Architectures. These skills, and the System security area in general, could be interpreted as a conceptual description of the operation of a company. This matches an (“abstract”) vision that educators could have about the six job profiles assessed. Instead, the (“concrete”) vision of practitioners is closer to the everyday operations that the job profiles entail: in this case, skills such as Documentation and Fundamental Principles raise to the top in Table 6, explaining the high position of Software security in the industrial ranking.

Another conspicuous difference is Societal security, that includes the skills Privacy and Cyber Law, respectively in positions 6 and 13 of the industrial skills ranking—see Tables 6 and A.1. The relevance of these skills for a company is apparent, e.g. regarding liabilities for undesired events, and thus its first place in this ranking is unsurprising. However, this contrasts strongly to the academic ranking, which puts Societal security in seventh place.

Instead, academic respondents selected Data security as the most important area, by virtue of the skills Access Control, Secure Communication Protocols, and Data Integrity and Authentication. Such skills, and the area in general, are (less so but still) highly relevant for the industrial respondents, so this is interpreted as a mild coincidence in the assessment of the two sectors.

Oppositely, while System security occupies the second position in the academic ranking, it appears seventh in the industrial ranking, also with a significant assessment value gap in Fig. 6, which marks it as a notorious difference. The same cannot be said of Operate & Maintain: despite exhibiting a similar gap in Fig. 6, it occupies the same position in the rankings of both sectors. Therefore, in this case, the difference in absolute mean value is not indicative of different priorities in the two sectors.

Human security requires further analysis: Fig. 6 shows a statistical significant difference, and Table 5 places the area in positions 6 and 5 for the academic and industrial rankings respectively. Studying the mean values in the table, we observe that Human se-

curity is 0.08 points below the area in position 5 for academia, and 0.13 points above the one in position 7. These differences are the second and third largest in that ranking, placing Human security quite strongly as a mid-importance area for academia.

For industry instead, the differences with respect to the previous and next areas in the ranking are lower. However, industrial assessments show less variability—see the standard deviations in Table 5—and Human security is in the exact middle of the ranking. This suggests that the area is also in the mid-importance region for the industrial sector. We do note, however, that Social Engineering (a Human security skill) appears at the bottom of the top-10 skills ranking for industry in Table 6. In contrast, the most important Human security skill for academia is Identity Management, which is only at position 19 of the total ranking (Social Engineering is at position 30). Thus, despite the coincidences highlighted above, it would appear that Human security skills are considered more important by industrial respondents than by academic ones.

However and in general, the main differences are observed for the areas of Software security and Societal security, which industrial respondents consider more important than their academic counterparts, and System security, for which the opposite is true. These differences suggest misaligned perspectives:

- On the one hand, educators are traditionally more prone to consider abstract systematisations, susceptible to management, planning, and optimisation;
- On the other hand, practitioners are more concerned about current needs, privacy-preserving measures, and legal aspects of the company's actions.

Such interpretation is coherent with the skills rankings presented in Table 6, where we observe Data Privacy (from the area of Data security) in position 5, and Privacy (Societal security) in position 6 for industrial respondents. None of these skills appear in the top-10 for academic respondents—instead, we observe there the first place of Network Defense and fourth place of Network Architecture, which speaks of a high consideration for network-based attacks, as opposed to (possibly lower complexity) human-interaction attacks. This is also in line with our earlier discussion on the Human security area.

Nevertheless, recent works like van Oorschot (2022) show a growing awareness in academic education of (typically industrial) values such as legal aspects of cybersecurity, and measures for privacy-preserving implementation. This is a promising sign, likely the fruit of active efforts from European bodies—e.g. universities, governments, and the European Commission—to create opportunities for direct collaboration between companies and universities.

Table 5

Area ranking: academic vs. industrial respondents. The value for an area is the average of the values of its skills, that follow the Likert scale of Section 2.2 from 0 (irrelevant) to 3 (advanced).

Academia			Industry		
Area	Mean	Stdev	Area	Mean	Stdev
Data S.	1.96	0.86	1 Societal S.	2.00	0.74
System S.	1.95	0.89	2 Software S.	2.00	0.83
Connection S.	1.87	0.96	3 Data S.	1.94	0.79
Organizational S.	1.86	0.90	4 Organizational S.	1.92	0.81
Software S.	1.82	1.05	5 Human S.	1.91	0.73
Human S.	1.74	0.90	6 Connection S.	1.87	0.79
Societal S.	1.61	0.95	7 System S.	1.66	0.85
Component S.	1.54	1.07	8 Component S.	1.60	0.96
Oper. & Maint.	0.97	0.97	9 Oper. & Maint.	1.33	0.85

Table 6

Top-10 skills of academic and industrial respondents. The (mean and standard deviation of the) assessment values follow the Likert scale of Section 2.2, from 0 (irrelevant) to 3 (advanced).

