Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs

Nicola Dragoni | Technical University of Denmark
Alberto Lluch Lafuente | Technical University of Denmark
Fabio Massacci | University of Trento and Vrije Universiteit Amsterdam
Anders Schlichtkrull | Aalborg University Copenhagen

We present a review of European master of science programs in cybersecurity and reflect on the presence (and lack) of knowledge and skills needed to build security in.

Industry and government organizations have been using encryption to protect the data at rest and data in transit in information and communications technology networks for several decades. Only in the last 10–20 years has there been a growing interest to "build security in,"[1] with "security and privacy-by-design" being a recent buzz phrase. As a result of past history, traditional skills are well anchored (for example, 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 master of science (M.Sc.) programs in cybersecurity.

This article 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 the directors of studies of educational programs about their offerings and then check how well building security in topics fare in the classroom. We report here a review of more than 100 European M.Sc. programs in cybersecurity at the university level[2] from 28 countries, and we look forward to extending this survey to more countries. Figure 1 shows the countries represented in the survey.

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

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 the Carnegie Mellon University Software Engineering Institute.[5,6] In our work, we seek to identify these aspects in the teaching programs delivered by each educational institution.

Cybersecurity encompasses many different concepts, techniques, methodologies, and tools. To define a common set of elements in the courses we

Digital Object Identifier 10.1109/MSEC.2020.3037446
Date of current version: 25 January 2021

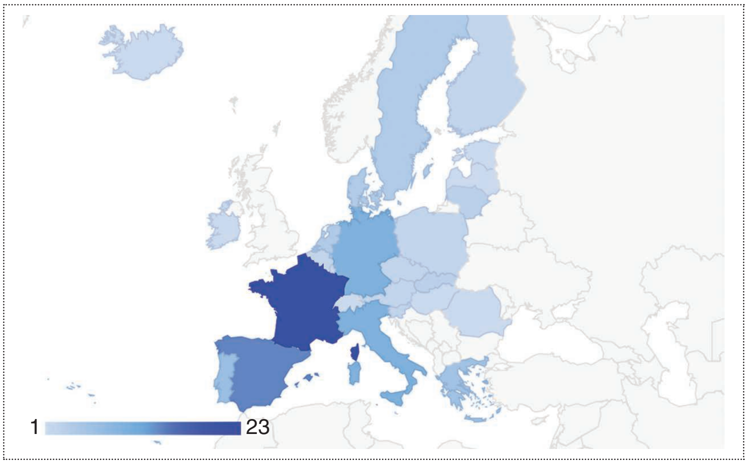


Figure 1. The number of education programs in the survey, distributed by country. The darker the blue is, the more programs participated; 19 is the maximum.

looked for, we first surveyed several existing cybersecurity frameworks:

- Association of Computing Machinery (ACM) Cybersecurity Curricular Guidelines[7]
- The National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education Cybersecurity Workforce Framework[8]
- The European Joint Research Centre (JRC) European Cybersecurity Taxonomy[9]
- The Cyber Security Body of Knowledge (CyBOK).[10]

Table 1 gives an overview of the various frameworks and their focus and structure. While these frameworks 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 arguably have more familiarity with the scientific terminology of 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 summarized in Table 2, where each knowledge area (KA) is broken down into several smaller knowledge units (KUs).

We mention two other examples that are suitable to structure education in building security in: the software assurance (SwA) curriculum,[11] which provides an M.Sc. curricular framework, and the related SwA competency model,[12] which provides a structured model for training and education beyond a university education. Starting with Howard,[3] Mead and Hilburn,[5] and Hilburn and Mead,[6] most authors emphasize the importance of skills in security design, the understanding and assessment of threats, automated security analysis, and the 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 required the responder to indicate the degree to which each KU 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 programs, typically the head of education or a faculty member. We exploited the vast network of the European project CyberSec4Europe[13] as well as other channels, including national mailing lists and the European Union Agency

Table 1. The cybersecurity knowledge frameworks.

