Are We Preparing Students to Build Security In?

A Survey of European Cybersecurity Higher Education Programmes

N. Dragoni
Technical University of Denmark

A. Lluch Lafuente
Technical University of Denmark

F. Massacci
University of Trento and Vrije Universiteit Amsterdam

A. Schlichtkrull
Aalborg University Copenhagen

***Abstract*—**
We present a review of European MSc programmes in cybersecurity and reflect on the presence (and lack of) knowledge and skills needed to build security in.

Industry and government organisations have been using encryption to protect the data at rest and data in transit in ICT networks for several decades. Only in the last 10-20 years, there has been a growing interest to *build security in* [1], with 'security & privacy-by-design' being a recent buzzword. As a result of past history, traditional skills are well anchored (e.g. almost every university has a cryptography course), but we do not know how prevalent courses that teach building security in topics are, as offered by European MSc programs in cybersecurity. This paper aims to answer the following question:

Are (European) universities preparing students to build security in?

To answer our question, a reasonably good approach is to ask directors of studies of educational programs about their offering, and then check how well *building security in* topics fare into the classroom. We report here the review of more than 100 European MSc programmes from 28 countries in cybersecurity at the University level [2] and look forward to extend this survey to more countries. Fig. 1 shows the countries represented in the survey.

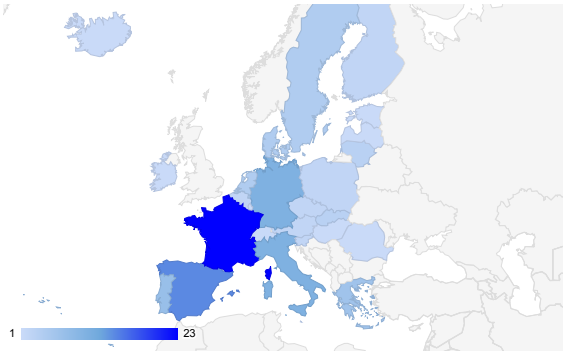

Figure 1. Number of education programmes in the survey distributed by country. The darker the blue is, the more programmes participated and 19 is the maximum.

Our main finding is that the current landscape of education programmes does not seem to put the required emphasis in *building security in* skills.

Published by the IEEE Computer Society

Table 1. Cybersecurity Knowledge Frameworks

Framework	Owners	Focus	Structure
CSEC	ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8	Academic Curriculum	8 areas / 54 KUs
CFW	NIST	Workforce Skills	7 categories / 33 specialty areas
JRC	JRC	Research & Technology	15 research domains / 150 subdomains
CyBOK	NCSC	Scientific Knowledge	19 KAs / 244 topics

Structuring Cybersecurity Knowledge

There is no silver bullet answer to the question of how to become a (software) security expert [3] but we take guidance from Dan Geer's introduction to Gary McGraw's 'Building Security In' [4] to identify features indicative of building security in:

> [...] baking in security only happens when there is *intent* to do so. [...] You convert rare expertise into *a process that others can follow*, but the kind of process has to be one that reinforces disciplined thinking [...] and *can be measured* sufficiently well to know if it works. Better still if [...] you can *get real value out of doing only some of it*. [Our emphasis]

While all cybersecurity topics are important, here we have a clear emphasis on the design, intentional, and process aspects also advocated by CMU SEI [5], [6]. In our work we seek to identify these aspects in the teaching programmes delivered by each educational institution.

Cybersecurity encompasses many different concepts, techniques, methodologies, and tools. To define a common set of elements of courses we look for, we surveyed first several existing cybersecurity frameworks (cf. Table 1):

- The ACM *Cybersecurity Curricular Guidelines* (ACM) [7].
- The NIST-NICE *Cybersecurity Workforce Framework* (NICE) [8].
- The European Joint Research Centre *European Cybersecurity Taxonomy* (JRC) [9].
- The *Cyber Security Body of Knowledge* (CyBOK) [10].

