energies

MDPI

Article

Enhancing Smart Grid Resilience: An Educational Approach to Smart Grid Cybersecurity Skill Gap Mitigation

Rūta Pirta-Dreimane [1], Andrejs Romanovs [1,*], Jana Bikovska [1], Jānis Pekša [1], Tero Vartiainen [2], Maria Valliou [3], Jirapa Kamsamrong [4] and Bahaa Eltahawy [2]

[1] Information Technology Institute, Riga Technical University, LV-1048 Rīga, Latvia; ruta.pirta-dreimane@rtu.lv (R.P.-D.); jana.bikovska@rtu.lv (J.B.); janis.peksa@rtu.lv (J.P.)
[2] Computing Sciences Department, School of Technology and Innovations, University of Vaasa, FI-65200 Vaasa, Finland; tero.vartiainen@uwasa.fi (T.V.); bahaa.eltahawy@uwasa.fi (B.E.)
[3] School of Electrical and Computer Engineering, National Technical University of Athens, 157 73 Zografou, Greece; mariavalliou@mail.ntua.gr
[4] OFFIS—Institute for Information Technology, 26121 Oldenburg, Germany; jirapa.kamsamrong@offis.de
* Correspondence: andrejs.romanovs@rtu.lv

Abstract: Cybersecurity competencies are critical in the smart grid ecosystem, considering its growing complexity and expanding utilization. The smart grid environment integrates different sensors, control systems, and communication networks, thus augmenting the potential attack vectors for cyber criminals. Therefore, interdisciplinary competencies are required from smart grid cybersecurity specialists. In the meantime, there is a lack of competence models that define the required skills, considering smart grid job profiles and the technological landscape. This paper aims to investigate the skill gaps and trends in smart grid cybersecurity and propose an educational approach to mitigate these gaps. The educational approach aims to provide guidance for competence-driven cybersecurity education programs for the design, execution, and evaluation of smart grids.

Keywords: smart grid cybersecurity; cybersecurity education; cybersecurity skill gaps; educational approach

Citation: Pirta-Dreimane, R.; Romanovs, A.; Bikovska, J.; Pekša, J.; Vartiainen, T.; Valliou, M.; Kamsamrong, J.; Eltahawy, B. Enhancing Smart Grid Resilience: An Educational Approach to Smart Grid Cybersecurity Skill Gap Mitigation. *Energies* **2024**, *17*, 1876. https://doi.org/10.3390/en17081876

Academic Editors: José Matas, Jorge El Mariachet and Sen Tan

Received: 16 March 2024
Revised: 9 April 2024
Accepted: 10 April 2024
Published: 15 April 2024

1. Introduction

Cybersecurity is characterized by the European Union (EU) [1] as a strategic digital capability; therefore ensuring the security of information technology (IT) and operational technology (OT) environments is paramount [2]. At the same time, cybersecurity skill gaps have been widely acknowledged across the industry and academia [3]. The ISC2 Cyber Workforce Study 2023 estimates a lack of more than 5.5 million cybersecurity specialists worldwide and this number is continuing to rise [4]. The existing education approaches, programs, and methods are insufficient to bridge the current skill gaps and ensure industry requirements. Educational advancements are required to engage more students in the field of cybersecurity.

The smart grid environment introduces additional complexity in terms of the protection of digital assets. Technological innovations, emerging technologies, and interconnected devices (such as IoT, 5G networks, and AI) facilitate the development of new products and services, but also introduce new cybersecurity threats [5]. In recent years, the energy sector has experienced a marked enhancement in its digital maturity, characterized by the integration of diverse digital computing, communication, and industrial control systems and technologies into an advanced power grid. The intention of those within the sector is to further enhance it by facilitating the cross-border real-time exchange of market data. With the vast amount of data and widespread use of IoT, the energy sector has become increasingly attractive to attackers. At the same time, power systems have high inertia due to their volume and complexity, and that inertia leads to technologies of varying ages often having

to co-exist. This means that legacy equipment that cannot be yet decommissioned will have to be safeguarded against modern cyberattacks. This indicates the considerable demand for cybersecurity expertise tailored to the energy sector. The European Commission stresses the crucial necessity of heightening awareness regarding data security among all stakeholders engaged in the design and operation of smart grids. The offering of qualitative education is a catalyst to counteracting cybersecurity threats on smart grids. At the same time, the existing cybersecurity education programs weakly address the complexity of the smart grid environment. Further, investigation into smart grid cybersecurity skill gaps is limited. The wider adoption of smart grid cybersecurity education would raise the overall awareness level of industry-required skills, along with the suggested knowledge areas, units, topics, and expected learning outcomes.

In addition to the complexity of smart grids, recent advancements in cybersecurity education emphasize the multidisciplinary nature of the subject [6]. Cybersecurity competence models, such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework (NIST NICE framework) [7] and the European Union Agency for Cybersecurity (ENISA) skill framework (ENISA framework) [8], traditionally focus on technical proficiency while related research places more emphasis on a solid mix of technical skills, soft skills, and social intelligence [9,10]. Therefore, new educational approaches are required to address smart grid cybersecurity, concerning a diverse set of competences.

This paper aims to investigate the skill gaps and trends in the field of smart grid cybersecurity and proposes an educational approach to mitigate such gaps. The educational approach aims to provide guidance for competence-driven cybersecurity education programs for smart grid design, execution, and evaluation. The key contributions of this paper are multi-fold. Firstly, we investigate the existing skill gaps in smart grid cybersecurity. Secondly, an educational approach is suggested to mitigate those skill gaps and ensure workforce requirements. Additionally, this study provides an overview of prospective educational methods and tools to be used in smart grid cybersecurity education. The research questions (RQ) of this study are defined as follows: RQ1. What are the current educational provisions in the field of cybersecurity, particularly focusing on the specialized domain of smart grid cybersecurity? RQ2. What are the gaps in cybersecurity education and what are improvement areas? RQ3. How to design smart grid cybersecurity education programs?

This study delivers two primary contributions. First, this paper fills the knowledge gap on the topic of education for smart grid cybersecurity, as it is one of the few available that covers this topic. Second, by writing this paper and conducting associated literature and qualitative analysis reviews, the main aim is to fill the found gap on frameworks and competences, we achieve the main gaol of enhancing the resilience of the smart grid. This paper proposes a new educational approach to building smart grid cybersecurity education programs, considering the best practices, industry standards, and stakeholder requirements. This study aims to offer new knowledge to educators in various sectors, as the proposed approach is applicable to different levels of study, including formal education and lifelong learning.

The rest of this paper is structured as follows. Section 2 introduces the main findings from related research. The research methodology is presented in Section 3. Section 4 presents the analysis of current education offerings, along with an overview of the industry requirements towards smart grid cybersecurity competencies. Section 5 includes the proposed educational approach, considering the education design model, proposed work roles and competencies, corresponding tools and methods, and approach implementation plan. Section 6 outlines the preliminary evaluation findings of the proposed approach. Finally, Section 7 concludes and provides an overview of future research directions.

2. Background

As it is stated in [11], the share of electricity in final energy consumption is projected to rise up to 53% by 2050, with more than 80% of electricity coming from renewable sources. In addition, the traditional consumer market will change and transform into an electricity

supply system increasingly based on distributed generation and energy storage [11]. The digitalization/modernization of the power grid is essential for integrating distributed energy resources (DERs) and ensuring effective monitoring and control. Energy and resource efficiency, decarbonisation, electrification in remote areas, sector integration, the emerging citizen energy community, and decentralisation of the energy system require a massive effort towards digitalisation. Investing in digital technologies such as smart IoT devices and metres, 5G and upcoming 6G connectivity, a pan-European energy data space powered by Cloud-edge computing servers, and digital twins of energy systems facilitates the clean energy transition while bringing benefits to our everyday life. For example, these technologies can assist in visualising real-time energy consumption and receiving personalised advice on how to decrease it with minimal impact on the quality of services that the end user receives. Digital tools can also help regulate room temperatures, charge electric vehicles, and manage appliances to take advantage of the lowest energy prices while maintaining a comfortable and healthy indoor environment. Public authorities can also use digital tools to better map, monitor, and address energy poverty, while the energy sector can optimize its operations and prioritize the use of renewables.

The integration of DERs into the power grid necessitates advanced digitalization and modernization efforts. By leveraging smart grids and innovative digital technologies, such as IoT devices and cloud and fog computing, the power grid can effectively monitor and control the flow of electricity from various renewable sources, ensuring stability and efficiency in the energy system. This integration enables the seamless incorporation of renewable energy sources, such as solar panels and wind turbines, into the grid, reducing reliance on fossil fuels and facilitating a sustainable and resilient energy future.

For example, in [12], the authors emphasize the importance of addressing cybersecurity challenges in IIoT-based environments and highlights the vulnerability of systems utilizing advanced wireless ICT to new cybersecurity problems.