Framework	Owners	Focus	Structure
CSEC	ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8	Academic curriculum	8 areas/54 KUs
CWF	NIST	Workforce skills	7 categories/33 specialty areas
JRC	JRC	Research and technology	15 research domains/150 subdomains
CyBOK	NCSC	Scientific knowledge	19 KAs/244 topics

CS: Computer Society; AIS: Association for Information Systems; SIGSEC: Special Interest Group in Information Security and Privacy; IFIP WG: International Federation for Information Processing Working Group; NCSC: National Cyber Security Centre; JRC: European Union Joint Research Center; CWF: National Initiative for Cybersecurity Education Cybersecurity Workforce Framework.

Table 2. The ACM+NIST Framework.

KA	KU
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

The design and process skills more relevant to building security in *are bold.*

for Cybersecurity map of cybersecurity education programs.[14] The survey is still open[15] and is not limited to Europe.

The key summary results presented here are based on more than 100 M.Sc. education programs from higher education institutions in European countries. The map of the participating institutions is available on a dedicated webpage (https://cybersec4europe.eu/cyber-security-msc-education-survey-map). Further details on our methodology to gather and validate the data can be found in Dragoni et al.[2]

From a bird's-eye view, all cybersecurity KUs seem covered to some extent, and there is no single cybersecurity KA being entirely neglected. Figure 2 illustrates a star plot (https://www.itl.nist.gov/div898/handbook/eda/section3/starplot.htm), the extent to which our ACM+NIST framework's KAs are covered by the educational programs. Detailed numbers can be found in Dragoni et al.[2] Each of the plot's spokes (black lines)

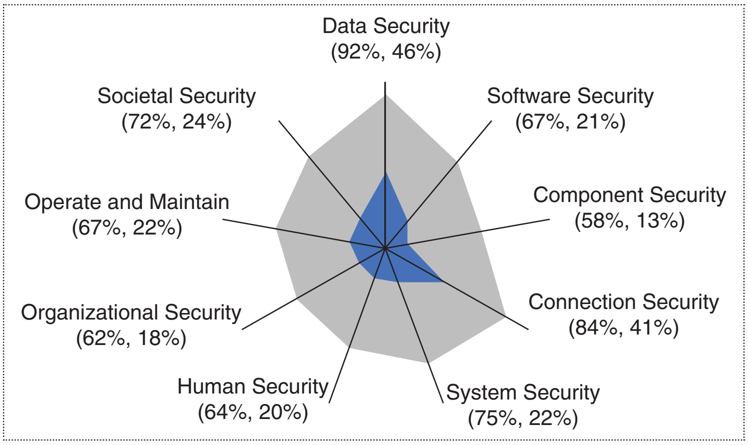


Figure 2. The average global coverage of KAs. The shapes display for each KA the average percentage that is covered by universities with mandatory courses (blue) and with nonmandatory ones (gray). Traditional KAs like data, connection, and system security are well covered by mandatory courses. Other KAs are more of an optional kind.

correspond 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%. The gray 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 Versus New Areas

In Figure 3, we give a quick overview of the coverage of each KA's KUs. Here, each KA is represented by a star plot, and its KUs are represented as spokes. The part of each spoke covered in blue corresponds to the percentage of the education programs covering the KU by mandatory courses, with gray representing coverage by other courses.

Most noticeably and, perhaps, not surprisingly, the traditional KAs of data security and communication

