A Maturity Assessment Model for Cyber Security Education in Europe

Silvia Vidor and Carlos E. Budde

University of Trento, Trento, Italy

Abstract. Maturity assessment models have repeatedly been applied to education and to cyber security with the aim of improving the performance and management of private and public institutions. However, no attempts have been made so far to create a framework for the evaluation of cyber security education, which is an increasingly pressing matter due to the demand for cyber security professionals in the European Union. This paper contributes with a proposal for a maturity assessment model of cyber security education, including a discussion of one of the main issues in the field: the definition of knowledge units for the standardization of cyber security education in Europe.

Keywords: Cyber Security · Security Education · Maturity Assessment · Maturity Models.

1 Introduction

The growing threat of cyber attacks for both public and private organizations has stimulated, in recent years, the slow but steady growth of educational and training programs aimed at providing graduates and workers with the necessary instruments to implement cyber security measures, as well as creating dedicated professional figures [1]. Beyond national security, this is of particular relevance for the industrial sector, where e.g. SMEs can seldom afford exclusive resources for security-specialised personnel, and moreover whose level of information security is generally low [2,3].

Nevertheless, in the European context, overarching educational efforts in the area of cyber security training remain sparse. On top of this, the lack of standardized educational frameworks and curricula makes it difficult to investigate the factors that contribute to the development and diffusion of quality cyber security education. While methods for evaluation in the wider fields of education and cyber security have been previously defined, to the best of our knowledge that has not happened for *cyber security education* [4,5,6].

Due to its relatively recent emergence and lack of standardized curricula, we argue that cyber security education presents specific characteristics and unattended issues that cannot be fully addressed through more general analyses. For example, it has been argued that cyber security should be seen as a meta-discipline and thus includes a variety of disciplinary variants, leading to the

necessity for any cyber security education-related framework to include a series of degrees potentially very different in structure [7]. Cyber security education would then need a dedicated analysis, starting from a framework for the definition of key domains impacting the overall quality of cyber security education in Europe and the evaluation of the different levels of capability of educational organizations [1,8].

Objective. The aim of this paper is, then, to propose a maturity assessment model for the use of organizations involved in the field of cyber security education, particularly universities and institutions involved in cyber security training.

Content and outline of this work. In Section 2 we provide a brief review of existent maturity assessment models, describing their definition, history, main elements and two examples of models used in the education and cyber security fields. Then, in Section 3 we describe our proposal for domains, parameters and levels constituting a maturity assessment model for cyber security education in Europe. Our decisions are oriented to the expected (main) end beneficiary of such education, namely industry in general and SMEs in particular. In Section 4, starting from the surveys on formal cyber security education in Europe [1] and professional needs in cyber security [8], we discuss one of the main issues in the evaluation of cyber security educational programs: the identification of standardized knowledge units. We conclude the paper with some considerations over the next steps to be taken, specifically concerning the evaluation of the model we have developed.

2 Review of Existing Maturity Assessment Models

This section summarizes the main elements in relation to maturity assessment models, specifically concerning their definition, their history and development from the field of software development to business, education and cyber security, and their essential components. Two examples of maturity assessment models used in education and cyber security are briefly described in Sections 2.4 and 2.5 to provide a specific insight into the structure of popular frameworks in the areas of relevance to our work.

2.1 Maturity Assessment Models: a Definition

Maturity assessment models (also known as maturity assessment frameworks or maturity evaluations) can be described as *collections of elements, or attributes, representing capability and progression in a particular discipline or sector*. The content of a model typically includes best practices and standards of practice of the field [9]. As a consequence, *maturity models provide a benchmark against which an organization can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement.*

2.2 History and Development of Maturity Assessment Models

The origins of maturity evaluations can be traced back to the Capability Maturity Model (CMM), which was originally developed with the aim of evaluating software contractors' capabilities when working with the US Department of Defense. The CMM was formalized by Watts Humphrey of the Software Engineering Institute in 1988 [10], and later defined in detail with five maturity levels, each characterized by specific process areas and practices, by Mark C. Paulk, Charles V. Weber, Bill Curtis, and Mary Beth Chrissis [11]. Though its original use case was that of evaluating government contractors specifically operating in the software development field, the CMM – and its derivation, the Capability Maturity Model Integration (CMMI) – have been regarded more generally as methods to evaluate the maturity of processes and have thus gained traction in other sectors, such as business. Today, the CMM and its derivations constitute the basis upon which the great majority of maturity models are built.