As electricity will play an increasingly important role in the future, the integration of DERs into the electricity grid is becoming mandatory. However, the risk of cyber threats increases with this integration. The security and resilience of smart grids is crucial to ensure the stability and reliability of energy systems. Cybersecurity measures must be implemented and continuously updated to protect against potential cyberattacks that could disrupt critical services and threaten the integrity of the grid. Only by addressing these challenges can we fully exploit the potential of the digitisation and modernisation of our energy infrastructure, while ensuring a secure and sustainable energy future for generations to come.

2.1. Smart Grid Cybersecurity

Smart grids play a critical role in modernising and optimising the energy sector by integrating advanced technologies and communication systems into traditional electrical grids. The cybersecurity of European energy systems is threatened due to major trends in our energy systems:

1. Europe's objective of creating a fully integrated internal energy market implies real-time, high-volume markets. This requires cross-border coordination and increased data exchange, especially with the emergence of new actors such as prosumers. Managing the operation of these new actors presents a security challenge that requires ongoing security analyses;
2. The movement towards decentralized renewable energy production creates a larger surface area of attack points (e.g., a smart meter being installed in a home will probably not have the same level of security as a SCADA system in a power plant). In decentralised energy systems, distribution networks will play a key role in providing security measures;
3. Regarding the implementation of digital solutions in energy systems, a significant challenge arises from the increasing connectivity of essential components such as generators, distribution networks, and smart meters within households to the internet.

This interconnectedness exposes these distributed systems to potential cyber threats, leaving them vulnerable to attacks.

As energy systems adopt more of the proposed digital tools, attackers have new attack surfaces to exploit. Cyber criminals have become aware of this and there has been a massive increase in the number of successful cyberattacks, especially now that electricity networks such as smart grids interconnect a vast number of users and power systems' infrastructure. Therefore, a single disturbance may propagate into a large power outage of the network, resulting in widespread negative effects. We are thus entering an era marked by smart, decentralized, and interconnected energy systems, presenting substantial advantages and opportunities for the advancement of new energy services. Nonetheless, this transformation brings forth new cybersecurity challenges. The escalation of cybercrime is detrimentally affecting both energy systems and society at large. The energy industry faces a shortage of cybersecurity professionals to adequately address these emerging threats.

Cybersecurity threats to the energy system encompass operational disruptions, data breaches, and financial losses, posing significant risks to both infrastructure and consumer privacy. The risks of an attack on the energy system include the loss of access to electricity; the theft of personal data of customers (potentially including financial information, or other sensitive information that can be deduced from the load profile of a household); the destruction of on-site data used to operate the facility, leading to a prolonged out of service state for the facility (as in the 2015 attack on the Ukrainian power grid); and severe damage to the infrastructure, which can be very costly or time-consuming to replace. More importantly, when the various components of the system operate using false data or in a compromised state, the safety of the people who interact with the system cannot be guaranteed.

2.2. Smart Grid Cybersecurity Competence Models

Several frameworks define cybersecurity-related roles, associated tasks, and required competencies, for example, the National Initiative for Cybersecurity Education (NICE) Workforce Framework (NIST NICE framework) [7] and the European Union Agency for Cybersecurity (ENISA) skill framework (ENISA framework) [8].

The NIST NICE framework defines cybersecurity roles, describes task statements, and the knowledge, skill, and ability statements required to perform the necessary tasks. According to the NIST NICE framework, these statements are the foundation for cybersecurity education.

ENISA presented a new version of their cybersecurity skills framework (ECSF) in September 2022. The aim of the ECSF is to create a common understanding of the relevant roles, competencies, skills, and knowledge required; to facilitate the recognition of cybersecurity skills; and to support the design of cybersecurity-related training programs [8]. Additionally, in 2023, a new European policy initiative, the Cyber Skills Academy, was adopted to bring together existing initiatives on cyber skills and improve their coordination, in view of closing the cybersecurity talent gap and boosting the EU's competitiveness, growth, and resilience [13].

Several cybersecurity curriculum recommendations suggest main knowledge areas, knowledge units, learning topics, and learning outcomes. For example, Cybersecurity Curricular Guidance for Associate-Degree Programs (Cyber2yr2020), prepared by the Association for Computing Machinery Committee for Computing Education in Community Colleges [14] and the CSEC2017 Joint Task Force on Cybersecurity Education (JTF)'s global cybersecurity curricular recommendations [15].

The JTF's recommendations are based on a comprehensive view of the cybersecurity field, the base discipline's specific demands, and the relationship between the curriculum and cybersecurity workforce frameworks. The JTF emphasizes that cybersecurity is an interdisciplinary course of study, including law, policy, human factors, ethics, risk management, and computing. Their model consists of eight knowledge areas—data, software, component, connection, system, human, organization, and societal—and six

cross-cutting concepts—confidentiality, integrity, availability, risk, negative thinking, and systems thinking.

Cyber2yr2020 is based on CSEC2017 and inspired by CAE-CD 2Y knowledge units [16] and NIST NICE [7]. Competencies and learning outcomes are the focus of these guidelines. Competencies for Cyber2yr2020 include the ability to describe different human factors that can affect privacy and security, and the ability to compare different mental models and their impact on a user's response to cybersecurity risks. The model consists of eight knowledge areas—data security, software security, component security, connection security, system security, human security, organisational security, and social security.

2.3. Smart Grid Cybersecurity Education

Education plays a critical role in the cybersecurity of smart grids by providing the knowledge, skills, and understanding needed to effectively secure and protect smart grid systems against cyber threats. Education in smart grid cybersecurity should:

- Raise stakeholder awareness of the importance of cybersecurity in the context of modern energy systems;
- Build technical expertise for the design, implementation, and maintenance of secure smart grid systems;
- Promote the best practices for smart grid design, implementation, and operation, and familiarise stakeholders with industry standards, guidelines, and cybersecurity fundamentals;
- Build risk management skills by teaching professionals as well as students how to identify, assess, prioritise, and mitigate cyber risks to smart grid assets, infrastructure, and operations, ensuring that energy services are resilient to cyber threats;
- Build trust in collaboration and information sharing among stakeholders in the smart grid ecosystem;
- Facilitate the ongoing training and professional development of cybersecurity professionals and smart grid stakeholders.

The state of the art in education in smart grids and cybersecurity is analysed in [17]. In this paper, the authors conclude that the current education offering of specialized education programs does not address all needs, especially those of adults who want to re-skill or up-skill and new specialists. Cybersecurity is widely represented in different education forms; however, smart grid security topics are addressed relatively rarely.

In [18], it is pointed out that meeting the increasing demand for ICT experts and ICT security experts with operational knowledge in electricity has become challenging and requires updating engineering and ICT education curricula. Similar conclusions are made in [19], where workshop participants, including representatives from academia and the industry, discussed the skill gaps of the subject of cybersecurity and smart grids.

Thus, smart grid cybersecurity education plays an important role in enhancing the resilience of energy systems by raising awareness, building technical expertise, disseminating best practices, and ensuring that critical infrastructure and consumer data are protected from cyber threats.

2.4. Educational Tools and Methods

Choosing appropriate methods and tools for smart grid cybersecurity education is essential to ensuring that educational activities are effective, engaging, relevant, accessible, practical, evaluable, adaptable, and resource-efficient. By carefully considering the unique needs and objectives of smart grid cybersecurity education, educators can design and implement effective learning activities that will enable participants to address cybersecurity challenges and improve the resilience of energy systems.

Smart grid cybersecurity training would benefit from using active learning, an educational approach that engages students in activities that promote critical thinking and problem solving, rather than passive lecturing. The various methods and tools available for effective and engaging smart grid cybersecurity education include simulations, virtual labs,

capture-the-flag competitions, interactive workshops and seminars, gamification, scenario-based learning, and collaborative learning. By using these educational tools and methods strategically, educators can create effective learning experiences that enable participants to address cybersecurity challenges and improve the resilience of energy systems.

3. Materials and Methods

This study employs the design science problem-solving method [20] as an overarching framework for the selected issue's investigation and solution design, and the evaluation of the domain of this paper, i.e., smart grid cybersecurity education. It is a structured approach that links real-world challenges with solutions that are specific to particular domains through the conduct of multiple studies. The aim of this paper is to investigate the skill gaps in the smart grid cybersecurity field and propose recommendations regarding the educational approach to these gaps. The design science method consists of three repetitive cycles [21]. The relevance cycle uses the environmental context and provides research requirements to improve the knowledge base and solve the research problem. The design cycle comprises the development and evaluation of artifacts, while the rigor cycle substantiates the research with prior knowledge and verifies the innovative nature of the solution.

This study aims to identify the skill gaps in the smart grid cybersecurity field and provide recommendations to bridge those skill gaps, considering the requirements of stakeholders. Figure 1 illustrates the study's environment, design, and knowledge base. This study was performed in the research project "Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)", realized between 2017 and 2020.