Academia			Industry		
Skill	Mean	Stdev	Skill	Mean	Stdev
Network Defense	2.30	0.85	1 Fundamental Principles	2.38	0.62
Access Control	2.15	0.78	2 Documentation	2.33	0.72
Secure Comm. Protocols	2.14	0.77	3 Network Defense	2.19	0.83
Network Architecture	2.12	0.82	4 Incidents & Continuity	2.14	0.81
Risk Management	2.12	0.87	5 Data Privacy	2.12	0.77
System Control	2.11	0.86	6 Privacy	2.10	0.76
Information Storage Security	2.07	0.80	7 Digital Forensics	2.10	0.85
Data Integrity & Authentication	2.07	0.80	8 Cybersecurity Planning	2.07	0.84
Incidents & Continuity	2.07	0.90	9 Social Engineering	2.05	0.73
Common System Architectures	2.05	0.79	10 Information Storage Security	2.05	0.70

From the above we find a mostly positive answer to RQ3.a)—Are there different perceptions in the relevance of skills from the perspective of professionals (in the industrial sector) vs. educators (in the academic sector)?—where the industrial sector is more concerned with implementation-, deployment-, and legal-related skills, whereas the academic sector prioritises conceptual- and network-based cybersecurity knowledge. Despite the possibility to comprehend these differences, their existence—as exemplified in our study—suggests that cybersecurity education in Europe still requires active endeavours from the community, to best articulate the educational offer with the professional demand.

4.3. Managerial vs. technical job profiles

The last part of our study compares skills from the perspective of the specific job profiles where these are required. This concerns RQ3.b), which we addressed by selecting two types of occupations for our survey:

- **Managerial job profiles**—Enterprise Cybersecurity Practitioner, General Cybersec Auditor, and Technical Cybersec Auditor—represent positions expected to be in charge of supervising the

results of other personnel on the activities of the company, i.e. without participating directly in the implementation of policies or standards.

- **Technical job profiles**—Threat Modelling Engineer, Security Engineer, and Cybersecurity Analyst—represent occupations expected to implement and deploy the decisions made by other people in the company.

As indicated in Section 3.4, this categorisation has the double objective to (a) sample the top skills that the cybersecurity community expects/demands from people performing in these different types of occupations, and also (b) serve as indicator on whether the description of the profiles was properly communicated to our respondents.

Regarding the first (and main) objective, the managerial/technical division allows us to build two separate hierarchies of skills, that can be consulted for the design of cybersecurity curricula by teaching institutes oriented to these two sectors. In particular, the study on transversal skills in Section 4.1 showed that, as expected, curricular subjects should be prioritised based on the occupations to fill, since the majority of cybersecurity skills are job-specific. We use RQ3.b) to observe concrete differences in

Table 7

Top-10 skills for managerial vs. technical job profiles. The (mean and standard deviation of the) assessment values follow the Likert scale of Section 2.2, from 0 (irrelevant) to 3 (advanced).

Managerial			Technical		
Skill	Mean	Stdev	Skill	Mean	Stdev
Risk Management	2.25	0.79	1 Network Defense	2.48	0.76
Incidents & Continuity	2.15	0.86	2 Secure Comm. Protocols	2.24	0.74
Access Control	2.06	0.73	3 Fundamental Principles	2.24	0.84
Security Govern. and Policy	2.05	0.84	4 Network Architecture	2.22	0.75
Cybersecurity Planning	2.04	0.82	5 Digital Forensics	2.21	0.83
Personal Compliance	2.04	0.86	6 Access Control	2.18	0.77
System Access	2.03	0.8	7 Network Implementations	2.16	0.84
Security Program Management	2.02	0.85	8 Information Storage Sec.	2.14	0.8
Network Defense	2.02	0.88	9 Analysis and Testing	2.14	1.02
System Control	2.02	0.88	10 Data Integrity & Authentication	2.12	0.82

this division, to learn which skills are of highest importance for managers, and which are for technicians/engineers.

With that in mind we present in Table 7 the ranking of skills for both types of job profiles.

Discussion

The skills in positions 1, 2, 4, 5 and 8 for the managerial job profiles in Table 7 pertain to the Organizational security area; System Access and System Control in positions 7 and 10 are from System security. These are seven out of ten top skills for managerial job profiles, that correspond to the expected cybersecurity areas.

As exceptions to this trend we see Access Control and Network Defense in positions 3 and 9, and Personal Compliance in position 6. The first two are also in positions 1 and 2 of all skills assessments (see Table 4), so their presence in this ranking for managerial job profiles is not particularly surprising. The latter is in line with our previous observation in Section 4.2, about the relevance of legal aspects for companies, which is arguably more on the managerial side of a company's operation.

It is also interesting—although unsurprising—to observe Risk Management and Incidents & Continuity as the first two skills of the ranking. This might be indicating a prioritisation of topics easy to integrate into the general policies of a company, as opposed to skills specialised to cybersecurity such as Security Governance and Policy, Cybersecurity Planning, and Security Program Management. That said, the third position of Access Control in the managerial ranking suggests that this prioritisation is not necessarily a proven fact, and further studies in this direction are needed to substantiate or reject it.

Regarding technical job profiles, the skills in position 1, 4 and 7 pertain to Connection security, those in positions 2, 5, 6, 8, and 10 are from Data security, and in position 3 and 9 we have Fundamental Principles and Analysis and Testing from the area of Software security. Therefore, we observe the expected kind of skills selected for the technical job profiles of our study—see Section 3.4.

In summary, the above answers positively RQ3.b)—Are there different perceptions in the relevance of skills that correlate to the job profile type, e.g. managerial vs. technical?—where skills from the areas of Organizational and System security are mostly relevant for

managerial job profiles; while skills from the areas of Data, Connection, and Software security are more relevant for technical jobs.