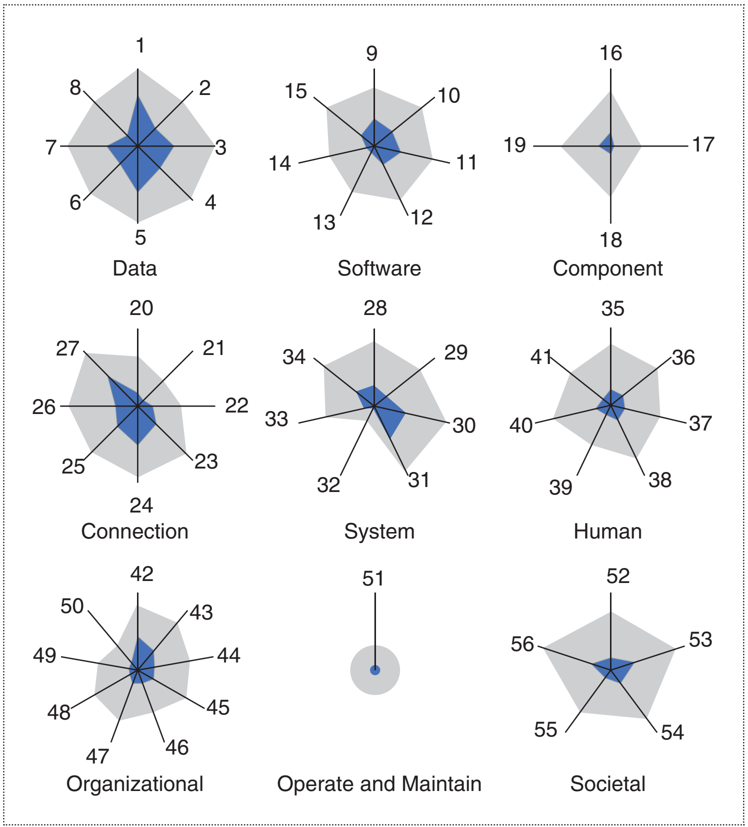


Figure 3. The top 10 most covered KUs in European M.Sc. programs. The bars show the percentage of the education programs covering the KU with mandatory courses (blue) and with other courses (gray). A look at the potential building security in KUs in Table 2 demonstrates that only risk analysis and network architecture made it to the top 10.

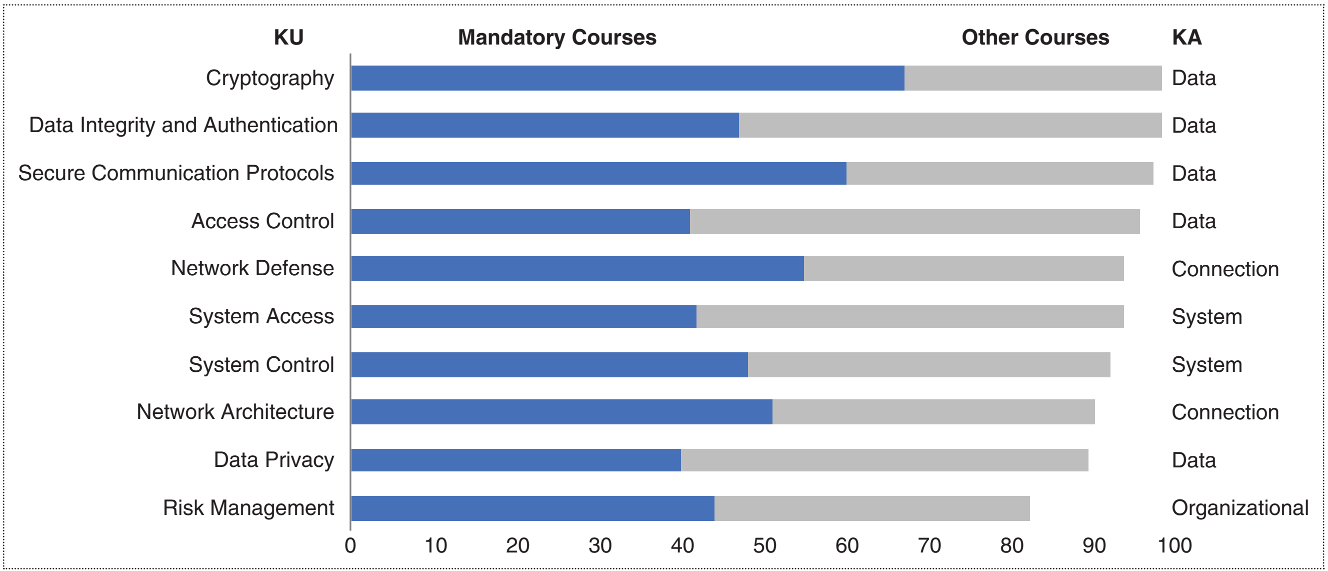


Figure 4. The coverage of each of the KA's KUs. The numbers correspond to the numbers of the KUs from Table 2. The shapes show the percentage of the education programs covering the KU with mandatory courses (blue) and with other courses (gray). Data security is well represented, while other KAs such as software and organizational security are less so.

security are covered to the largest extent. Figure 4 provides an overview of how the most popular KUs are covered, with cryptography, not unexpectedly, occupying the first place.