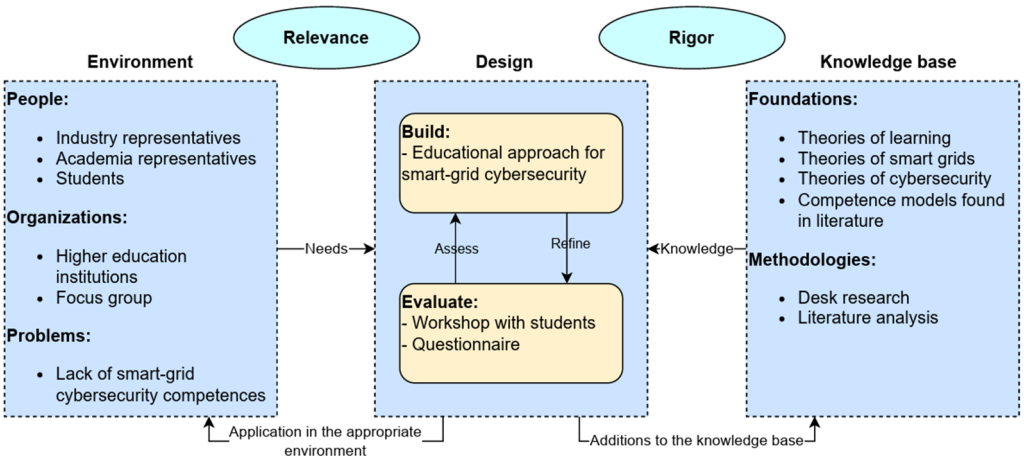

Figure 1. Research Methodology (adapted from [20]).

A literature review was conducted to discern the state of the art in cybersecurity within smart grids, gather insights into research trends and recent advancements, and identify the most effective educational methods and available curricula. The literature review utilized Google Scholar as a source pool, influenced by an article which suggests that its comprehensive search results extensively include popular and reliable sources. The keyword search terms utilized were "cybersecurity education", "smart grids cybersecurity education", and "smart grids security". Approximately three hundred results were obtained using the specified keywords, encompassing research articles, conference papers, and theses. Consequently, the literature published between the years 2017 and 2020 was selected for an in-depth review of the latest developments in smart grids. Desk research was then conducted to gather information pertinent to specific topics and domains, tailored to the research context and objectives.

In order to gain a comprehensive understanding of the current landscape within both the industry and academia, the project research team organized a stakeholder workshop. The purpose of the workshop was to inform stakeholders from the education and industry

fields about the findings of the performed literature review and facilitate discussions regarding the essential tools and skills required for cybersecurity specialists in the energy domain. The workshop spanned 2.5 h and involved 23 participants selected from associations, universities, and the industry. The snowball sampling technique was employed to identify and invite key stakeholders to participate in the workshop [22]. The stakeholder workshop commenced with an introduction outlining the project's objectives and presenting the findings of the literature review. Participants were then divided into four smaller groups, each facilitated by a moderator, to engage in open discussions on predetermined questions. These discussions primarily focused on the skills students acquire in academia for industrial roles and the expectations of the industry from young professionals. A virtual concept board was utilized to capture comments and ideas for subsequent discussions. Following the group discussions, each group reported their findings, leading to a broader discussion involving all participants to address any open questions and encourage cross-group dialogue.

The results of the literature analysis, combined with the stakeholders' feedback and added material, were used to create an initial educational approach. The approach is model-based, describing main components of smart grid cybersecurity education design (Section 4.1.) and a proposed implementation plan (Section 4.1.)

The approach was co-created by a project team from four different educational institutions across the Europe. The approach was evaluated using two main methods—expert evaluation and approach piloting with students. Initially, the proposed approach was presented to the stakeholders in two half-day seminars. Both seminars attracted 20–25 participants each, with one conducted in a hybrid format and the other delivered as a webinar. The participants included representatives from the industry, students, and educators. Each session commenced with presentations outlining the project's scope and main results, followed by a feedback and questions session. Stakeholder feedback was actively collected during the sessions, enabling iterative refinement of the proposed approach based on their input. The educational approach's reusability, adaptability, and scalability aspects were examined with representatives from six diverse educational institutions across Europe during workshops. No significant issues were identified, as there were notable similarities observed with the provision of education at the European level. After the approach's initial evaluation with the experts, a separate student session was organized. The educational approach and accordingly prepared study materials were presented to students (8 students) interested in smart grid cybersecurity. The student workshop lasted approximately 6 h, during which quantitative data were gathered. Although the student group was small, the assessment should be viewed primarily as qualitative feedback. Furthermore, there is a plan to incorporate additional model piloting and evaluation loops in the future.

4. Education Offering and Skill Gaps

Eighty-four universities with IT study programs linked to security were considered. It should be noted that, although undergraduate study programs may provide terms such as cybersecurity, ethical hacking, security management, data security, and information assurance track, they all closely adhere to the same basic idea. This idea is comparable to the courses needed to complete a study program in cybersecurity, beginning with a foundational understanding of computer architecture and information technology, moving on to a more in-depth grasp of data, networks, forensics, information systems, operating systems, and algorithms, and concluding with computer security study courses.

4.1. Education Offering

Regarding the education offered, it is noted that professional bachelor study programs offer study courses with real-world examples, supporting the study course with practical security testing tools and techniques for evaluating networks, systems, and peripheral devices that have an impact on the current infrastructure. Thus, diverse competencies, skills, and knowledge are acquired by transitioning between theory and practice. Of the 84 universities, 14 did not meet requirements. Study programs in information technology, computer science,

or computer systems do not go deeply enough into the contemporary field of cybersecurity, despite the fact that they have specific requirements related to cybersecurity.

Continuing with graduated study programs, the majority of master's degree programs focus on cyber security to a considerable extent, indicating that graduates have the necessary expertise, competencies, skills, and capacities to apply particular Cybersecurity subtopics practically. Examples include Privacy Engineering, which highlights various jurisprudentially derived aspects of the proceedings, such as the Law of Computer Technology, Information Security and Privacy, Privacy Policy, Law, and Technology, Foundations of Privacy, Usable Privacy and Security, and Engineering Privacy in Software. Aspects of human-based security, including computer forensics, information security management, physical security, personnel security, and human aspects of cybersecurity, are covered in the following section. The following division, which consists of several specialized study courses, is pertinent to both SMEs and the country of study. Examples include Critical Infrastructure Protection in Theory, Policy, and Practice; Enterprise Security Practices; Organizations, Management, and Work: Theory and Practice; and others. "Practice" serves as a keyword that not only signifies practical abilities but also denotes the practical application inherent in several of the course titles mentioned. The final category consists of particular subtopics, the majority of which are already applied to PhD study programs. Cyber Defense, Digital Transformation, Information Security Risk Management, and Cryptography are among the topics covered.

Doctorate study programs focusing on cybersecurity are a previously established higher level of study. Out of the 70 universities that were surveyed, only one offers a doctoral program, with the name Cybersecurity and Software Technology Doctoral Programme. As the university states with pride [23]: "We at De Montfort University (DMU) are acknowledged as global leaders in software technology and cybersecurity research. We assist in the creation of the most important international standards in the area and advise governments on it. Provide the most esteemed courses in software engineering and cybersecurity, publish our fascinating research in internationally recognized journals, and plan innovative international conferences that immerse students in the field of study. The DMU Doctoral Training Program in Cyber Security and Software Technology is headed by a highly skilled group of scholars from several faculties, such as Psychology, Law, English, and Computer Science. This special curriculum will supply informed, adaptable, and experienced researchers to satisfy the needs of the public and private sectors. Who will be able to successfully handle the difficulties involved in establishing a lucrative, safe, and secure environment that includes cyberspace, key infrastructures, and smart systems".

It is important to note that, as was previously emphasized, the subject of smart grids is only included in one study program—the University of Turku Master's program. This indicates that smart grid study courses have not yet been extensively introduced in the higher education system. Table 1 lists the number of universities that were covered from this review in the EU and USA for the three levels of study i.e., bachelor's, master's, and Ph.D.

Table 1. Cyber security universities in the EU and USA by degree (status on 2020).

	Bachelor's	**Master's**	**Ph.D.**
EU	3	29	2
USA	14	37	1

In Table 1, it is highlighted that, between the EU and USA, bachelor's study programs are significantly more in terms of the raw number in the USA compared to the EU, which seems to not provide enough study programs of this level. However, master's study programs are similar in their numbers. The number of Ph.D. study programs in both regions is dramatically low.

4.2. Skill Gaps

The evaluation of knowledge area coverage with relevant research was conducted through a literature review [19]. The results highlighted that the less-investigated areas are organization, human, and societal security areas (following the ACM classification), compared to the areas of system, connection, and component security (Figure 2). Similar findings were obtained in a related research study [24]. The emerging integration of information and communication technology (ICT) into existing systems raises concerns regarding interoperability, particularly when new connection protocols are implemented on legacy components, or vice versa, potentially jeopardizing the entire system. This underscores a lack of consideration for human, organizational, social, and, partially, data security aspects. It is evident that much of the literature focuses primarily on the technical perspective while neglecting societal dimensions.