While they all provide a good basis for academic curricula, we decided to base our survey mainly on the ACM framework because the target of the survey is composed of heads of studies and faculty members, who may arguable have more familiarity with the scientific terminology of the ACM. We slightly enriched the ACM framework with the NIST area *Operate and Maintain* for which we could not find an immediate mapping to areas and knowledge units in the ACM framework. The resulting ACM+NIST framework is summarised in Table 2 where each *Knowledge Area* (KA) is broken down into several smaller *Knowledge Units* (KUs).

We mention two other examples which are suitable to structure education in *building security in*: the software assurance (SwA) curriculum [11], which provides an MSc curricular framework, and the related SwA competency model [12] which provides a structured model for training and education beyond University education. Starting with [3], [5] and [6], most authors emphasize the importance of skills in security design, understanding and assessing threats, and automated security analysis and testing of newly developed and externally procured software components. Table 2 highlights the dozen of KUs that we think are most relevant to those skills.

Questioning Europe

To obtain a snapshot of the Higher Education landscape we used a questionnaire that, for each KU, required to indicate the degree to which it is covered: by mandatory courses, by optional courses, or not covered at all.

The questionnaire was distributed among faculty members with relevant roles in the education programmes, typically the head of the education or a faculty member. We exploited the vast network of the European project CyberSec4Europe [13] and other channels, including national mailing lists and the ENISA map of cybersecurity education programmes [14]. *The survey is still open* [15] and not limited to Europe.

The key summary results presented here are

Table 2. The ACM+NIST Framework. The design and process skills more relevant to *building security in* are highlighted.

KA	KUs
Data Security	1 Cryptography, 2 Digital Forensics, 3 Data Integrity and Authentication, 4 Access Control, 5 Secure Communication Protocols, 6 Cryptanalysis, 7 Data Privacy, 8 Information Storage Security
Software Security	9 Fundamental Principles, 10 Design, 11 Implementation, 12 Analysis and Testing, 13 Deployment and Maintenance, 14 Documentation, 15 Ethics
Component Security	16 Component Design, 17 Component Procurement, 18 Component Testing, 19 Component Reverse Engineering
Connection Security	20 Physical Media, 21 Physical Interfaces and Connectors, 22 Hardware Architecture, 23 Distributed Systems Architecture, 24 Network Architecture, 25 Network Implementations, 26 Network Services, 27 Network Defense
System Security	28 System Thinking, 29 System Management, 30 System Access, 31 System Control, 32 System Retirement, 33 System Testing, 34 Common System Architectures
Human Security	35 Identity Management, 36 Social Engineering, 37 Personal Compliance with Cybersecurity Rules/Policy/ Ethical Norms, 38 Awareness and Understanding, 39 Social and Behavioral Privacy, 40 Personal Data Privacy and Security, 41 Usable Security and Privacy
Organizational Security	42 Risk Management, 43 Security Governance and Policy, 44 Analytical Tools, 45 Systems Administration, 46 Cybersecurity Planning, 47 Business Continuity, Disaster Recovery, and Incident Management, 48 Security Program Management, 49 Personnel Security, 50 Security Operations
Operate and Maintain	51 Customer Service and Technical Support
Societal Security	52 Cybercrime, 53 Cyber Law, 54 Cyber Ethics, 55 Cyber Policy, 56 Privacy

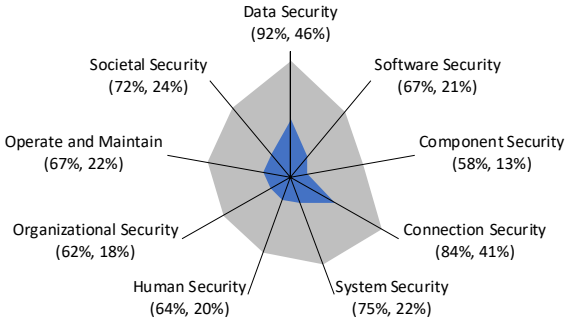

Figure 2. Average global coverage of KAs. The shapes show for each KA the average percentage that are covered by universities with mandatory courses (blue), and with non-mandatory ones (grey). Traditional KAs like Data, Connection, and System Security are well covered by mandatory courses. Other KAs are more of an 'optional' kind.

based on over one hundred MSc education programmes from higher education institutions in European countries. The map of participant institutions is available on a dedicated web page.[1] Further details on our methodology to gather and validate the data can be found in [2].