The progressively increasing popularity of CMM has resulted in a widespread diffusion of maturity models to areas not necessarily related to IT or business but considered as being in need of improved management, such as education. The education and training community began issuing its own versions of maturity models (particularly related to the introduction of digital technologies in education) in the early 2000s [12]. The aim was to identify and measure performance in a series of key indicators in the education and training fields – e.g. "learning effectiveness", "change readiness" or "time to competency" – to evaluate the ability of the concerned educational institution to reach its goals, and eventually improve.

More recently, maturity has also become central in the evaluation of the cyber security capabilities of organizations, with the consequent development of models specifically targeted to this field by both private and public institutions. In particular, maturity assessment models in the field of cyber security have been mainly employed as a means to manage, measure and monitor the efficacy of both cyber security implementation methods and their governance [13]. As of today, some of the most widely used cyber security maturity models are incorporated into international cyber security standards such as ISO/IEC 27001 and NIST, which define requirements for the maintenance and improvement of information security in organizations [4].

2.3 Characteristics of Maturity Assessment Models

The essential components of a maturity model include [4]:

- Levels (see Fig. 1) – constitute the measurement element of the model, and are generally organized in a scale from 1 (least mature) to 5 (most mature);
- Attributes – constitute the content of the model, at the intersection of domains and maturity levels;

– Appraisal and scoring methods – constitute the standards for the measurement of the levels;
– Model domains – constitute the areas of importance for the analysed topic and can be specified in attributes.

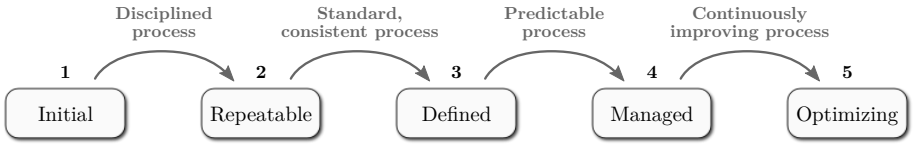

Fig. 1. The five levels of CMM [11]. The denominations of the levels (and sometimes its amount) vary between different authors and sectors of application.

According to [14], maturity models can also be divided into three different types: progression, capability and hybrid models.
Progression models focus on the model attributes and represent the scaling of one or more attributes, where the progression from one maturity level to the other indicates some progression of attribute maturity. Their purpose is to provide a roadmap of improvement as expressed by increasingly better versions of an attribute as the scale progresses; for this reason, they are the preferred kind of model for companies such as consultancies. An example of progression model is represented by the Smart Grid Maturity Model (SGMM), which is used to plan the development of smart grid facilities for electric power utilities [15].
Capability models, which are represented by the CMM and its derivations, focus instead on the broader organizational capability of the analysed institution, in an effort to evaluate the maturity of the "culture" instead of that of the single attribute. As a consequence, the levels of capability models represent states of organizational maturity specifically focused on so-called "process maturity" – leading to capability models being also known as process models.
Finally, hybrid models combine elements of both the progression and capability models. The transitions between one level and the other describe capability maturity, as in capability models, but the structure of the model reflects that of a progression model, for example by starting from an existing sectoral code of practice.

2.4 The e-Learning Maturity Model

As mentioned in Section 2.2, maturity assessment models in the field of education tend to focus on the introduction of digital technologies in the teaching and learning experiences, as well as on the ways to best integrate them for maximum results in terms of learning. Consequently, one particularly popular subject of maturity assessment has been e-Learning, with several higher education institutions developing and applying their own version of the model.

Among the most used models for the evaluation of e-Learning capability and maturity in educational institutions is the e-Learning Maturity Model (eMM), developed by Stephen Marshall of the Victoria University of Wellington in 2006 (an earlier version dates back to 2004). The eMM, in the words of its creator, is "aimed at [...] changing organisational conditions so that e-learning is delivered in a sustainable and high quality fashion to as many students as possible" [16]. Based on the CMM and on the Software Process Improvement and Capability dEtermination (SPICE) model, the eMM builds upon the idea that the ability of an institution to be effective in sustaining and delivering e-Learning depends on its capability to operate optimally in five "process categories" (known as domains in the CMM) as defined in Table 1. Each of these categories is defined by a series of "dimensions of capability" (ranging in number from 3 for the Evaluation category to 10 for the Learning category), which are evaluated on a maturity scale from 1 to 5. Each dimension can be further broken down into essential or useful practices that are necessary to achieve the objective of the process from the perspective of the considered dimension.