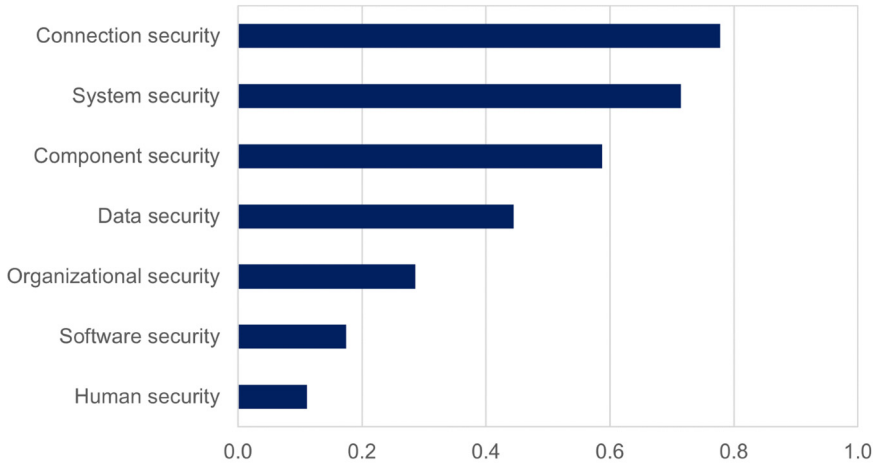

Figure 2. Categorization of skill gaps based on the literature review (adapted from [19]).

The non-technical aspects of smart grid cybersecurity include awareness, perception, and understanding of the way that the equipment works, a lack of knowledge on which can lead to misconceptions such as fear of electromagnetic radiation, over-expectation of its benefit, and privacy concerns. The presence of non-technical factors may give rise to objections against the widespread deployment of smart grid technology. Both technical and non-technical aspects should be taken into account at the initial stage of deployment to mitigate opposition to the adoption of new technologies. This can be achieved by disseminating information and facts about new technologies and by raising awareness of their security and vulnerabilities.

4.3. Stakeholders Requirements

Industry requirements and academia recommendations were collected during the workshop with 23 experts from four countries [19]. The stakeholder workshop commenced with an overview and detailing of the anticipated objectives of the project, alongside a presentation of the initial findings from the literature review. Afterwards interactive brainstorming and an ideas exchange were conducted, organized into four smaller groups and each facilitated by a moderator. The groups discussed topics concerning the skill sets that academia imparts to students for their entry into the industrial workforce, as well as the expectations of the industry from professionals. A virtual concept board served as a tool for participants to express ideas and comments for further discussion. Subsequently, each group presented their findings, and all participants engaged in discussions to address open topics across the groups. The requirements were summarized according to the START, CONTINUE, DO MORE, and LESS OF aspects (Table 2).

Table 2. Stakeholders' requirements overview (adapted from [19]).

Domain/ Aspects	Academia	Industry
START	• Facilitating the integration of knowledge between power system and communication infrastructure. • Proactively design, develop, and monitor cybersecurity measures and policies. • Increase budget allocation for research initiatives.	• A comprehensive understanding of various types of security threats.
CONTINUE	• Testbed usage in the study process. • Necessary tools for development and testing purposes. • Understanding of cybersecurity across multiple domains, such as critical infrastructure, communication systems, and power systems. • Integrate practical experience sharing into the study process.	• Independent learning or self-education. • Comprehension of multi-domain environments, encompassing power systems and communication networks. • Zero trust principles and methods implementation.
DO MORE	• Familiarity with power system components such as Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), and Phasor Measurement Units (PMUs). • Engagement in international cybersecurity research initiatives. • Understanding of network security principles. • Participation in professional training programs. • Attainment of certifications such as Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Certified Ethical Hacker (CEH).	• Independent learning or self-education. • Knowledge on the vulnerabilities of a power system and communication networks. • Workable Soft-Skills Learn new technologies. • Knowledge of most popular SCADA platforms. • Practical use cases. • Basic tools for threat analysis.
LESS OFF	Plain theory provision in the study process.	N/A

The workshop underscored the necessity for a foundational understanding of cybersecurity across various domains, including communication networks and critical infrastructure. Additionally, there was an emphasis on the importance of gaining practical experience and proficiency with diverse cybersecurity tools within academic settings. The participants of the workshop reached the conclusion that merely teaching and presenting theoretical concepts within cybersecurity curricula falls short for students aspiring to enter the industry in the future. Another outcome of the analysis revealed disparities between the commonly utilized tools discussed during the workshop and those documented in the literature. In the literature, testbeds were commonly used to examine systems, their components, and their connection. The workshop highlighted a widespread utilization of tools, platforms, and standards to support security professionals in their daily activities. These include security information and event management (SIEM), information security management systems (ISMS), and tools for networking, endpoint security, access management, encryption, incident response, and vulnerability management. Open-source software is also used to enhance security measures without costly license fees.

5. Proposed Educational Approach

The proposed educational approach in this study encompasses several interrelated components. The education design model provides an overview of the suggested smart grid cybersecurity educational approach and recommends applicable principles, a content-development model, and an education design methodology. The education curricula content building block proposes smart grid cybersecurity-related roles and their competences. The methods and tools bank identifies prospective tools and methods for smart grid cybersecurity education. The roadmap for implementing the educational approach outlines the key activities that educators need to undertake to ensure effective implementation of the approach.

5.1. Education Design Model

The education design model (Figure 3) provides recommendations for competence-driven smart grid cybersecurity education implementation in different forms, including formal and non-formal education at different levels.

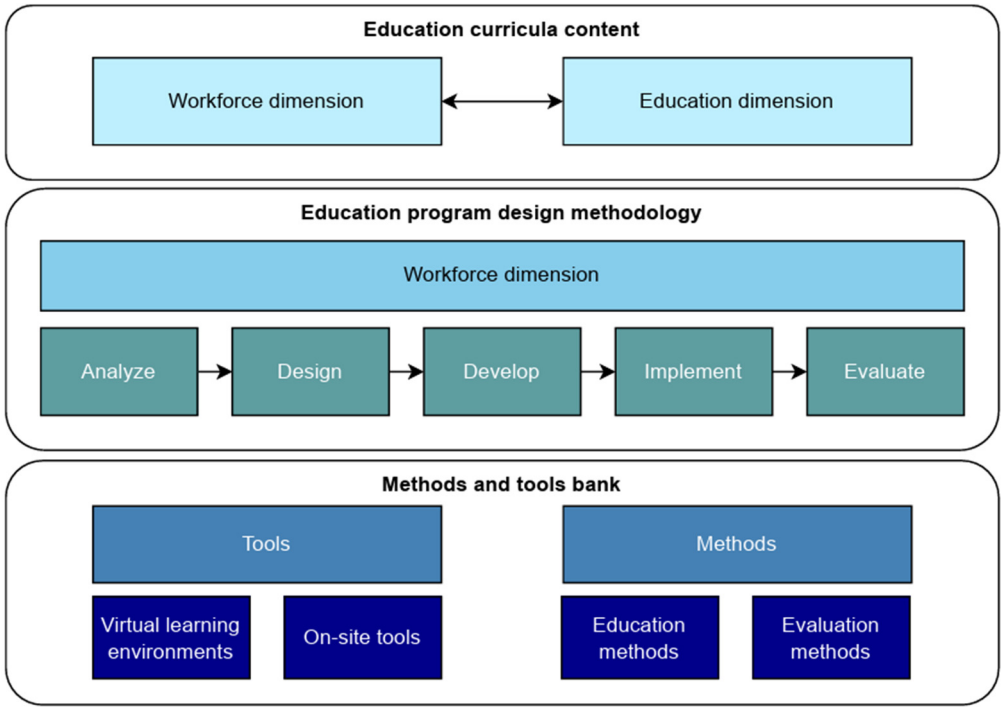

Figure 3. Education design model (adapted from [25]).

The model, which is adapted from [25], consists of several interconnected building blocks. The "Education curricula content" building block suggests the work-roles-based definition of competencies to ensure workforce needs are met. The "Education program design methodology" block recommends design processes for education programs, following defined guiding principles. The "Tools and methods bank" block incorporates the best practices regarding the tools and education methods to be used in smart grid cybersecurity education provision.

5.1.1. Curriculum Content Model

The curriculum content model proposes an approach for smart grid cybersecurity education curriculum design. The design of educational curricula should consider workforce requirements to ensure that the competencies of smart grid cybersecurity specialists align with industry demand, encompassing the necessary skills and areas of expertise to be addressed [26]. The proposed model connects two dimensions—the workforce dimension and the education dimension (Figure 4).