By contrast, our results indicate that the KAs of component security and operate and maintain are clearly the least covered (Figure 3). But they also show that not all KAs are covered consistently, and that several popular KAs contain KUs whose coverage proportions are very low (Figure 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 (Figure 5). This is quite worrying given the unavoidable need to use third-party components

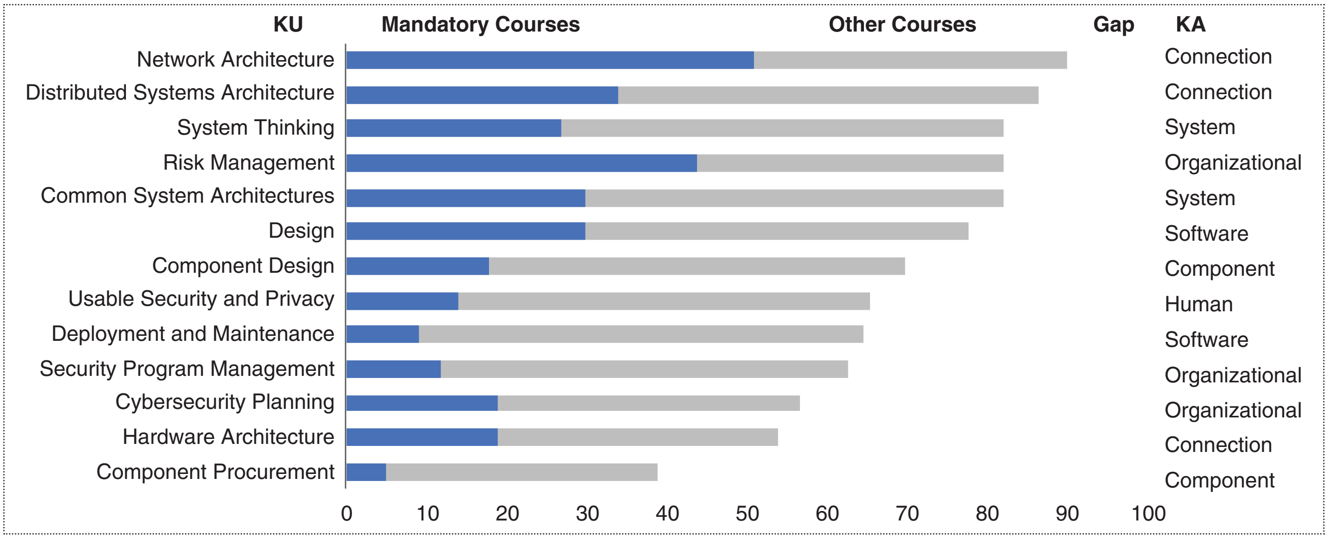


Figure 5. The coverage of building security in KUs in European M.Sc. programs.