Table 1. The five process categories of the eMM as described in [16].

Category	Description
Learning	Processes that directly impact on pedagogical aspects of e-learning.
Development	Processes surrounding the creation and maintenance of e-learning resources.
Support	Processes surrounding the oversight and management of e-learning.
Evaluation	Processes surrounding the evaluation and quality control of e-learning through its entire lifecycle.
Organisation	Processes associated with institutional planning and management.

An example of application of the eMM to the context of e-Learning in Finnish universities has been described in [17].

2.5 The Cybersecurity Capability Maturity Model

In 2012, the U.S. energy sector and the Department of Energy (DoE) developed a dedicated maturity model, known as Cybersecurity Capability Maturity Model (C2M2), which is aimed at public or private organizations wishing to improve their cyber resiliency through the implementation and management of cyber security practices. The most recent version of the model, dated July 2021, includes input from internationally recognized cyber security bodies, such as the National Institute of Standards and Technology (NIST) [9]. Similarly to the eMM, the C2M2 includes 342 practices divided into 10 domains:

- Asset, Change, and Configuration Management;
- Threat and Vulnerability Management;
- Risk Management;

– Identity and Access Management;
– Situational Awareness;
– Event and Incident Response, Continuity of Operations;
– Third-Party Risk Management;
– Workforce Management;
– Cybersecurity Architecture;
– Cybersecurity Program Management.

Practices are the actions that the concerned organization can take to improve its capability into the considered domain. Each practice is also organized into a series of objectives, representing achievements supporting the domain at hand. In applying the model, each domain is evaluated according to three maturity levels (1 to 3), differently from the original CMM. A simplified representation of the C2M2's structure is shown in Fig. 2.

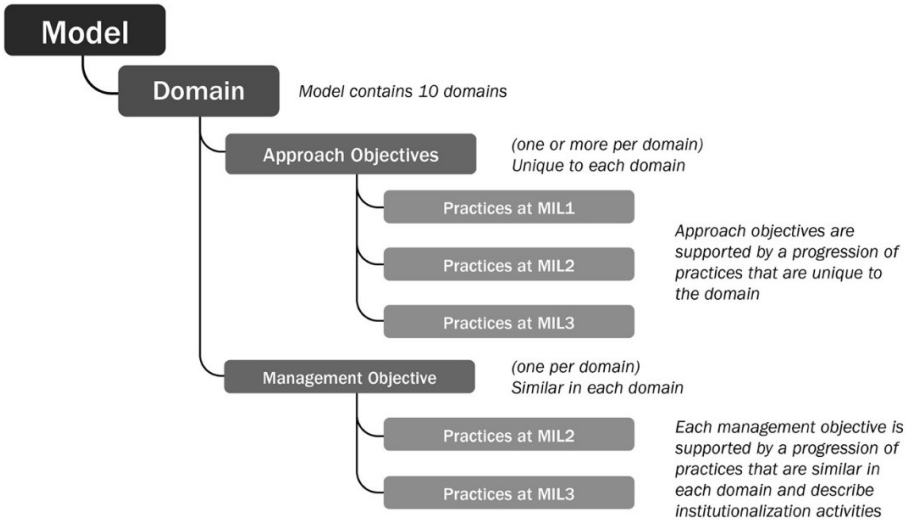

Fig. 2. Practices and objectives in each domain according to the C2M2. Notice that objective can be of "approach" or "management" nature [9].

The C2M2 is highly complex, partly due to the extensive amount of aspects included in the evaluation of cyber security maturity within an organization and partly due to the inclusion of additional standards, frameworks and requirements compared to the previous versions.

3 Maturity Evaluation of Cyber Security Education

In order to develop a maturity assessment model for cyber security education in Europe, we took inspiration from the 6P assessment implemented by Manufac-

turing Industry Digital Innovation Hubs (MIDIH), a EU H2020 program aimed at implementing technological, business and skills building services to European stakeholders in the field of digital innovation [18].