5. Conclusions

In this work we have taken steps to determine which skills should be covered by European curricula to satisfy the current and future needs in cybersecurity. To do this in a representative manner, the assessment and prioritisation of skills was performed by experts from the cybersecurity community, coming from the industrial and academic sectors of 14 countries in Europe. These assessments were gathered by means of surveys, structured according to the CSEC⁺ framework to determine which skills are needed—and to which degree—to perform in six job profiles. The profiles, related to the use of a threat model in border control posts, are expected to be of high relevance for cybersecurity in the EU for the following 10–20 years.

Regarding concrete results, our study highlights the following main points. The most important (“transversal”) cybersecurity skills from the framework are *Network Defense* and *Network Architecture* (from the Connection security area), *System Control* and *System Access* (from System security), *Fundamental Principles* (from Software security), *Secure Communication Protocols* (from Data security), and *Incidents & Continuity* (from Organisational security). Furthermore, *Risk Management* and *Access Control* were also highly valued skills, but mostly in relation to specific job profiles, such as Enterprise Cybersecurity Practitioner (for *Risk Management*) and Security Engineer (for *Access Control*).

Beyond such top skills, we observe that the priorities of academic and industrial respondents differ in some clear points. Educators from universities and teaching institutes placed the areas of Data, System, and Connection security at the top, prioritising skills such as *Access Control*, *Secure Communication Protocols*, and *Network Architecture* (which do not make it to the industry top-10). Instead, professionals and practitioners from companies considered *Fundamental Principles*, *Documentation*, and *Data Privacy* among the most relevant skills, in contrast to the academia top-10 which does not include these skills. In the bigger picture, this makes the areas of Software and Societal security to be significantly more important

for industrial respondents than for academic ones, while the opposite occurred with System security.

That said, the academic and industrial sectors are not entirely misaligned. Both place *Network defense* among their top-3 skills, and *Incidents & Continuity* is slightly less aligned but still in the top-10 for both sectors in Table 6. Furthermore, the area of Organizational security is in position 4 of Table 5 for both sectors, while Component security and Operate & Maintain appear at the last positions.

Table 5 also shows that both sectors give middle importance to the area of Human security. As noted in Section 4.2, industry seems to assign slightly more importance than academia to this area, as indicated by the ninth position of the *Social Engineering* skill in Table 6. However, responses from both sectors do not place the Human security area among the most relevant to perform in the job profiles assessed. This seems to be another point of consistency between industry and academia.

Such ranking of Human security by our assessors is conjectured to be related to at least two other factors. First, the high ranking of skills from Connection security could be a correlated event, suggesting a perception of cybersecurity as a means to defend (mostly) against remote attacks. Second, the difficulty to incorporate such concepts in traditional education and professional training might also be playing a substantial role. In view of this, we expect that the use of non-traditional education—e.g. from medium to academic level—can help to alleviate this relatively low appreciation of the human factor in the role of cyber attacks. For example, Security Serious Games could be an excellent tool to awake and train security-hygienic individual behaviour.

Regarding the managerial vs. technical categorisation of the job profiles, we observed the expected priorities: skills from the areas of Data, Connection, and Software security in the CSEC⁺ framework were mostly relevant to technical job profiles; instead, managerial job profiles benefit the most from skills pertaining to the areas of Organizational, System, and Societal security.

Limitations and future work

A factor that limits the generality of our conclusions is the description of a use case and scenario to interpret the job profiles. Although this was done to facilitate the assessments, by giving the respondents a concrete situation to think of, it can also narrow the interpretations of the skills required by the profiles.

We see two workarounds: providing purely abstract descriptions of the profiles, or describing more use cases to exemplify situations where these operate. Purely abstract descriptions are, by their very nature, detached from concrete exercises of the abilities required by the profiles. We thus expect this approach to be more vulnerable to misinterpretations by the respondents. Our analysis of managerial vs. technical job profiles in Section 4.3 suggests that this did not occur in our case. Therefore, we recommend to extend our studies by providing more use cases in which to interpret the profiles, thus offering further perspectives. However, this should be done with moderation, to avoid increasing too much the survey response time, which is a fundamental aspect to consider as discussed next.

Another factor playing against the generality of our conclusions is the participation rate of interested European parties. Although covering 14 countries, the number of responses gathered for our studies—60 in total, but only 12 from the industrial sector—could still improve.

Our three phases of data collection show that the fully online survey was the most effective. This was at least partly caused by the existence of a mobile version, and the possibility to select which and how many job profiles to assess. All in all, comparing the three surveys and the feedback from our respondents, the key

factor was allowing a full unit of data input (for us, assessing a job profile) to be completed in 5 to 10 min.

Having achieved the above, we expect that a stronger dissemination of the survey—e.g. resorting to official European bodies with high incidence in the industrial sector—can result in an even higher response rate. For instance, this could be practiced by setting a shared agenda with ECSO or ENISA, who could propose further job profiles to be assessed, and exploit their network to gather responses from large companies and SMEs.

Finally, besides the number of respondents, further representativeness for Europe requires gathering input from non-EU countries. In this respect, we plan to collaborate with organisations such as the British Computer Society, to get new input data that extends our current studies.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Carlos E. Budde: Conceptualization, Methodology, Validation, Investigation, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision. **Anni Karinsalo:** Conceptualization, Validation, Investigation, Data curation, Writing – original draft. **Silvia Vidor:** Validation, Investigation, Writing – original draft, Visualization. **Jarno Salonen:** Validation, Project administration, Funding acquisition. **Fabio Massacci:** Methodology, Validation, Writing – review & editing, Supervision, Project administration, Funding acquisition.