At a bird's eye view, all cybersecurity KUs seem covered to some extent and there is no single cybersecurity KA being entirely neglected. Fig. 2 shows as a star plot[2] to which extent our ACM+NIST framework's KAs are covered by the educational programmes.[3] Each of the plot's spokes (the black lines) corresponds to a KA. The part of each spoke covered in blue is proportional to the coverage proportion with mandatory courses of the corresponding KA – the maximal magnitude possible being 100 percent. The grey part extends the blue and from this we can read the coverage proportion with any kind of course of the corresponding KA. The results also show a skewed distribution of how topics are covered by mandatory courses. Digging deeper we find more interesting results.

Traditional vs New Areas

In Fig. 4 we give a quick overview of the coverage of each KA's KUs. Here each KA is represented by a star plot where its KU are represented as spokes. The part of each spoke covered in blue corresponds to the percentage of the education programmes covering the KU with mandatory courses and grey representing coverage with other courses.

Most noticeably, and, perhaps, not surprisingly, traditional KAs of *data security* and *connection security* are covered to the largest extent.

[1] https://cybersec4europe.eu/cyber-security-msc-education-survey-map

[2] https://www.itl.nist.gov/div898/handbook/eda/section3/starplot.htm

[3] Detailed numbers can be found at [2].

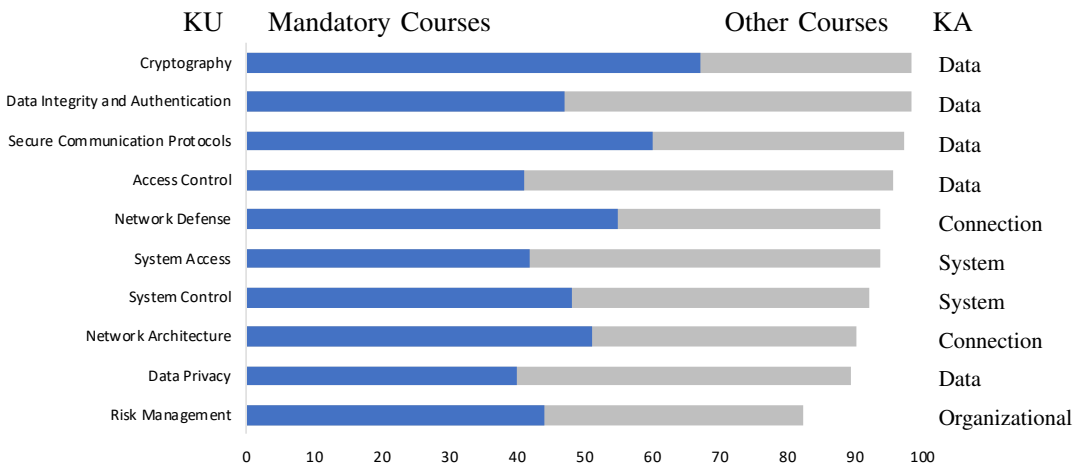

Figure 3. Top 10 most covered KUs in European MSc programmes. The bars show the percentage of the education programmes covering the KU with mandatory courses (blue), and with other courses (grey). A quick look at the potential building security in KUs in Table 2 shows that only Risk Analysis and Network Architecture made it to the top ten.

Fig. 3, provides an overview of how the most popular KUs are covered, with cryptography, not unexpectedly, occupying the first place.

By contrast, our results show that the KA of *component security* and *operate and maintain* are clearly the least covered (cf. Fig. 2). But they also show that not all KAs are covered consistently (cf. Fig. 4), and that several popular KAs contain KUs whose coverage proportions are very low (cf. Fig. 4). A significant example is the KU *component procurement*, which belongs to the otherwise popular KA of *system security* and is practically not covered at all (cf. Fig. 5). This is quite worrying given the unavoidable need to use third-party components, as well as the common practice of public sectors to offer time-limited contracts to IT providers.