Interest in cyber security education in Europe has been increasing steadily in the past years, particularly among industry actors, who are in need of high-quality education on the subject for their current and future employees. Maturity assessment models can provide a tool for industry in general, and SMEs in particular, to understand where to turn to for high-quality cyber security-educated hires [2]. We thus chose the MIDIH over other relevant models in the fields of security or education due to its closer alignment with the needs of industry, which is not present in models such as the eMM.

The original 6P model, which is a derivation of the CMM, includes six domains (Product, Process, Platform/Technology, People, Partnership and Performance) and five levels of maturity; we propose an adaptation to the field of cyber security education as described in the following sections.

3.1 Proposed Domains and Parameters

In line with the original 6P model, we have chosen to define six domains for the assessment of maturity of organizations involved in cyber security education. However, differently from 6P, we have made the decision to change two of them to fit specifically the cyber security education field as opposed to a wider focus on innovation. In particular, the "Product" domain has been changed into the "Students" domain to better reflect the reference to the subjects of education, while the "People" domain has been changed into the "Educators" domain, given its exclusive attention to teachers and trainers compared to the wider perspective of the original domain as defined in the 6P model.
For each domain, our model provides a description of the parameters that are subject to the evaluation of maturity, as follows:

1. **Students** – concerns the students' interest in cyber security-related subjects, their background and experience in the field, and their enrollment in different types of educational offerings (e.g. seminars, full degrees) on the topic. For instance, the percentage of students that choose a clear-cut cyber security-related career or subject, such as cryptography, falls within this domain. Another example are surveys that reveal the intention of pre-university students to follow studies in the field of cyber security.
2. **Process** – concerns the coverage of different knowledge units, depending on which ones are considered as a priority by the concerned country, or by supranational authorities. For example, measures related to the adherence of degree courses (or syllabi) to curricula requirements for cyber security education fall within this domain.
3. **Platform** – concerns the use and integration of platforms for cyber security education, such as cyber arenas, into the teaching program. The modality and frequency of the platforms' use would also be relevant to achieve full maturity in this domain.

4. **Educators** – concerns the level of experience and expertise on the topic of cyber security (and its subtopics) on the side of professors, teachers and trainers. For instance, cyber security-related qualifications and certifications obtained by educators are relevant to this domain.
5. **Partnership** – concerns the presence of partnerships between stakeholders (e.g. academia, industry, public institutions) on the topic of cyber security education and their contributions to the improvement of education quality. An example would be that of a partnership between an university offering cyber security degree courses and a company offering internships to selected students.
6. **Output** – concerns the overall impact on society of the process of cyber security education, in the form of outgoing student quality. For example, the percentage of former students employed in the cyber security or closely related sectors is included in this domain, as well as the percentage of former students that choose to start an academic career in cyber security.

The specifications of the six domains throughout the five levels of maturity are listed in Table 2.

Table 2. Proposed maturity assessment model for cyber security education. The model can be read horizontally as a progression between different levels of maturity w.r.t. a specific domain, or vertically as a transversal maturity scenario w.r.t. a specific level.

Domains	Initial	Consolidating	Defined	Managed	Optimizing
Students	Self-initiative; students enroll in generic courses for the wide public	Seminar; students attend mini-courses on basic topics	Course(s); students attend full courses on fundamentals	Degree; students pursue an educational path dedicated to cyber security	Career; students follow a comprehensive and coherent educational path (with practical experiences) in cyber security
Process	Cyber security as extra topic	Few fundamentals covered	Fundamentals mostly covered	Fundamentals and few optional topics covered	Fundamental and optional KUs required by national (or other) institutions are fully covered
Platform	No use of tools or platforms	Few tools available for educators	One platform for students to train basic skills	Some platforms for basic skills and technology-oriented needs	Integrated use of various platforms for theoretical and practical competences
Partnership	No partnerships	Single, limited-topic with already known contacts	Multi-topic between selected stakeholders	Adaptive, ad hoc with actors from different environments	Wide network with balanced representation of different-background stakeholders
Educators	Inexperienced; superficial knowledge	Competent; some years of training or experience	Formally educated; specific knowledge	Limited practical experience; multiple-area knowledge	Experienced and formally educated; implementation of theoretical and practical teaching
Output	No quality measurement available	Knowledge of general concepts (e.g. phishing)	Selective, topic-specific competences	Internship-level knowledge	Career-ready, wide-ranging theoretical and practical competences