Data Availability

Data will be made available on request.

Acknowledgments

This work was funded by the European Union grant 830929 (H2020-CyberSec4Europe), and GA n° 101067199-ProSVED. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or The European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Appendix A. The CSEC⁺ framework applied to the six job profiles: survey results

The CSEC⁺ framework is divided in nine knowledge areas, each comprising several knowledge units. The notation was adopted from CSEC (Joint Task Force on Cybersecurity Education, 2018)—this also covers all specialty areas from CWF (Petersen et al. 2020), with the exception of *Customer Service and Technical Support*, which CSEC⁺ places in a knowledge area of its own: *Operate and Maintain*.

Thus, CSEC⁺ has a total of 55 knowledge units partitioned into 9 different knowledge areas. The exact correspondence between CSEC and CWF to define the CSEC⁺ framework can be found in Dragoni et al. (2020).

In Table A.1 (page 17) we present the numeric results of our study, where CSEC⁺ was applied by 29 expert respondents from the cybersecurity community in Europe to assess the skills required by six job profiles. Thus, Table A.1 lists—for each job profile and skill—the mean and standard deviation of the 29 assessments gathered.

We recall that an assessor would choose the value zero (0) for a skill with respect to a job profile if the skill is considered ir-

Table A.1

Numeric results of our survey with the CSEC* framework. For each job profile—columns “Cybersec Analyst” through “General Cybersec Auditor”—and skill—rows “Cryptography” through “Customer Serv. & Tech. Support”—we report the mean (left) and standard deviation (right, italicised) of the 29 independent assessments recorded in our survey. Assessments use the Likert scale from 0 (irrelevant) to 3 (advanced) of Section 2.2: the higher the mean, the more knowledge of the skill is required to perform in the job.

Area	Skills	Overall Mean	Overall Stdev	Cybersec Analyst		Enterprise Cybersec. Pract.		Security Engineer		Threat Modelling Engineer		Technical Cybersec Auditor		General Cybersec Auditor	
Data security	Cryptography	1.80	0.83	1.97	0.77	1.52	0.74	2.30	0.74	1.66	0.84	1.91	0.84	1.19	0.60
	Digital Forensics	1.95	0.91	2.39	0.69	1.41	0.98	2.30	0.91	1.91	0.78	2.00	0.90	1.45	0.77
	Data Integrity and Authenticat.	2.05	0.78	1.94	0.86	1.93	0.70	2.44	0.67	1.91	0.85	2.30	0.64	1.65	0.66
	Access Control	2.13	0.76	2.00	0.68	2.07	0.75	2.51	0.67	1.97	0.86	2.27	0.76	1.84	0.64
	Secure Communication Protocols	2.11	0.76	2.19	0.67	2.03	0.73	2.51	0.67	1.94	0.80	2.24	0.71	1.58	0.67
	Cryptanalysis	1.57	0.98	1.72	0.94	1.14	0.92	2.02	0.99	1.60	1.03	1.73	0.88	1.00	0.73
	Data Privacy	1.99	0.83	1.78	0.83	1.66	0.81	2.26	0.82	1.89	0.90	2.09	0.77	2.16	0.69
Information Storage Security	2.07	0.78	1.94	0.71	2.03	0.78	2.42	0.76	2.00	0.84	2.21	0.70	1.68	0.70	
Software security	Fundamental Principles	2.12	0.89	2.11	0.82	1.93	0.92	2.42	0.85	2.14	0.85	2.12	0.89	1.84	0.97
	Design	1.77	1.00	1.58	1.00	1.52	0.99	2.26	0.93	2.00	1.00	1.73	0.98	1.35	0.88
	Implementation	1.72	1.03	1.72	1.00	1.48	0.87	2.42	0.93	1.63	0.97	1.70	1.05	1.10	0.87
	Analysis and Testing	1.97	1.02	2.00	0.96	1.66	0.97	2.56	0.85	1.77	1.11	2.06	1.00	1.52	0.89
	Deployment and Maintenance	1.76	1.02	1.81	0.95	1.69	0.93	2.42	0.96	1.60	1.03	1.58	1.00	1.23	0.84
	Documentation	1.94	1.02	1.72	0.94	1.72	1.03	2.35	0.87	1.91	1.01	1.85	1.12	1.97	1.08
	Ethics	1.72	1.03	1.56	1.13	1.55	0.95	2.00	1.07	1.60	1.03	1.67	0.99	1.90	0.91
Compon. security	Component Design	1.62	0.99	1.67	0.89	1.41	0.98	2.07	0.94	1.71	1.10	1.52	0.91	1.13	0.92
	Component Procurement	1.34	1.02	1.22	0.96	1.24	1.06	1.74	1.05	1.31	0.93	1.21	0.99	1.16	1.10
	Component Testing	1.71	1.04	1.89	0.92	1.31	1.07	2.30	0.89	1.60	1.09	1.73	1.01	1.13	0.88
	Component Reverse Engineering	1.54	1.10	1.89	1.04	1.14	0.99	2.02	1.10	1.51	1.20	1.42	1.03	0.97	0.80
Connection security	Physical Media	1.57	0.94	1.58	0.87	1.38	0.98	1.98	0.91	1.51	0.95	1.64	0.82	1.13	0.96
	Physical Interf. and Connectors	1.56	0.98	1.61	0.93	1.28	1.03	1.98	0.89	1.40	0.98	1.73	0.88	1.19	1.01
	Hardware Architecture	1.62	0.95	1.64	0.99	1.41	1.09	1.88	0.91	1.66	0.91	1.82	0.81	1.19	0.91
	Distributed Systems Architecture	1.91	0.85	2.03	0.74	2.00	0.85	2.21	0.77	1.86	0.88	1.91	0.80	1.35	0.88
	Network Architecture	2.09	0.81	2.33	0.68	2.14	0.74	2.35	0.69	1.94	0.84	2.09	0.80	1.58	0.92
	Network Implementations	1.97	0.90	2.31	0.71	1.97	0.87	2.37	0.72	1.74	0.95	1.91	0.88	1.35	0.95
	Network Services	1.92	0.89	2.11	0.92	1.86	0.95	2.30	0.67	1.83	0.89	1.82	0.92	1.45	0.85
Network Defense	2.28	0.85	2.47	0.77	2.31	0.89	2.63	0.62	2.31	0.87	2.12	0.82	1.65	0.84	
System security	System Thinking	1.86	0.93	1.69	0.89	2.03	0.87	1.93	0.88	2.20	0.83	1.76	0.97	1.52	1.03
	System Management	1.87	0.91	1.58	0.94	2.03	0.87	2.09	0.81	1.97	0.86	1.79	0.99	1.74	0.96
	System Access	1.99	0.80	1.69	0.86	2.07	0.65	2.09	0.78	2.03	0.75	2.15	0.91	1.87	0.81
	System Control	2.01	0.86	1.75	0.91	2.10	0.77	2.16	0.81	2.09	0.78	2.12	0.96	1.84	0.90
	System Retirement	1.60	0.94	1.39	0.90	1.55	0.95	1.93	0.86	1.71	0.96	1.55	1.06	1.39	0.88
	System Testing	1.90	0.92	1.94	0.89	1.69	0.93	2.21	0.80	1.86	0.97	2.06	0.90	1.52	0.96
	Common System Architectures	2.02	0.80	1.89	0.75	2.21	0.62	2.19	0.76	2.09	0.85	2.00	0.90	1.74	0.82