The workforce dimension includes several important concepts, following the NIST definitions [7]: "Work roles are the most detailed groupings of cybersecurity-related work, including a list of attributes, i.e., knowledge, skills, and abilities required to perform tasks associated with the role. Tasks represent specific defined pieces of work that, combined with other identified tasks, compose the work scope in a specialty area or work role. Competencies describe capabilities of applying or using knowledge, skills, abilities, behaviours, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position". It is important to distinguish the different capabilities required between subject-specific, e.g., "hard skills", and general/social, e.g., "soft skills". Hard skills encompass technical or administrative competencies, while soft skills refer to a cluster of personality traits that influence one's interactions within

a social environment. These skills encompass a wide range of abilities, including social graces, communication skills, language proficiency, personal habits, empathy (both cognitive and emotional), time management, teamwork, and leadership qualities. The ENISA competence model is selected in this study as the foundational framework for designing proposed approach to cybersecurity education in smart grids, as it has a more concentrated work-role structure compared to NIST. Existing cybersecurity competence models focus on cybersecurity governance and IT-specific cybersecurity aspects, but they do not address smart grid cybersecurity roles, tasks, and competencies. Therefore, it is proposed to incorporate the smart grid cybersecurity-specific roles and tasks into the ENISA model (Section 4.1).

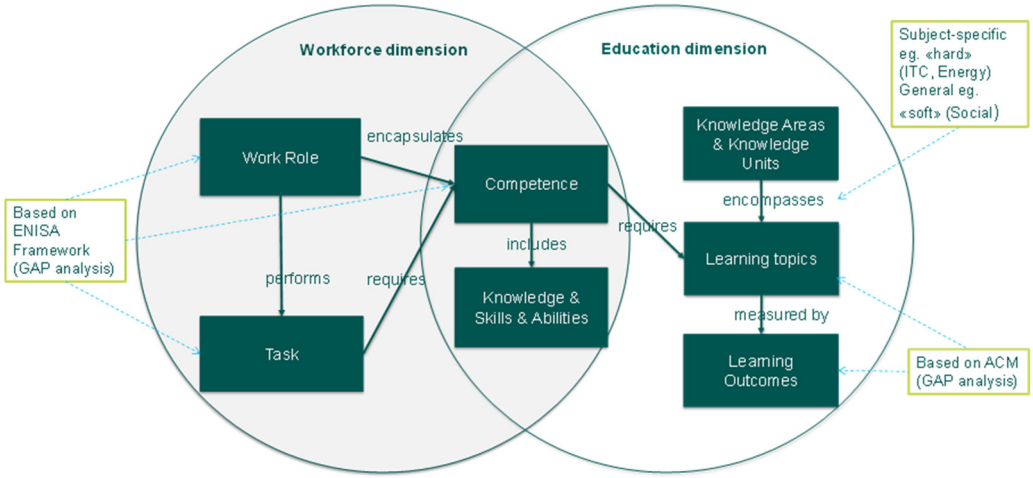

Figure 4. Curriculum content model.

The workforce dimension interacts with the education dimension via competencies that include skills, abilities, and knowledge. The education dimension includes several key concepts, considering the Cyber2yr2020 definitions [14]: "Knowledge areas and knowledge units are thematic grouping that encompass multiple, related learning topics. Learning outcomes represent more detailed outcomes than the competencies and may be seen as course or lesson learning outcomes. Learning outcomes emphasize what students can do over merely what students know". For cybersecurity education for smart grids, the Cyber2yr2020 model is selected in this study as the foundation of the definitions of IT-specific cybersecurity knowledge units, knowledge areas, topics, and learning outcomes. Consideration of smart grid-specific cybersecurity education is limited in existing frameworks; therefore, smart grid cybersecurity-specific competencies, learning topics, and learning outcomes are incorporated into the Cyber2yr2020 model (Section 4.1). Four groups of competencies are used (Table 3).

Table 3. Competencies classification schema.

Competence Group	Description
IT-specific competences	The knowledge, abilities, and skills necessary to execute IT-specific cybersecurity tasks. These competencies delineate the "what is to be done" aspects, considering IT responsibilities.
Smart grid specific competences	The knowledge, abilities, and skills necessary to execute smart grid-specific cybersecurity tasks. These competencies delineate the "what is to be done" aspects, considering IT responsibilities.
Operational competences	Managerial and operational competences that define "how activities should be done" in both—IT specific and smart grid-specific areas.
General competences	Expected "soft skills".

To summarize, the foundation of the smart grid cybersecurity content model is workforce requirements that are incorporated into competence maps. The workforce requirements are captured from existing cybersecurity work profiles, enriching them using smart grid-specific aspects. The requirements are mapped with knowledge areas, knowledge units, learning topics, and learning outcomes, defined in cybersecurity curricula guidelines, and supplemented by smart grid-specific concepts and identified skill gaps (Section 4).

5.1.2. Education Design Methodology

The education program design methodology outlines the fundamental principles to be adhered to and the primary steps for defining an educational program.

Education programs should be prepared following several guiding principles. According to the design thinking approach, regarding its usage in educational design, [16,17] design principles are frequently used to state the main direction that must be followed in programs' design and execution [18]. The design principles are defined as [17]: "... an intermediate step between scientific findings, which must be generalized and replicable, and local experiences or examples that come up in practice. Because of the need to interpret design-principles, they are not as readily falsifiable as scientific laws. The principles are generated inductively from prior examples of success and are subject to refinement over time as others try to adapt them to their own experiences". Design principles elicit design knowledge from successful learning environments [18] and summarize reusable best practices. For cybersecurity education in smart grids, it is suggested to follow the below key principles:

1. Target roles and task-driven competence design—competences must be defined based on learners' target roles to enable workforce and education dimensions' integration;
2. Learner centricity and personalization—study programs must focus on students' needs and provide profile-specific competence development;
3. Subject-specific and general competencies synergy—general competencies must be integrated in every learning topic along with subject-specific competencies;
4. Real-world experiences integration—study programs' and courses' content must reflect real-world challenges and must adapt over time;
5. Vertical integration—cybersecurity is a multi-disciplinary subject; programs must integrate social sciences (such as psychology) to enable general competencies' development;
6. Feedback based continuous improvement—continuous improvement must be planned based on learners' and workforce feedback.

The education design process outlines the main activities for smart grid cybersecurity education programs' design (Figure 5). Educators can employ the smart grid cybersecurity competence model and curricular content recommendations outlined in this document for program definition, execution, and evaluation. Nonetheless, it is essential to ensure that the specific content is tailored to align with the profiles of the program learners and their requirements, such as target roles.

The suggested education program design process is based on the ADDIE model [27]. The ADDIE model is a widely recognized and traditional process utilized by instructional designers and training developers, comprising five distinct phases (Table 4).

This study focuses on the 'Design' phase, offering suggestions for the roles, tasks, and competencies necessary for the smart grid cybersecurity field. The education program design process can be supported by tools and methods, defined in the methods and tools bank (Section 4).

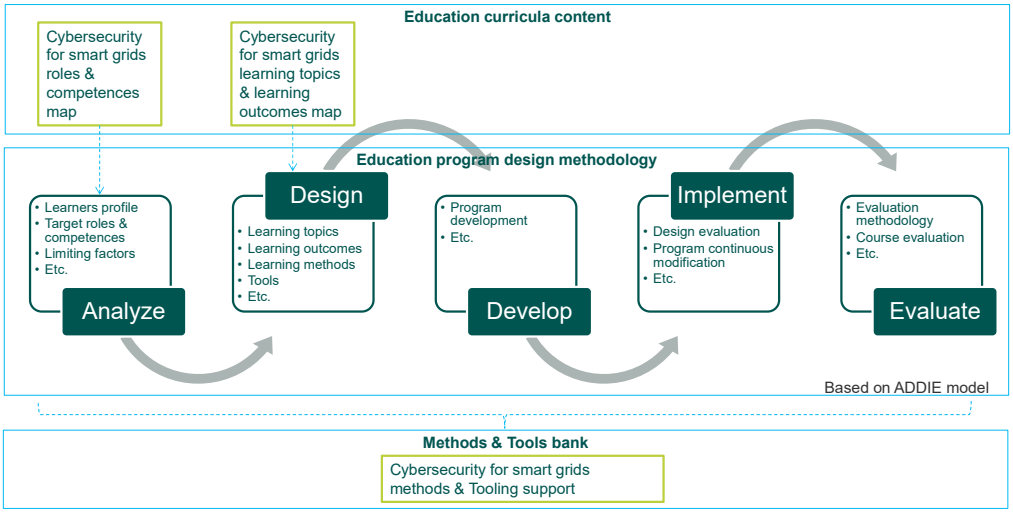

Figure 5. Education design process.

Table 4. Education design process (adapted from [27]).