3.2 Proposed Levels of Maturity

In line with the approach of the CMM, which the 6P model derives from, we have chosen to maintain the original five levels of maturity in our cyber security

education maturity assessment model, so as to define in a detailed manner the evolution from one level to the other. We have, however, changed the name of the second level coherently with the characteristics of the level, which do not fit the original "Repeatable" label. Even though it is probable that organizations involved in cyber security education may fare differently in the six domains, registering different levels of maturity in different areas, the model that we propose can also be read vertically, depicting five scenarios of maturity that give a full picture of the state of cyber security education in an organization:

1. The **Initial** scenario describes the starting point of cyber security education, where the topic is still unaddressed or only of minor interest, students lack knowledge in the field, and the availability of experienced teaching personnel is low.
2. The **Consolidating** scenario describes a situation of growth of interest and knowledge on the topic of cyber security on the side of students and institutions, with short-term courses on basic issues (e.g. fundamentals for cyber hygiene for office jobs) being taught by educators with sufficient foundations on the matter at hand. Partnerships and platforms still play a minor role, but might be present.
3. The **Defined** scenario describes a case in which cyber security fundamentals are covered in full-length courses (with the use of at least one training platform, for example through Massive Online Open Courses [20]) taught by personnel with a formal education in cyber security. Partnerships on multiple topics are possible, but still restricted to stakeholders from the same environment (e.g. academia-academia).
4. The **Managed** scenario describes an advanced (but not yet optimal) level of maturity of cyber security education, where students (who may have previous experience or knowledge in the field) can follow dedicated degree courses and may benefit from the existence of *ad hoc* partnerships between the educational institution and other stakeholders for the improvement and practical application of their education, e.g. through internships.
5. The **Optimizing** scenario describes the final level of maturity for cyber security education, with the possibility to pursue full educational paths on the topic (extensively covering both fundamental and optional knowledge units) taught by experienced personnel and allowing the development of theoretical and practical competences (with the help of platforms such as cyber ranges), to be later spent in the job market.

Scenarios may also represent different cycles or generations of progress of cyber security education. The passage from one level to the other, then, would be enabled by the completion of the elements in the previous one. For example, the improvement in terms of educators' preparedness and competence on the topic of cyber security is made possible by the quality of their education in the previous scenario, when they held the position of students.

The model we propose for the evaluation of the maturity of cyber security education may be used, where needed, in combination with other maturity as-

sessment models for a more well-rounded assessment of the quality level of an educational or training institution. This is particularly relevant in the case of other models evaluating specific aspects of education, such as the e-Learning Maturity Model mentioned in Section 2.4. While the eMM analyzes a different aspect of education, that is, the impact of e-Learning on the wider learning experience of students and on the institutions offering such service, given the recent popularity of online learning (also in the field of cyber security education), the parallel assessment of these two aspects can help in determining the overall quality of cyber security teaching or training in the examined organization.

Still, there are some elements that remain of difficult definition within our proposed model: among them is the identification (and prioritization) of the cyber skills that are necessary for a complete cyber security education, that is, the identification of which knowledge units educational institutions should be required to cover to stimulate the development of those skills—both in terms of fundamental and optional topics. This issue, which relates to the Process domain of our model, is discussed in the following section.

3.3 Validation and Evaluation

Albeit based on MIDIH and other consolidated works, our model remains at theoretical level. Subsequent refinements and modifications must be preceded by a validation phase, where the model is evaluated by educational practitioners and also intended end users, e.g. SMEs which require cyber security personnel.

In this respect, a questionnaire is being designed that describes the maturity assessment framework of Table 2. Survey participants are asked whether the selected domains are relevant as indicators for the maturity degree of the cyber security education of their respective institutions. The survey includes open answers, where respondents can propose additional domains, thus signaling areas possibly not being covered by the six domains of our model. When deemed necessary, interviews will be carried out with selected respondents.

The survey will be primarily disseminated among educational and training organizations involved in cyber security education in Europe. This includes universities, other cyber-security relevant centres of public studies, and also possibly private education institutions. Industrial sectors not necessarily involved in education per se, but whose IT assets demands personnel expected to have undergone education at the Managed or Optimizing maturity level—e.g. telecommunications and consultants—will also be targeted as survey respondents.