(continued on next page)

Table A.1 (continued)

Area	Skills	Overall Mean	Overall Stdev	Cybersec Analyst	Enterprise Cybersec.	Security Engineer	Threat Modelling Engineer	Technical Cybersec Auditor	General Cybersec Auditor						
Human security	Identity Management	1.95	0.81	1.69	0.95	1.86	0.83	2.02	0.83	2.03	0.71	2.09	0.77	2.00	0.73
	Social Engineering	1.86	0.82	1.97	0.88	1.69	0.85	1.81	0.82	2.03	0.82	1.82	0.85	1.81	0.65
	Personal Compliance with Cybersec. Rules/Policy/Ethical Norms	1.86	0.91	1.61	0.93	1.86	0.92	1.81	0.85	1.69	0.99	2.00	0.87	2.26	0.77
	Awareness and Understanding	1.68	0.94	1.44	0.94	1.83	0.93	1.67	0.89	1.60	0.91	1.67	1.02	1.90	0.94
	Social and Behavioral Privacy	1.58	0.89	1.36	0.93	1.66	0.90	1.65	0.92	1.51	0.85	1.55	0.90	1.77	0.80
	Personal Data Privacy and Sec.	1.83	0.80	1.75	0.84	1.72	0.80	1.84	0.81	1.77	0.81	1.82	0.81	2.10	0.75
Organizational security	Usable Security and Privacy	1.64	0.84	1.56	0.88	1.62	0.86	1.67	0.78	1.63	0.91	1.58	0.83	1.77	0.80
	Risk Management	2.09	0.85	1.72	0.91	2.38	0.78	1.81	0.79	2.37	0.84	2.00	0.87	2.39	0.67
	Security Governance and Policy	1.86	0.89	1.50	0.97	2.21	0.82	1.74	0.85	1.89	0.87	1.67	0.85	2.32	0.70
	Analytical Tools	1.90	0.89	2.08	0.84	1.79	0.86	1.81	0.82	1.97	1.12	1.94	0.86	1.81	0.79
	Systems Administration	1.71	0.84	1.72	0.91	1.83	0.93	1.70	0.86	1.63	0.91	1.73	0.72	1.68	0.75
	Cybersecurity Planning	1.95	0.89	1.64	1.02	2.14	0.88	1.93	0.88	2.03	0.92	1.79	0.82	2.23	0.72
	Business Continuity, Disaster Recovery, and Incident Mgmt.	2.09	0.88	1.86	0.99	2.45	0.74	2.02	0.86	2.23	0.84	1.88	0.96	2.16	0.78
	Security Program Management	1.86	0.87	1.56	0.91	2.24	0.74	1.77	0.87	1.83	0.86	1.67	0.82	2.19	0.87
Personnel Security	1.55	0.86	1.33	0.83	2.00	0.71	1.40	0.82	1.63	0.91	1.36	0.82	1.71	0.94	
Societal security	Security Operations	1.82	0.87	1.64	0.96	2.10	0.77	1.81	0.85	1.86	0.94	1.73	0.84	1.81	0.83
	Cybercrime	1.74	0.91	1.94	0.95	1.62	0.86	1.67	0.87	1.80	0.93	1.61	1.00	1.81	0.87
	Cyber Law	1.62	0.91	1.75	0.84	1.55	0.83	1.63	0.93	1.40	0.85	1.48	1.03	1.94	0.93
	Cyber Policy	1.65	0.94	1.61	0.90	1.62	0.86	1.58	0.93	1.60	0.91	1.55	1.06	2.00	0.93
Operate & Maintain	Privacy	1.74	0.92	1.69	0.98	1.79	0.86	1.60	1.00	1.69	1.02	1.76	0.83	1.97	0.80
	Customer Serv. & Tech. Support	1.04	0.96	1.08	0.97	1.41	1.09	1.33	0.94	0.83	0.92	0.91	0.88	0.65	0.75

relevant to perform in the job; the value one (1) means that basic knowledge of the skill is needed to perform in the job; two (2) means that intermediate knowledge is needed; and three (3) means that advance knowledge is needed. Further details about this scale and the six job profiles can be found in Secs. 2.2 and 3.3 above.