Phase	Description
Analysis	Learners' profiles analysis (including their characteristics, existing competence, expected target roles and training needs), instructional goals and objectives definition. The program must be designed to incorporate competences that are required for learners' target roles.
Design	Study program objectives, learning topics, learning outcomes and teaching methods definition. This paper defines a set of learning topics and learning outcomes that defined roles must have (Section 4.1). The topics are encapsulated in knowledge areas and units. The topics must be selected based on identified learners target roles. Learners can have individual plans, based on their existing competences (e.g., if learner has previous education in IT specific cybersecurity and he aims to became Security architect in energy sector institution, he/she must obtain smart grid specific cybersecurity competences).
Development	Study program materials development and loading in e-learning systems (if applicable).
Implementation	Study program and courses delivery.
Evaluation	Feedback and data collection for improvement areas identification.

5.2. Work Roles and Competences

Smart grid cybersecurity roles define the workforce requirements regarding specialists' tasks and competencies. The smart grid cybersecurity work roles are based on the most common cybersecurity roles in the ENISA framework. According to the focus groups with industry representatives, the following roles has been selected: chief information security officer (CISO), cybersecurity architect, cyber incident responder, cybersecurity auditor, cybersecurity implementer, cyber legal, policy and compliance officer, and cybersecurity risk manager. The tasks and competences of the roles have been adapted, considering smart grid specifics and identified skill gaps (Section 4). Additionally, the roles were supplemented by new smart grid-specific roles: energy citizen, grid assets manager, and grid communication engineer. The common business objectives for smart grid specific roles are [28]: "maintain safety, maintain power system reliability, maintain power system resilience, and support grid modernization". Illustrative examples of smart grid-specific competencies, operational competencies, and general competencies are compiled in Table 5, while a full set of roles, tasks, and competencies is available in the project report [29].

Table 5. Illustrative example of smart grid cybersecurity roles.

Tasks	IT-Specific Competences	Smart Grid Competences	Operational Competences	General Competences
Role: Grid Asset Manager				
- Being updated on the subject of the communication protocols that are used by the various components. - Identify cybersecurity risks in the form of proprietary software, legacy devices, devices that were not designed to operate while connected to the internet (designed when security by obscurity was used). - Being updated on the subject of the limitations that the legislation poses for a smart grid to operate (requested ancillary services, reserve capacity, limitations in reconnecting after loss of power). - Being updated on the ownership of the various devices. Inform Cyber Incident Responder for changes.	N/A	Identify all distributed, modernized assets owned by the enterprise, including IT components embedded in OT devices within the grid modernization infrastructure [20].	- Empower business asset owners, executives, and other stakeholders to make risk-informed decisions for managing and mitigating risks. - Propose and manage risk-sharing options.	- Communicate, coordinate and cooperate with internal and external stakeholders in a written and oral form [26,30]. - Manage time, people, assets and projects [31]. - Collaborate effectively in a team [32].
Role: Energy Citizen				
- Use information and information systems in a secure manner. - Use energy systems and connected devices in a secure manner.	Understand and manage information system use through intuitive and undemanding means.	Understand and manage energy use through intuitive and undemanding means.	- Understand cybersecurity threats and their potential impact. - Understand personal data protection legalization and data subject rights. - Identify and assess information security risks.	- Understand, practice and adhere to ethical requirements and standards. - Think critically, strategically and systematically [15,21,22,24].

Grid asset manager is a typical role acknowledged by the research team. The role involves selecting third-party components based on technical attributes and serving as a central source of knowledge and communication regarding a system's components, including its characteristics, communication protocols, and ownership status. The energy citizen is another important role, identified in related research [33] and acknowledged by the research team. The role engages with energy as a meaningful part of citizen's practices, i.e. the use of energy systems and connected devices.

The defined roles, tasks, and competencies, along with the identified skill gaps, provide grounds for the curriculum recommendations by extending "ACM Cybersecurity Curricular Guidance for Associate-Degree Programs 2020 Cyber2yr2020" with smart grid cybersecurity-related knowledge areas, units, and learning outcomes. Moreover, other supplements are suggested, mainly related to the organizational security and societal security knowledge areas. The smart grid security knowledge area focuses on protecting the modern power grid's assets and data from unauthorized access and any sort of malicious activity that might result in malfunction or degradation of the grid's performance. Information technology, operational technology, advanced metering infrastructure, the SCADA supervisory and control system, and communication protocols are the key elements for smart grid security. The following knowledge units are suggested: Smart Grid Supply Chain, Smart Grid Infrastructure, Electrical and Cyber-physical Systems, Smart Grid Threats, Risks and

Vulnerabilities, and IT and OT Security. The suggested learning outcomes are summarized in Table 6.

Table 6. Suggested smart grid cybersecurity knowledge overview.

Learning Outcomes	Competences
Smart Grid Supply Chain	- Describes the systems, facilities and processes involved in the production and delivery of energy as well as information exchange within the grid. - Highlights associated complexity of the smart grid since many systems are involved in generation and distribution of energy. - Introduces communication protocols used for data exchange - Gives emphasis on renewable resources integration, and their economic and environmental benefits. - Gives consideration to consumers and other stakeholders' demands
Smart Grid Infrastructure	Introduces the architecture of the smart grid, the components involved, the relationship between the different layers, the flow of information within the grid, and the control system
Electrical and Cyber-physical Systems	- Presents the structure and gives an example of conventional electrical systems. - Defines physical and cyber systems. - Introduces the concept of cyber-physical systems and gives an example of the smart grid as a typical cyber-physical system and what benefits such a concept brings. - Highlights other technologies related to the CPS concept, such as Internet of Things IoT, Cloud computing, and so.
Smart Grid Threats, Risks and Vulnerabilities	- Gives an introduction to risk analysis and risk assessment. - Defines threats, risks and vulnerabilities. - Describe risks associated with the modern grid. - Provides a framework and methodology for conducing risk and vulnerability analysis. - Introduces technologies used for risk mitigation. - Consider legalization, authority, and sector standards and/or practices.
IT and OT Security	- Differentiates between security practices for IT and OT systems. - Emphasis on the integration of different security solutions when dealing with Critical Infrastructure CI. - Reviews the CIA Triad model and introduces other measures. such as non-repudiation, utility, Authentication, Authorization, and Access Control AAA concepts. - Presents the different drives and methods for hacking the grid. - Presents the different attack tools. - Introduces models utilized for securing the grid, such as NISTIR 7628, EU M/490, and SGCG reference architecture, as well as ISA-62443 zones and conduits, and the McAfee security model for Critical Infrastructure (CI). - Introduces the concepts of Layered security architecture, endpoints, field zone protection, control zone protection, zone separation, advanced network monitoring, and situational awareness.

5.3. Methods and Tools Bank

The methods and tools bank lists and describes methods and tools that are suggested to be used in smart grid cybersecurity education (Figure 6). In the literature review, eight educational methods were mentioned as applied in teaching cybersecurity (involving smart grids and power systems): (1) experiential learning, (2) active learning, (3) cooperative learning, (4) flipped classroom, (5) inquiry-based learning, (6) problem-based learning, (7) project-based learning, and (8) gamification. From the toolset perspective, simulation testbeds were mentioned as the most promising tool to simulate smart grid-specific cases. According to the research team evaluation, the most frequently used tools and methods are simulation tools, CPES laboratories and testbeds, gamification, project/problem-based learning, and flipped learning. As the discipline of smart grid cybersecurity is novel, the majority of the methods were investigated in terms of the general cybersecurity education

provision with the assumption that they would be applicable also for the smart grid security. This assumption was validated with the expert group.

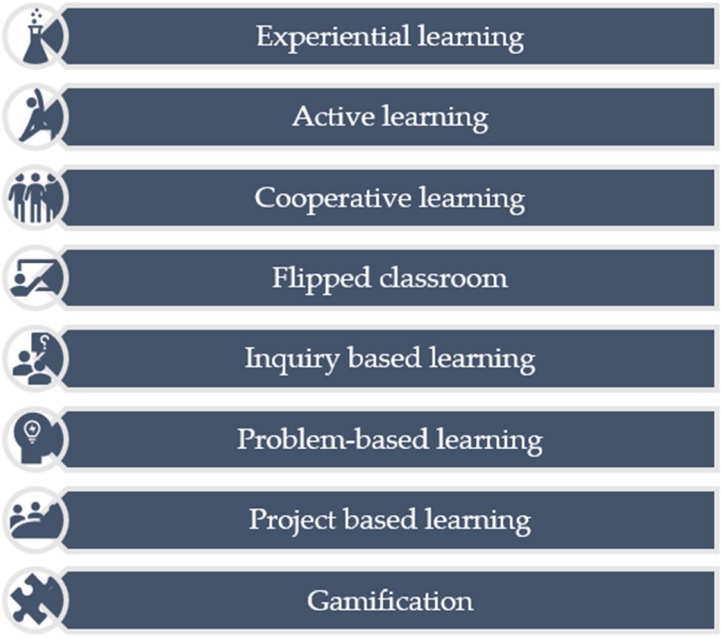

Figure 6. Prospective tools and methods for smart grid cybersecurity education.