4 Knowledge Units

Given the extraordinary growth in cyber threats to private and public organizations alike in Europe, as well as the increasing emphasis on security- and privacy-by-design, it is by now beyond doubt that there is the need for capable specialists in all areas of cyber security [19,1]. These specialists need to possess a

variety of skills and competences that are generally acquired through education and, in part, through practical experience. At the moment, however, institutions teaching cyber security around the European Union are not adopting a common approach to cyber security education, covering a variety of topics and on occasions not distinguishing adequately between fundamental and optional subjects. The lack of a clear definition of the cyber security curricula across the continent, thus, makes it difficult to evaluate the level of maturity of cyber security education, and represents a critical issue for addressing Europe's need for a unified approach to the subject.

4.1 A CyberSecurity Education Framework

To try and address this issue, we build upon the framework developed in [1] to perform a review of existing European MSc programs in cyber security. This framework has been extended to professional education in [8]. Our aim is to create a comprehensive, credible structure containing easily recognizable and common terminology in order to provide a point of reference for the organization of cyber security curricula. The framework is based upon a comparison of a series of existing cyber security curricula and taxonomies, such as:

- the ACM Cybersecurity Curricula framework, developed by the Association for Computing Machinery in collaboration with the IEEE Computer Society, the Special Interest Group on Information Security and Privacy of the Association for Information Systems, and the Committee on Information Security Education of the International Federation for Information Processing;
- the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, developed by the US National Institute of Standards and Technology.

While more bodies of knowledge were originally considered, such as the Proposal for a European Cybersecurity Taxonomy developed by the EU Joint Research Centre and the Cybersecurity Body of Knowledge (CyBOK) developed by the UK National Cyber Security Programme and the University of Bristol, the ACM and NICE frameworks were preferred due to their reputation. The final version of the framework identifies nine knowledge areas, each including a series of more specific knowledge units. Knowledge units are sets of topics connected by a common theme, while knowledge areas are aggregates of related knowledge units. The framework is shown in detail in Fig. 3.

4.2 Known issues and pivotal decisions

While the definition of a common framework can help to determine which subjects need to be covered in cyber security education, there are some persistent problems that remain to be solved e.g. with extensions or modifications to the framework illustrated in Fig. 3.

The primary issue concerns the hierarchy of knowledge units: *there is currently no concretely specified distinction between "fundamental" or "core" units,*