Appendix B. Heatmap of survey results

While Table A.1 in Appendix A gives the numeric summaries of the assessments gathered, Fig. B1 (in page 18) shows a graphical representation of those values. The darker a circle in Fig. B1, the more important the skill for the corresponding job profile—i.e. the

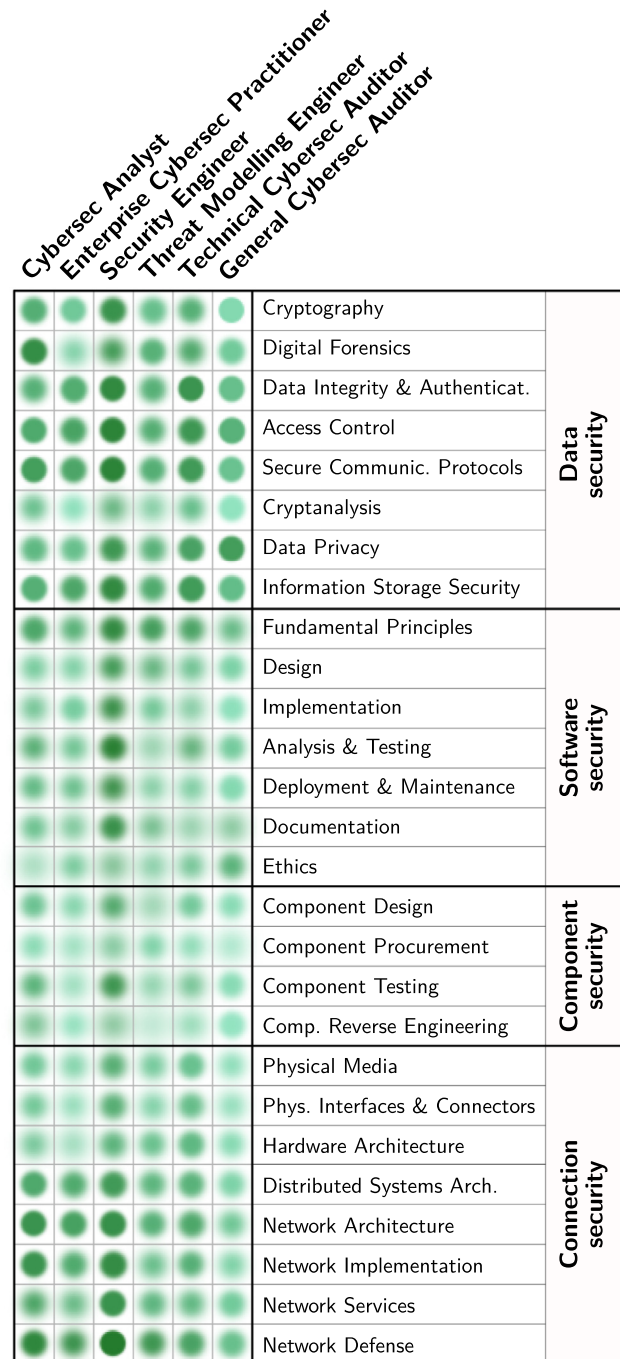
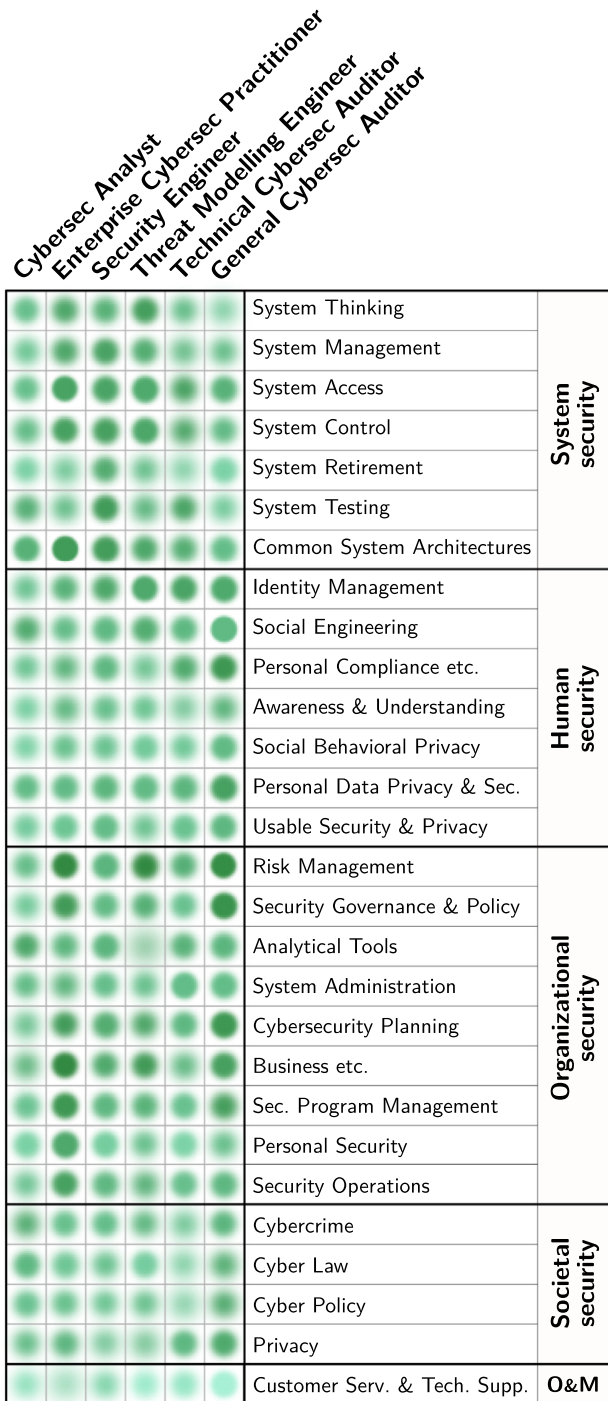