What about Building Security In?

Our results show that the KUs that are more relevant to building security in are not covered to a good extent. *Design*, arguably the flagship *buliding security in* KU, is entirely neglected in a quarter of the education programmes surveyed and only a third make it mandatory.

On the bottom of the rank, we found the already discussed KU of *component procurement*, a topic that most approaches to building security in consider of utmost importance given that, nowadays, it is hardly conceivable to develop

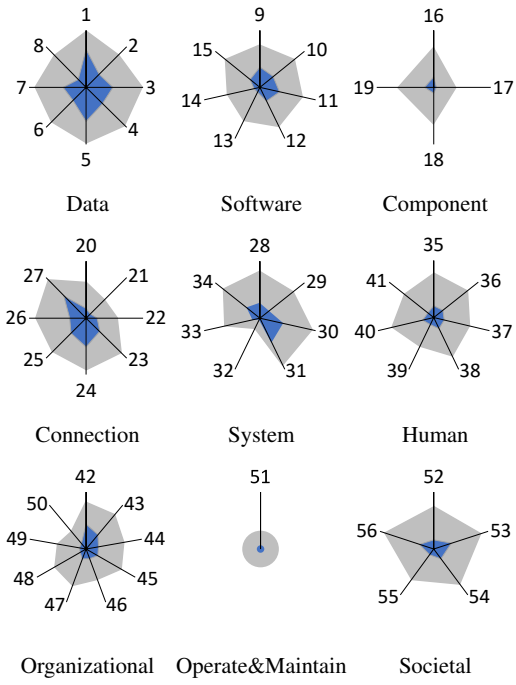

Figure 4. The coverage of each of the KA's KUs. The numbers correspond to the numbers of the KUs from table 2. The shapes show the percentage of the education programmes covering the KU with mandatory courses (blue), and with other courses (grey). Data Security is well represented while other KA such as Software and Organizational Security are less so.

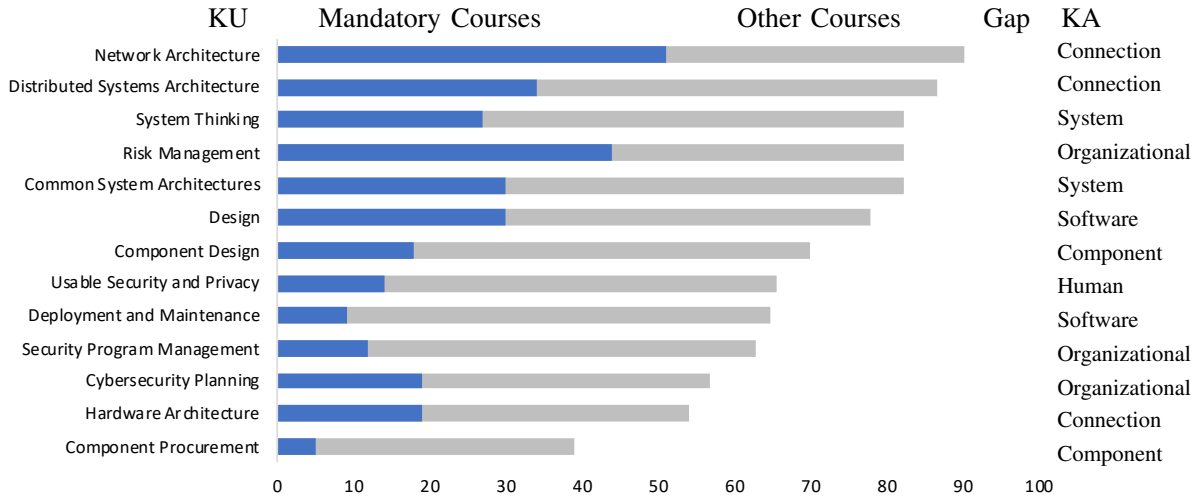

Figure 5. Coverage of *building security in* KUs in European MSc programmes

software without resorting to third-party libraries and components.