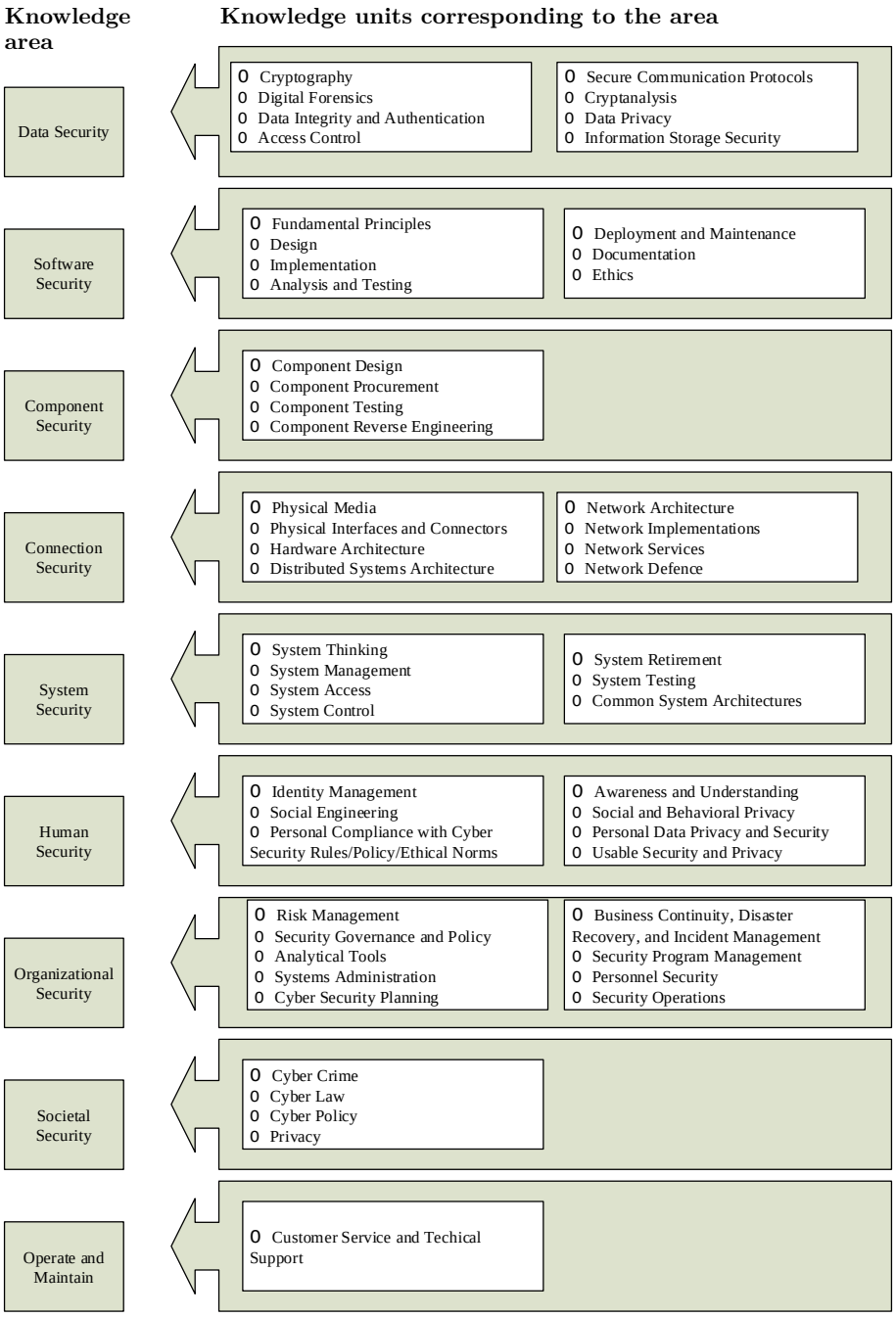

Fig. 3. The relevant knowledge areas identified in [1,8] for cyber security (left) and the relative knowledge units (right). The concepts were taken from the ACM and NICE frameworks, although further sources were considered.

and "optional" ones. This is shown for instance by the survey performed in [1], which included questions verifying the coverage of the cyber security-related knowledge units defined in the framework throughout higher education institutions in 25 EU countries. This survey put in evidence that current cyber security courses across Europe cover different topics in quantitatively different ways.

For example, even though all knowledge units identified by the framework were covered with mandatory courses, this only applies to the entire set of respondents. More specifically, not all countries covered all knowledge units: Spanish, French and German institutions covered more than 80% of the knowledge units with dedicated mandatory courses; in contrast, Slovakia, Romania and Ireland covered less than 10%. The focus of these three last countries was on Connection Security, Data Security and Organizational Security (Slovakia); Connection Security (Romania) and Data Security (Ireland), while other countries offered much more variety [1]. Such variations, not only from country to country but also across different higher education institutions in the same nation, can be interpreted by saying that at the moment, *the definition of one knowledge unit as fundamental over another is a quite complex task.*

The differences from country to country also raise another question, that is, *whether it is preferable for cyber security education across the European Union to adopt a homogeneous approach in terms of which knowledge units include in the cyber security curriculum, and in which measure, or whether it is better to allow each country to specialize in one or more specific sub-field(s)*—e.g. cryptography in Spain, access control in Belgium. The second option would entail, of course, that maturity assessments for the Process domain would need to be adapted to the curriculum developed by the country in which the analysed institution is situated.

5 Conclusion

In this paper, a proposal for a maturity assessment model was presented with the aim of defining a method for the evaluation of the maturity of institutions involved in cyber security education in the European Union. While some issues pertaining to the definition and standardization of knowledge units remain, our proposal tries to build upon the existing models in the areas of education and cyber security to lay the foundations of a common approach to cyber security education in Europe.

Future work. As a next step, the model will be tested across educational and training institutions in the cyber security field to verify its applicability and to try to provide *ad hoc* solutions for the issues we have identified and described in Section 4.2. Depending on the next steps taken at the European level concerning cyber security education, however, it remains possible that the model will need to be adapted to every country's specific necessities or desires for specialization, requiring a dedicated evolution of the Process domain to better account for these peculiarities.

Acknowledgments

This work has been performed in the framework of the European Union's Horizon 2020 Programme under grant 830929 (CyberSec4Europe).