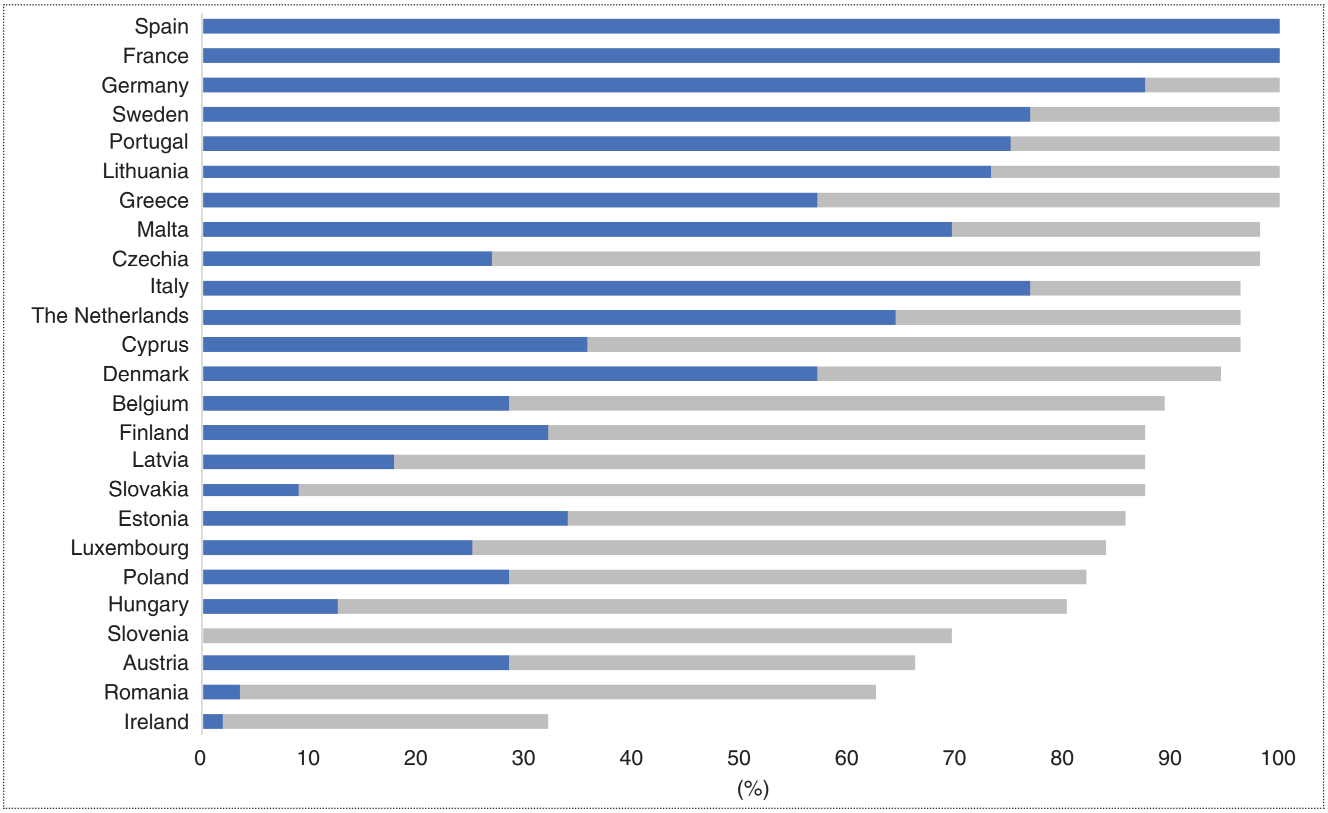


Figure 6. The percentage of the KUs that each country covers with mandatory courses (blue) and other courses (gray).

as well as the common practice of public sectors offering time-limited contracts to IT providers.

What About Building Security in?

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

At the bottom of the rank, we found the KU component procurement. This is a topic that most of the approaches to building security in consider of the utmost importance given that, nowadays, it is hardly conceivable to develop software without resorting to third-party libraries and components.

Is There a Difference by Country?

Unsurprisingly, large countries show a higher coverage of KUs (that is, there is at least one education program 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, the size of the country is not a decisive factor. Some smaller countries have good coverage as well (Figure 6). This might, of course, also be the result of bias and over claiming (or being too modest) by some directors of studies; thus, the data should be interpreted with care.

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

There are countries that seem to neglect certain KAs, even though their education programs cover a large proportion of the KAs with mandatory courses. An example is