Is there a Difference by Country?

Unsurprisingly, large countries show higher coverage of KUs (i.e. there is at least one education programme covering each KU in the country). For example when considering the strictest coverage metric, Spain, France, Germany, and Italy cover 75% of the KUs with mandatory courses. However, size of the country is not a decisive factor. Some smaller countries have a good coverage (see Figure 6).

This might, of course, be also the result of bias and over claiming (or being too modest) by some directors of studies so this data should be interpreted with care.

Countries with higher coverage of the KUs tend to have a more uniform distribution of the coverage of each KA, whereas countries with lower coverage of the KAs exhibit 'peaks of excellence' (see Figure 7).

There are countries that seem to neglect certain KAs even though their education programmes cover a large proportion of the KAs with mandatory courses. An example is Sweden, which ranks fifth on global coverage with mandatory courses thanks to individual KUs that are covered almost entirely, while they do not cover the *component security* KA at all with mandatory courses. See again figure 7.

Conclusions

We believe that our findings will help decision makers, such as heads of study programmes and policy makers, to identify, prioritize and demand skills taught by European MSc in cybersecurity needed by industry and government. *Building security in* approaches are needed to ensure that future IT systems are less vulnerable to attacks than today's systems, and such approaches require specialised skills.

Further details on our survey can be found in [2]. We look forward to your opinion and, if you are involved in a programme, do not forget to participate in the survey [15]!

Acknowledgements

This work has been supported by the EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe (cybersec4europe.eu). The authors would like to thank all members of CyberSec4Europe for the dissemination of the survey and for reaching out to key persons in higher education institutions throughout Europe, as well as all people and institutions that participated to the survey. The authors are also grateful to Ross Anderson, Joseph Hallett, Andrew Martin, Gary McGraw, Jelena Mirkovic, Wiliam Newhouse, and Awais Rashid, and, for their fruitful comments and suggestions on early versions of this work.