Smart grid laboratory is the primary training tool applied specifically for cybersecurity in smart grids. Testbeds serve to simulate real-life smart grid systems, considering software components and hardware components. Certain testbeds simulate only specific system elements, whereas others replicate the entire system. Combining a real-time simulator with actual hardware, such as inverters and PMUs, to emulate an entire microgrid represents the most comprehensive and authentic method for investigating an electrical grid's response to cyber-attacks. In the literature, several simulation testbed use cases are described. The study [34] outlines the utilization of a testbed composed of commercial equipment, software, hardware, and simulation/emulation, through which students can learn about communications and conduct comprehensive security analyses. A testbed using a real-time digital simulator to simulate a power system is developed in [35]. The communications subsystem is simulated through DeterLab, which allows for the creation, planning, monitoring, and analysis of cybersecurity aspects of the system. A larger testbed is used in [36]. With a control system at its heart, a distribution management system, along with smart meters, RTUs, and PVs, is simulated. Based on this testbed, a subject is developed regarding "Critical infrastructure security: Smart Grid", where students learn about SCADA systems and the communication protocols that are used for the control of power systems in general. However, there are several prerequisites for testbeds' usage. This educational tool relies on the use of equipment. It can be a mixture of commercial and non-commercial equipment, simulation tools, real-time simulation (specific computers), a remote connection system, and/or virtual machines. The remote and/or 24 h access of the students to the equipment requires the need for additional staff to support lab access.

Active learning is not only about including activities in the learning process, but rather intends to increase the engagement of the students by asking them to participate in the learning process and processing their responses before new information is introduced. The main elements or activities used are talking and listening, writing, doing, reading, and reflecting, and they can be done individually, in pairs, or in smaller or larger groups [37]. According to [38], active learning techniques include both experiential (like simulations) and non-experiential techniques. They are all characterized by student involvement, the development of students' skills, and higher-order thinking on behalf of the

students. By fostering collaboration and communication among trainees, these methods simulate the teamwork necessary to address complex cybersecurity challenges within dynamic operational environments. Personalized instruction and targeted feedback further enhance learning outcomes, empowering trainees to effectively safeguard critical energy infrastructure against evolving cyber threats.

Gamification employs mechanisms from game design to increase students' engagement [39]. Examples of such elements and mechanisms include narrative storytelling, time constraints for task completion, point systems, badges, and level progression. Gamification consists of three elements: mechanics, dynamics, and emotions. Mechanics refers to the decisions of the teachers (rules and context of the game). The dynamics are the result of the implemented mechanics in the form of strategies employed by the students. The emotions aimed for are fun, excitement, and curiosity. While employing an actual game is not obligatory, certain types of games can be readily tailored to meet the demands of a technical subject. Strategy games have the potential to train learners in efficiently managing limited resources, such as generator allocation, and developing strategies for planning and recovering from incidents [39]. An analysis of the different types of drivers for players and kinds of games is given in [40].

Problem-based learning involves students working together to explore real-world problems and propose solutions, which they then present to their peers. Project-based learning, like problem-based learning, extends over a longer period and focuses on achieving tangible outcomes rather than theoretical solutions. Problem- and project-based learning require a small group of students to work on an open-ended problem. Initially, students are introduced to the problem, then they need to identify the facts, generate some hypotheses, identify the knowledge deficiencies, and apply the new knowledge through self-directed learning. In the cybersecurity education area, there are several cases of the method's successful application. The study [41] describes the method's application in social engineering and unauthorized data access cases' investigation. Campus-area network exploration is proposed in [42] to identify cyber threats and propose security measures. Several scenarios and practices are proposed for enabling problem-based learning in training regarding industrial control systems [43]. Meanwhile, problem-based learning and project-based learning could be more complex in the case of large and un-homogeneous student groups with a low level of previous knowledge and autonomy.

The flipped classroom method involves students learning lecture material at home and using class time to enhance their understanding with instructor guidance. Study materials in the flipped classroom model can range from course textbooks to web videos or slides prepared by the teacher. In the classroom, educators may utilize various techniques, including active learning methods such as concept maps, experiential learning through simulations, and problem-based learning approaches to foster higher levels of critical thinking skills among students. In terms of cybersecurity education, the flipped classroom method's successful application has been highlighted in several studies. Project-based learning and the flipped classroom method's introduction into the teaching of computer science subjects was investigated in [44]. The study tested benefits of applying different teaching methods in a computer course over a six-year period. It was observed that providing students with videos of hands-on activities for later review proved to be advantageous. This approach notably elevated students' interest levels and motivation. An increase in student engagement was also reported also in [45]. This approach has been effectively implemented in the realm of computer security. Following a 15-week course where the approach was tested, the authors contend that applying the flipped classroom method enhances student engagement. The flipped classroom method also seems promising for smart grid specific cybersecurity education [46]. This study proposes teaching industrial control system security by applying flipped classroom and gamification elements. It focuses on cyber-attack investigation and encompasses a diverse range of tasks, such as preparing presentations, perusing papers, outlining game concepts, iteratively refining drafts to completion, and designing surveys for game evaluation.

To summarize, there is a number of methods and tools to be applied in smart grid cybersecurity education. The research team highlighted that conventional teaching methods used in general cybersecurity education could also be adapted to address the specifics of smart grid technology. In addition, it is argued that, from the toolset perspective, the most promising are simulation tools, CPES laboratories, and testbeds.

5.4. Implementation Roadmap

The implementation roadmap suggests the main activities to be performed to implementing the proposed educational approach, with a focus on the preparation of a new curriculum and study programs, considering the proposed education design methodology:

Stakeholder analysis—identify the main stakeholders of the smart grid cybersecurity educational program who have concerns and interest regarding the topic, including industry representatives responsible for validating workforce requirements, community representatives, and educational and research institutions;

Learning objectives definition—define the learning objectives centered on cybersecurity in smart grids through collaboration with stakeholders to guarantee alignment with their requirements;

Curriculum content preparation—outline and describe smart grid cybersecurity curriculum content concerning the industry guidelines, workforce competence models, and stakeholders' recommendations. Consider technical skills and soft skills' implementation;

Delivery mechanisms identification—recognize the delivery mechanisms of the educational program, encompassing various methods and tools to enable smart grid cybersecurity-specific competency development;

Evaluation mechanisms identification—define the evaluation mechanisms to assess the learning outcomes' realization, including various methods and tools such as developing assessment methods and tools, e.g., quizzes, exams, and hands-on projects that simulate real-world cybersecurity scenarios in smart grids.

Instructors training—educate instructors on the effective delivery of the educational curricula, such as training material provision and conducting workshop, addressing the distinctive challenges associated with securing smart grid infrastructure;

Education curricula implementation—promote the program to individuals and organizations within the smart grid industry, enrolling students, and providing partnerships with industry stakeholders; practical study program execution;

Education curricula evaluation and improvement—evaluate and improve the education curriculum model by gathering feedback from students, instructors, and industry representatives, analyzing assessment results, and updating the curriculum content to ensure that it remains relevant to the rapidly evolving smart grid cybersecurity landscape.

The potential timeframe is illustrated in Figure 7, considering that the entire duration for implementing the study program could range from 24 to 42 months.

It is suggested to group the main activities into the four phases. The first phase includes the planning of the education program. The second phase involves the curriculum development, while the third phase focuses on the pilot testing of the education program with a small group of the students and evaluation of the required amendments. The fourth phase concludes the implementation of the program with the program's delivery and continuous improvement.

The primary limitation of implementing the proposed educational approach lies in the relatively lengthy release cycle, particularly concerning the establishment of new graduate- or undergraduate-level study programs. Given the dynamic nature of smart grid cybersecurity, the regular reviewing and updating of the curriculum content is essential to ensure alignment with evolving industry trends and technological advancements.

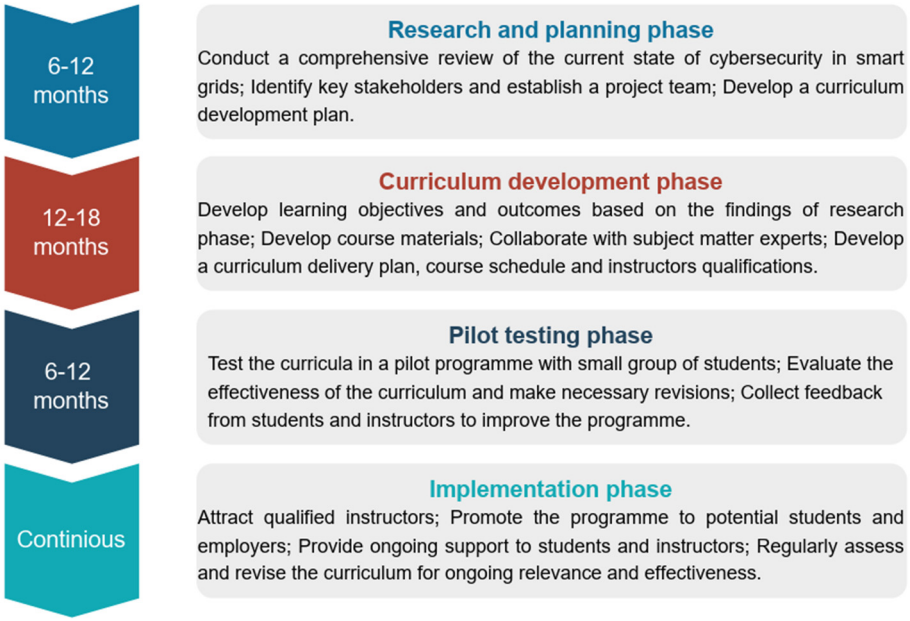

Figure 7. Proposed smart grid cybersecurity curriculum implementation roadmap.