References

1. Dragoni, N., Lafuente, A. L., Massacci, F., Schlichtkrull, A.: Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs. IEEE Security & Privacy **19**, 81–88 (2021). https://doi.org/10.1109/MSEC.2020.3037446
2. Manso, C.G., Rekleitis, E., Papazafeiropoulos, F., Maritsas, V.: Information security and privacy standards for SMEs. ENISA report (2016). https://www.enisa.europa.eu/publications/standardisation-for-smes
3. Ruiz, J.F. et al.: Security characteristics description, security and market analysis report. SMESEC deliverable D2.1 (2017). https://www.smesec.eu/deliverables.html
4. Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., Janicke, H.: A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. Applied Sciences **10**(10), 3660 (2020). https://doi.org/10.3390/app10103660
5. Marks, A., AL-Ali, M., Atassi, R., Abualkishik, A. Z., Rezgui, Y.: Digital transformation in higher education: a framework for maturity assessment. International Journal of Advanced Computer Science and Applications **11**(12), 504–513 (2020). https://doi.org/10.14569/IJACSA.2020.0111261
6. Ozkan, B. Y., van Lingen, S., Spruit, M.: The Cybersecurity Focus Area Maturity (CYSFAM) Model. Journal of Cybersecurity and Privacy **1**(1), 119–139 (2021). https://doi.org/10.3390/jcp1010007
7. Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., Pereira, T., Stavrou, E.: Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. ITiCSE 2018 Companion. Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education, pp. 36–54 (2018). https://doi.org/10.1145/3293881.3295778
8. Karinsalo, A. et al.: D6.3 - Design of Education and Professional Framework. Cyber Security for Europe (2021). https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf.
9. Muneer, F. et al.: Cybersecurity Capability Maturity Model, Version 2.0. U.S. Department of Energy, Office of Cybersecurity, Energy Security and Emergency Response, Washington, D.C. (2021). https://c2m2.doe.gov/C2M2%20Version%202.0%20July%202021.pdf.
10. Humphrey, W.: Characterizing the software process: a maturity framework. IEEE Software **5**(2), 73–79 (1988). https://doi.org/10.1109/52.2014
11. Paulk, M. C., Curtis, B., Chrissis, M.B., Weber, C. V.: Capability Maturity Model for Software, Version 1.1. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania (1996). https://resources.sei.cmu.edu/asset_files/TechnicalReport/1993_005_001_16211.pdf.
12. Wagenstein, H. N.: A capability maturity model for training & education. Chapter one: background and rationale. PMI Global Congress 2006. North America, Seattle, WA. Newtown Square, PA: Project Management Institute (2006).

13. De Bruin, R., von Solms, S. H.: Cybersecurity Governance: How can we measure it?. 2016 IST-Africa Week Conference, pp. 1–9 (2016). https://doi.org/10.1109/ISTAFRICA.2016.7530578
14. Caralli, R., Knight, M., Montgomery, A.: Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennysilviania (2012). https://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_58920.pdf.
15. Software Engineering Institute: Smart Grid Maturity Model, Version 1.2. Model Definition. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania (2018). https://doi.org/10.1184/R1/6583835.v1
16. Marshall, S.: eMM Version 2.3 Process Descriptions. Victoria University of Wellington, New Zealand (2007). http://e-learning.geek.nz/emm/documents/versiontwothree/20070620ProcessDescriptions.pdf.
17. Haukijärvi, I.: E-Learning Maturity Model – Process-Oriented Assessment and Improvement of e-Learning in a Finnish University of Applied Sciences. In: ITEM 2014. IFIP Advances in Information and Communication Technology, vol. 444, pp. 76–93. Springer, Berlin, Heidelberg (2014).
18. European Commission: Manufacturing Industry Digital Innovation Hubs FactSheet (2021). https://cordis.europa.eu/project/id/767498.
19. Crumpler, W., Lewis, J.A.: The Cybersecurity Workforce Gap. Center for Strategic & International Studies (2019). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf.
20. Fischer-Hübner, S., Beckerle, M., Lafuente, A. L., Ruiz-Martínez, A., Saharinen, K., Skarmeta, A., Sterlini, P.: Quality Criteria for Cyber Security MOOCs. In: WISE 2020. IFIP Advances in Information and Communication Technology, vol 579, pp. 46–60. Springer (2020). https://doi.org/10.1007/978-3-030-59291-2_4