Fig. B1. Heatmap of skills assessment. The lightness of the circles indicates the average assessment by the respondents: from irrelevant = 0.0 (light green) to advanced = 3.0 (dark green). The diffusion of the circles indicates the standard deviation: from a minimum of 0.60 (well defined circle) to a maximum of 1.20 (very diffused circle). For instance, the average assessment of *Network Defence* (Connection security) for the Security Engineer profile is 2.63, and its standard deviation is 0.62. In contrast, for the profile of Threat Modelling Engineer, the average assessment of *Component Reverse Engineering* (Component security) is 1.51, and the stdev is 1.20.

higher the (mean) value of the skill chosen by our assessors. The standard deviation is represented as the diffusion of the circles.

This heatmap tries to convey a quick qualitative overview of the “clear hot skills” identified in our study, faster to pick up than the numeric values presented in Table A.1.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at [10.1016/j.cose.2022.103082](https://doi.org/10.1016/j.cose.2022.103082)

References

- Ahrend, J.M., Jirotko, M., Jones, K., 2016. On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge. In: *Proceedings of the International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*. IEEE, pp. 1–10.
- Karinsalo, A., Halunen, K., 2021. D6.3: Design of education and professional framework. https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Framework_Final.pdf.
- Alsmadi, I., Zarour, M., 2018. Cybersecurity programs in Saudi Arabia: issues and recommendations. In: *Proceedings of the ICCAIS*. ACM, pp. 1–5. doi:10.1109/CAIS.2018.8442013.
- Ang, B., 2021. Singapore: A Leading Actor in ASEAN Cybersecurity, 1 Routledge doi:10.4324/9780429399718.
- Armstrong, M.E., Jones, K.S., Namin, A.S., Newton, D.C., 2020. Knowledge, skills, and abilities for specialized curricula in cyber defense: results from interviews with cyber professionals. *ACM Trans. Comput. Educ.* 20 (4), 29:1–29:25. doi:10.1145/3421254.
- Bahrke, J., Grammenou, M., 2021. Commission to invest nearly € 2 billion from the Digital Europe Programme to advance on the digital transition. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5863.
- Catota, F.E., Morgan, M.G., Sicker, D.C., 2019. Cybersecurity education in a developing nation: the Ecuadorian environment. *J. Cybersec.* 5 (1). doi:10.1093/cybsec/tyz001.
- Council of the European Union, European Parliament, 2015. Directive 2015/2366 on payment services in the internal market, amending directives 2002/65/EC, 2009/110/EC and 2013/36/EU and regulation (EU) no 1093/2010, and repealing directive 2007/64/EC. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN>.
- Crick, T., Davenport, J.H., Irons, A., Prickett, T., 2019. A UK case study on cybersecurity education and accreditation. In: *Proceedings of the FIE*. IEEE Computer Society, pp. 1–9. doi:10.1109/FIE43999.2019.9028407.
- Cyber Security for Europe, 2018. CS4E website. (last accessed 2022), <https://cybersec4europe.eu/about/>.
- Dragoni, N., Lafuente, A.L., Massacci, F., Schlichtkrull, A., 2021. Are we preparing students to build security in? A survey of European cybersecurity in higher education programs [education]. *IEEE Secur. Priv.* 19 (01), 81–88. doi:10.1109/MSEC.2020.3037446.
- European Commission, 2022. Entry/Exit System (EES). https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en, (last accessed 2022).
- European Commission, 2021. The Digital Europe Programme. <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>, (last accessed 2022).
- European Cyber Security Organisation, 2021. European cybersecurity education and professional training: Minimum reference curriculum. <https://www.ecs-org.eu/documents/publications/61967913d3f81.pdf>, SWG 5.2.
- European Cyber Security Organisation, 2022. ECSO website. (last accessed 2022), <https://ecs-org.eu>.
- European Union Agency for Cybersecurity, 2022. ECSF, European Cybersecurity Skills Framework. European Union Agency for Cybersecurity doi:10.2824/859537.
- Furnell, S., Clarke, N., 2012. Power to the people? the evolving recognition of human aspects of security. *Comput. Secur.* 31 (8), 983–988. doi:10.1016/j.cose.2012.08.004.
- ISO/IEC 27000:2016, 2016. Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary. International Organization for Standardization. <https://www.iso.org/standard/66435.html>
- Joint Task Force on Computing Curricula, Association for Computing Machinery, IEEE Computer Society, 2013. Computer Science Curricula 2013. <http://ai.stanford.edu/users/sahami/CS2013/final-draft/CS2013-final-report.pdf>.
- Joint Task Force on Cybersecurity Education, 2018. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery. <https://dl.acm.org/citation.cfm?id=3184594>.
- Kortjan, N., von Solms, R., 2013. Cyber security education in developing countries: A South African perspective. In: *e-Infrastructure and e-Services for Developing Countries*. Springer Berlin Heidelberg, pp. 289–297. doi:10.1007/978-3-642-41178-6_30.
- McDuffie, E., Piotrowski, V., 2014. The future of cybersecurity education. *Computer* 47 (08), 67–69. doi:10.1109/MC.2014.224.
- McGettrick, A., 2013. Toward effective cybersecurity education. *IEEE Secur. Priv.* 11 (6), 66–68. doi:10.1109/MSP.2013.155.
- Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019. A proposal for a European cybersecurity taxonomy. Technical Report. Joint Research Centre (EC) doi:10.2760/106002.
- Dragoni, N., Lafuente, A., Schlichtkrull, A., Zhao, L., 2020. D6.2: Education and training review. <https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submitted.pdf>.
- Network, E. C. C., 2022. CCN website. (last accessed 2022), <https://cybercompetencenetwork.eu/about/>.
- Nodeland, B., Belshaw, S., Saber, M., 2019. Teaching cybersecurity to criminal justice majors. *J. Crim. Justice Educ.* 30 (1), 71–90. doi:10.1080/10511253.2018.1439513.
- Nurse, J., Adamos, K., Grammatopoulos, A., Di Franco, F., 2021. Addressing the EU cybersecurity skills shortage and gap through higher education. <https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education>, European Union Agency for Cybersecurity (ENISA).
- van Oorschot, P.C., 2022. A view of security as 20 subject areas in four themes. *IEEE Secur. Priv.* 20 (1), 102–108. doi:10.1109/MSEC.2021.3130744.
- Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T., 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Comput. Secur.* 66, 40–51. doi:10.1016/j.cose.2017.01.004.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C., 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Comput. Secur.* 42, 165–176. doi:10.1016/j.cose.2013.12.003.
- Penchev, G., Shalamanova, A., 2020. A governance model for an EU cyber security collaborative network-ECSCON. *Inf. Secur. Int. J.* 46, 99–113.
- Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., Witte, G., 2020. NIST special publication 800-181, revision 1 – workforce framework for cybersecurity (NICE Framework). 10.6028/NIST.SP.800-181r1
- Task Group on Information Technology Curricula, Association for Computing Machinery, IEEE Computer Society, 2017. Information technology curricula 2017. <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/it2017.pdf>.
- The National Cyber Security Centre, 2019. The cyber security body of knowledge. <https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf>, Crown Copyright, licensed under the Open Government Licence v3.0.