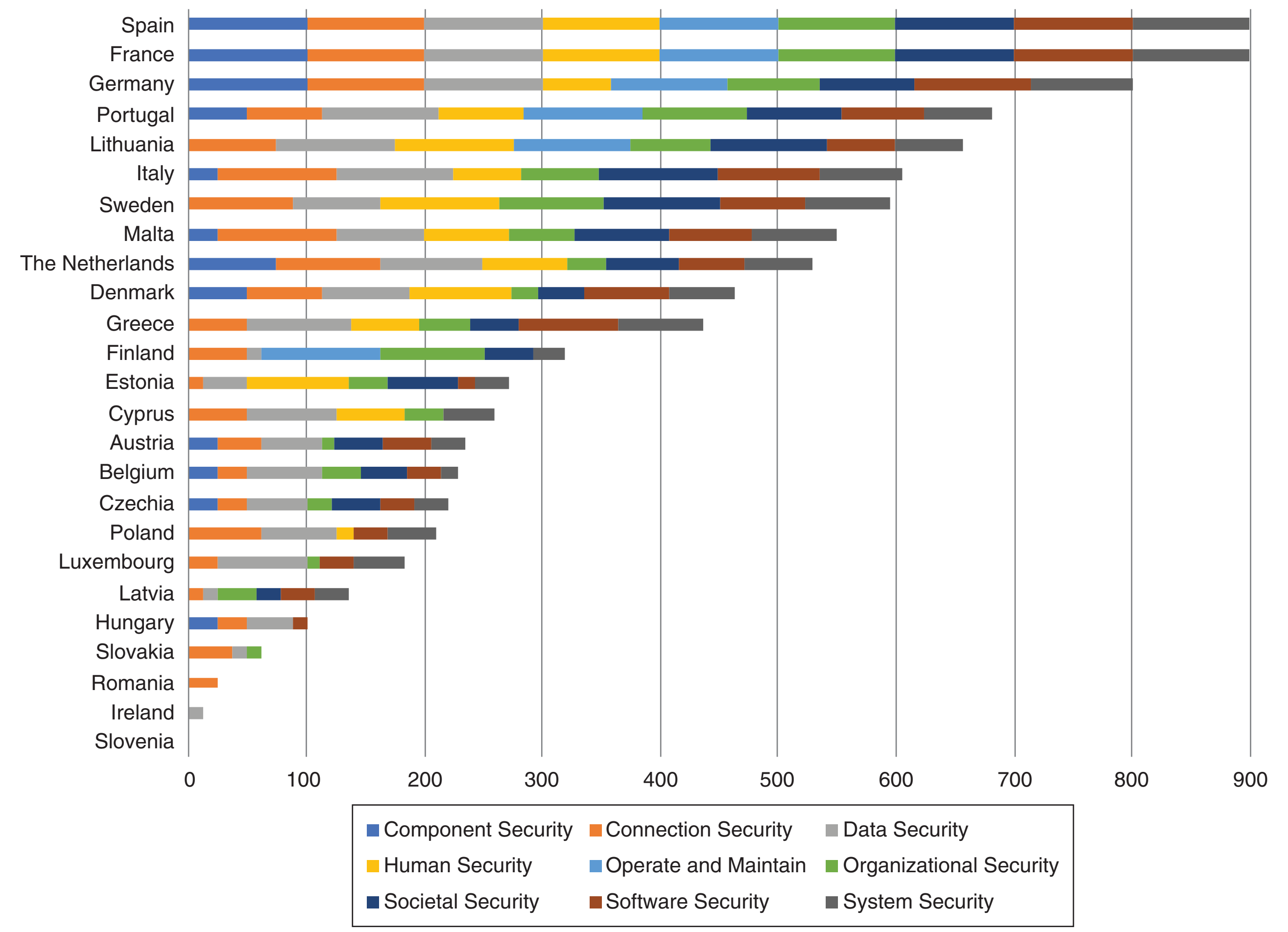


Figure 7. The percentage of each KA's KUs covered with mandatory courses for each country. Each KA is represented by a color. The bar diagram considers a KU covered by a country if there is at least one education program in the country that covers the KU with mandatory courses. The bar diagram shows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

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 (Figure 7).

We believe that our findings will help decision makers, such as the heads of study programs and the policy makers, to identify, prioritize, and demand that the skills needed by industry and government be taught by European M.Sc. programs in cybersecurity. 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 specialized skills.

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

Acknowledgments

This work was supported by the European Union Horizon 2020 Security Union Information and Communication Technologies-03–2018 Project 830929 CyberSec4Europe (cybersec4europe.eu). The authors would like to thank all of the 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 of the people and institutions that participated in the survey. The authors are also grateful to Ross Anderson, Joseph Hallett, Andrew Martin, Gary McGraw, Jelena Mirkovic, William Newhouse, and Awais Rashid and for their fruitful comments and suggestions on early versions of this work.