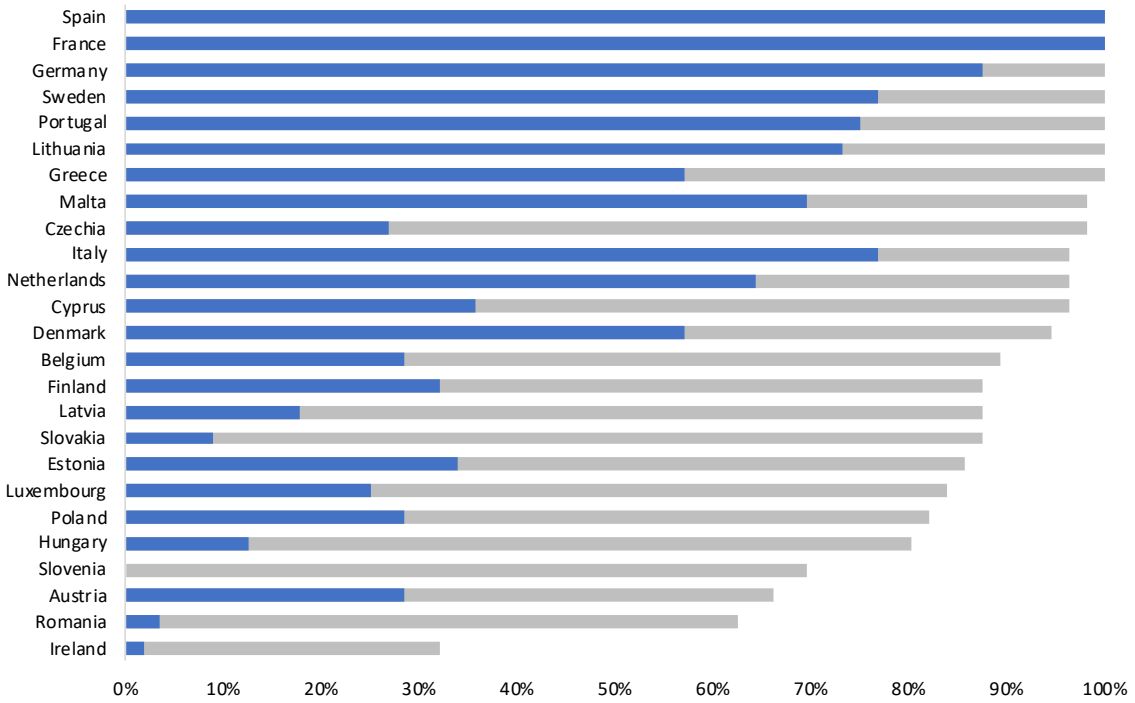

Figure 6. The percentage of the KUs that each country covers with mandatory courses (blue) and other courses (grey).

REFERENCES

1. J. Viega and G. McGraw, *Building Secure Software: How to Avoid Security Problems the Right Way (paperback)(Addison-Wesley Professional Computing Series)*. Addison-Wesley Professional, 2011.
2. N. Dragoni, A. Lluch Lafuente, A. Schlichtkrull, and L. Zhao, "D6.2 Education and Training Review," 2020, available at https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf.
3. M. Howard, "Becoming a security expert," *IEEE Security Privacy*, vol. 6, no. 1, pp. 71–73, 2008.
4. G. McGraw, *Software Security: Building Security In*. Addison-Wesley Professional, 2006.
5. N. R. Mead and T. B. Hilburn, "Building security in: Preparing for a software security career," *IEEE Security Privacy*, vol. 11, no. 6, pp. 80–83, 2013.
6. T. B. Hilburn and N. R. Mead, "Building security in: A road to competency," *IEEE Security Privacy*, vol. 11, no. 5, pp. 89–92, 2013.
7. CSEC2017 Joint Task Force, "Cybersecurity Curricula 2017 - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," 2017, available at https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.
8. Newhouse, K. W., B. S. Scribner, and G. Witte, "NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," 2017, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.
9. I. Fovino, R. Neisse, J. H. Ramos, N. Polemi, G. Ruzzante, M. Figwe, and A. Lazari, "A Proposal for a European Cybersecurity Taxonomy," 2019, available at https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf.
10. R. A., Chivers, H. Danezis, G. Lupu, E., and A. Martin, "The Cyber Security Body of Knowledge," 2019, version 1.0. [Online]. Available: https://www.cybok.org/
11. N. Mead, J. Allen, M. Ardis, T. Hilburn, A. Kornecki, R. Linger, and J. McDonald, "Software assurance curriculum project volume i: Master of software assurance reference curriculum," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU/SEI-2010-TR-005, 2010. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9415
12. T. Hilburn, M. Ardis, G. Johnson, A. Kornecki, and N. Mead, "Software assurance competency model,"