Carlos E. Budde received his PhD in Computer Science in 2017 from the Universidad Nacional de Córdoba (AR), specialising in rare event simulation for formal methods. From 2017 to 2021 he worked as postdoc researcher at the Universiteit Twente (NL), also in collaboration with Dutch Railways, applying simulation and machine learning to big data for risk management. Since 2021 Carlos holds a position as assistant professor at the Università di Trento (IT), using simulation-based analyses to assess the cybersecurity resilience of systems' models.



Anni Karinsalo is working as a Senior Scientist in the Applied Cryptography team at VTT Technical Research Centre of Finland. Throughout her research career starting from 2004, she has been working as a project leader and researcher covering fields of cybersecurity such as security metrics and critical infrastructure security. Her latest research interests include post-quantum cryptography and distributed ledger technologies.



Silvia Vidor received her Master's Degree in International Security Studies in 2020 from the University of Trento and Sant'Anna School of Advanced Studies with a thesis on Lethal Autonomous Weapons Systems. Since 2021, Silvia works as a research fellow at the University of Trento. She is also the Head of Research of the Italian association Privacy Network.



Mr. Jarno Salonen is working as a Senior Scientist in the Applied cybersecurity team at VTT Technical Research Centre of Finland. He has a professional background of over 20 years in making the digital world a better place for ordinary users especially in the areas of cybersecurity, privacy, resilience and development of electronic services. He is the representative of VTT in two of the working groups in European Cyber Security Organisation (ECISO), founding member of the North European Cybersecurity Cluster (NECC), member of the Finnish Information Security Cluster (FISC) management team, vice-chair for Association of Finnish Defence and Aerospace Industries (AFDA) cyber group and his work has been published in

several scientific journals and conferences.



Fabio Massacci (PhD in Computer Engineering, University of Rome "La Sapienza") is a full professor at the University of Trento, Italy, and at Vrije Universiteit, The Netherlands. He published 250+ peer-reviewed papers and received the Ten Years Most Influential Paper award by the IEEE RE'15 Conference for his work on security requirements. He coordinated several EU projects including SEC-ONOMICS "Socio-economics meet security"; he leads the H2020 AssureMOSS project, and participates in the Cyber-Sec4Europe pilot. He also participates in the CVSS SIG—the world standard on vulnerabilities—and is a member of the IEEE.