References

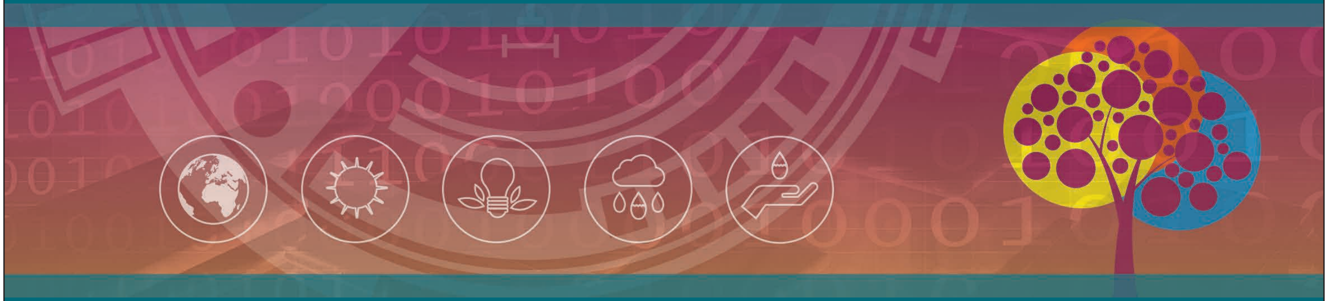
1. J. Viega and G. McGraw, *Building Secure Software: How to Avoid Security Problems the Right Way*. Reading, MA: Addison-Wesley, 2011.
2. N. Dragoni, A. Lluch Lafuente, A. Schlichtkrull, and L. Zhao, "D6.2 education and training review," Cybersec4europe, 2020. [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf
3. M. Howard, "Becoming a security expert," *IEEE Security Privacy*, vol. 6, no. 1, pp. 71–73, 2008. doi: 10.1109/MSP.2008.3.
4. G. McGraw, *Software Security: Building Security In*. Reading, MA: Addison-Wesley, 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. doi: 10.1109/MSP.2013.139.
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. doi: 10.1109/MSP.2013.109.
7. CSEC2017 Joint Task Force, "Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity," ACM, New York, 2017. [Online]. Available: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf
8. W. Newhouse, S. Keith, B. Scribner, and G. Witte, "NIST special publication 800-181: National initiative for cybersecurity education (NICE) cybersecurity workforce framework," NIST, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
9. I. Fovino et al., "A proposal for a European cybersecurity taxonomy," European Commission, Brussels, Belgium, 2019. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf
10. A. Rashid, H. Chivers, G. Danezis, E. Lupu, and A. Martin, "The cyber security body of knowledge," Version 1.0, CyBOK, 2019. [Online]. Available: https://www.cybok.org/
11. N. Mead et al., "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," 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. "Cybersecurity higher education database." ENISA. https://www.enisa.europa.eu/topics/cybersecurity-education/education-map
15. "Cyber security MSc education survey." EUSurvey. https://ec.europa.eu/eusurvey/runner/CS4E_MSc_Survey_2019

Nicola Dragoni is a professor at the Technical University of Denmark, Kongens Lyngby, 2800, Denmark, where he also serves as deputy head of the Ph.D. school and head of the Digital Security Center. He is also a part-time professor at Örebro University, Örebro, SE-701 82, Sweden. His research focuses on security for fog and Internet of Things devices. Dragoni received a Ph.D. from the University of Bologna. He is active in a number of national and international projects. Contact him at ndra@dtu.dk.

Alberto Lluch Lafuente is an associate professor at the Technical University of Denmark, Kongens Lyngby, 2800, Denmark, and the head of 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. His research focuses on formal methods for cybersecurity and distributed systems. Lafuente received a Ph.D. from the University of Freiburg. Contact him at albl@dtu.dk.

Fabio Massacci is a professor at the University of Trento, Trento, 38123, Italy, and Vrije Universiteit Amsterdam, Amsterdam, 1081 HV, The Netherlands. His research focuses on security economics, experimental methods for security, and cybersecurity education. Massacci received a Ph.D. from the University of Rome "La Sapienza." He received the Ten Years Most Influential Paper award by the IEEE Requirements Engineering Conference in 2015. He is the leader of the education work package 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 is an assistant professor at Aalborg University Copenhagen, Copenhagen, 2450, Denmark. His research focuses on formal methods. Schlichtkrull received a Ph.D. from the Technical University of Denmark. 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.



Digital Object Identifier 10.1109/MSEC.2020.3047282