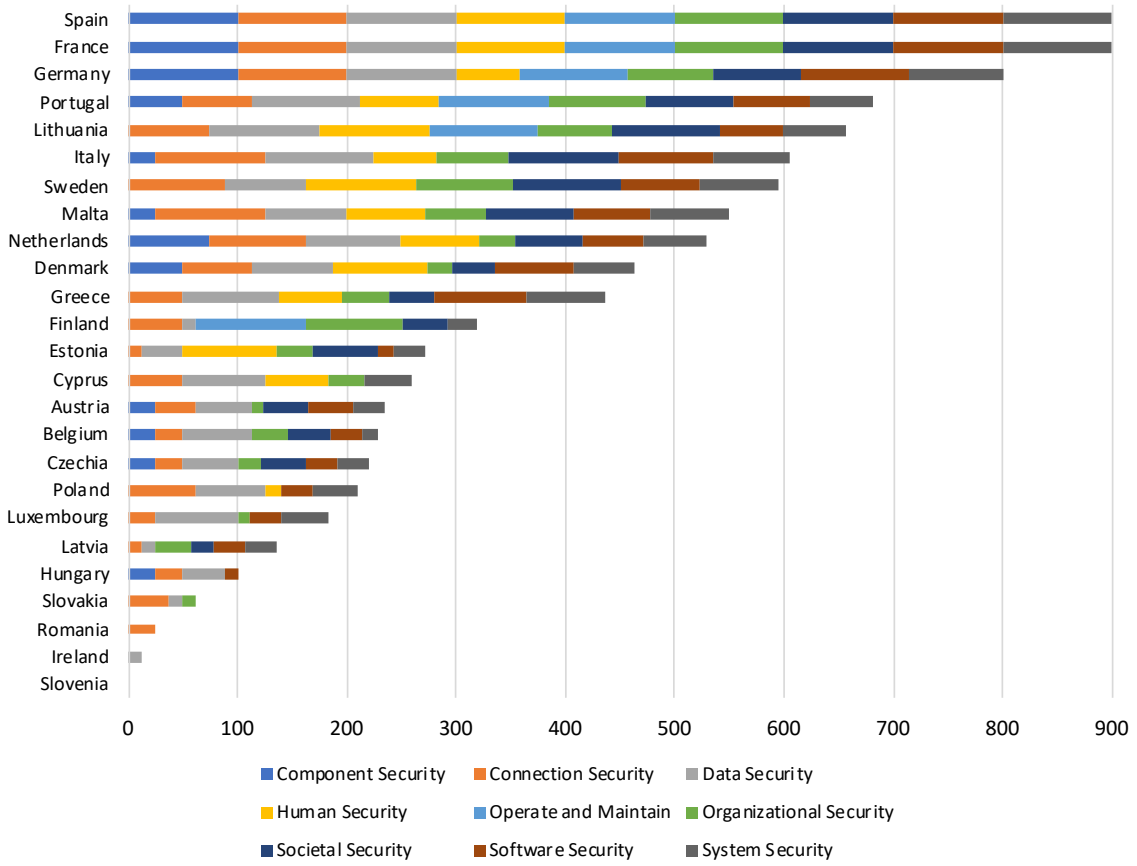

Figure 7. Percentage of each KA's KUs covered with mandatory courses for each country. Each KA is represented by a colour as shown above. The bar diagram considers a KU covered by a country if there is at least one education programme of the country that covers the KU with mandatory courses. The bar diagram shows for each country the percentage of KUs that are covered in each KA. Since there are 9 KAs, the total possible percentage per country is 900.

Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU/SEI-2013-TN-004, 2013. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=47953

13. "CyberSec4Europe," https://www.cybersec4europe.eu.
14. ENISA, "Education map," available at https://www.enisa.europa.eu/topics/cybersecurity-education/education-map.
15. CS4E, "Survey of higher cybersecurity education," https://ec.europa.eu/eusurvey/runner/CS4E_MSc_Survey_2019.

Nicola Dragoni (MSc'02, PhD'06) is professor at the Technical University of Denmark, where he also serves as deputy head of the PhD School and head of the Digital Security center. He is also part-time professor at Örebro University. He is active in a number of national and international projects. Contact him at ndra@dtu.dk.

Alberto Lluch Lafuente (MSc'99, PhD'03) is associate professor at the Technical University of Denmark and head of the the section on formal methods for safe and secure systems. He is the leader of the software development lifecycle research task of the CyberSec4Europe pilot. Contact him at albl@dtu.dk.

Fabio Massacci (MSc'93, PhD'98) is professor at the University of Trento and the Vrije Universiteit Amsterdam. He is the recipient of the Ten Years Most Influential paper award by the IEEE Requirement Engineering Conference

in 2015. He is the leader of the education WP of the CyberSec4Europe pilot and the coordinator of the AssureMOSS project on the security of open source software. Contact him at fabio.massacci@ieee.org.

Anders Schlichtkrull (MSc'15, PhD'18) is assistant professor at Aalborg University Copenhagen. He is a recipient of the Technical University of Denmark's Young Researcher Award 2019. He contributed to several tasks of the CyberSec4Europe pilot. Contact him at andsch@cs.aau.dk.