6. Benchmarking and Evaluation

The suggested educational approach was introduced to the stakeholders for initial assessment and feedback gathering. The benchmarking was implemented in two stages. Firstly, through a literature review, the characteristics that benefit the modern educational approaches were identified, and, secondly, a questionnaire was formulated to obtain the perspective of the stakeholders. The questionnaire included eight questions concerning the proposed methods, tools, and education content. The selected stakeholder group was composed of students interested in smart grid cybersecurity, as educators and industry experts' requirements were collected already during the education approach development. To enable student-oriented education provision, feedback from students was gathered.

The questionnaire had eight answers which can be perceived as a qualitative indicator, rather than quantitative data. All respondents had a background in smart grid cybersecurity, mainly from the perspective of the energy discipline. Half of the students were not familiar with the educational methods used (such as gamification, virtual labs etc.) and the other half were familiar with them. Probably, this indicates that familiarity with the methods is heavily influenced by the institute that the students were enrolled in. Regarding the cybersecurity frameworks, half of the students were aware of the NIST NICE framework, but their knowledge about this and other similar competence frameworks was limited. During the evaluation, the students were introduced to proposed smart grid cybersecurity education content, represented in the form of a massive open online course (MOOC) [47]. In addition to the MOOC, real-time simulator operation and learning scenarios for smart grid cybersecurity were also presented in a several-hour-long workshop. The students positively evaluated the suggested smart grid education topics and the use of simulation tools and gamification as educational methods for smart grid cybersecurity (Figure 8).

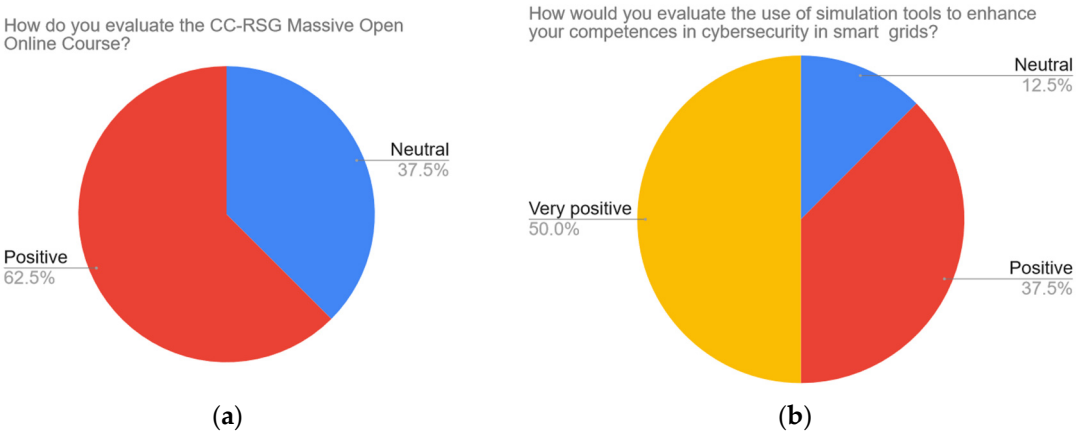

Figure 8. (**a**) Smart grid cybersecurity course evaluation results; (**b**) simulation tools usage in smart grid cybersecurity evaluation results.

In terms of comparing the proposed approach with traditional methods, students strongly agreed that it elevates the significance and credibility of the curriculum contents, as well as enhances learners' interest in the subject. Moreover, they expressed positivity regarding the improved efficiency and flexibility of the curriculum. Students also indicated optimism about the ease of implementing the simulation case studies presented to them (Figure 9) and expressed a preference for subjects with a similar approach in the future.

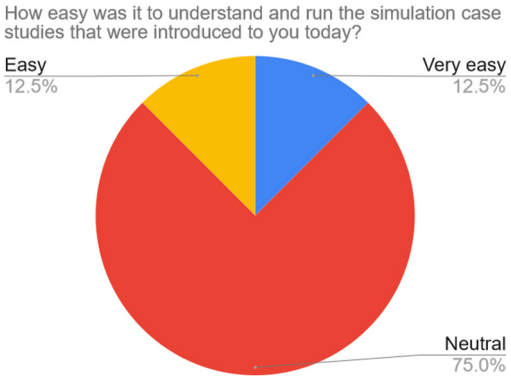

Figure 9. Educational approach evaluation results.

Other suggestions from the students include the addition of the subject of automation/control in the presented case studies and the possibility to work individually instead of working in small teams.

To summarize, the preliminary evaluation of the proposed approach highlighted that the content and proposed educational methods and tools are perceived positively from the student perspective. Meanwhile, the limitation of the evaluation is the rather small student group; therefore, further evaluation must be performed in the future. This is the early stage of applying this study's result for practical use in the classroom or as a course in some universities to obtain students' experiences regarding their learning process using this designed MOOC. As the education approach was prepared concerning the literature suggestions, industry expert recommendations, and educators' experience, additional evaluation sessions with these stakeholder groups were not conducted. While it would be preferable in the future, the primary concern regarding the comprehensive evaluation of this method is the limited number of smart grid cybersecurity experts, considering that this is a growing discipline with a relatively short history.

7. Discussion and Conclusions

This research investigated educational offerings and skill gaps in smart grid cybersecurity and proposed an educational approach to enhance smart grid resilience by bridging those skill gaps. It was concluded that, globally and within the EU, a substantial and ongoing gap in cybersecurity skills exists. Cybersecurity education is a strategic digital capability that needs to be enhanced by providing formal and informal education. The educational offerings of specialized programs do not fully meet all requirements, particularly for adults seeking to re-skill or up-skill, as well as new specialists. While general cybersecurity is integrated into various educational formats, such as higher education, continuing education, and MOOCs, smart grid security issues are relatively infrequently addressed.

This study proposed an educational approach for smart grid cybersecurity education program development, concerning the education content, education program's preparation steps, and useful tools and methods to be applied. It is designed to serve as a handbook for educators, aiding in the development of smart grid cybersecurity education programs across various educational levels and formats, encompassing both formal and informal settings. It recognizes 10 key cybersecurity roles that are relevant to the smart grid context. For each work role, essential tasks are delineated, and smart grid-specific competencies are detailed. The knowledge areas and units are adopted based on the ACM Committee for Computing Education in Community Colleges (CCECC). In addition, a specific smart grid security knowledge unit is developed to focus on protecting the assets and the data of grids from unauthorized access or any sort of malicious activities that might result in the malfunction or degradation of the grid performance.

The primary constraint of the proposed approach lies in its limited evaluation and practical validation. Currently, preliminary evaluation results are presented, including a relatively small stakeholder group's opinion, although it provides positive initial evaluation results. The future research directions include comprehensive approach evaluation, piloting, and improvement based on evaluation results. The proposed approach needs evaluation from users/students at the end of the course for the feedback to improve the content and method for teaching.

Author Contributions: Conceptualization, T.V. and A.R.; methodology, J.K., J.P., J.B., M.V. and R.P.-D.; validation, A.R. and M.V.; formal analysis, J.K., J.B., B.E. and J.P.; investigation, J.K., J.B., B.E. and J.P.; original draft preparation, J.B., J.P. and R.P.-D.; writing—review and editing, A.R. and T.V.; visualization, R.P.-D.; supervision, A.R. and T.V.; project administration, T.V.; funding acquisition, T.V. All authors have read and agreed to the published version of the manuscript.

Funding: This project has received funding from the European Union's Erasmus+ Programme under Grant Agreement No. 2020-1-FI01-KA203-066624.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding authors.

Acknowledgments: Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG) project is funded by Erasmus+ Strategic Partnership program. The European Commission's support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. European Commission. The Digital Europe Programme. *Off. J. Eur. Union* **2021**, *2019*. Available online: https://digital-strategy.ec.europa.eu/en/activities/digital-programme (accessed on 11 April 2024).
2. European Union Agency for Cyber Security a Trusted and Cyber Secure Europe: ENISA Strategy. 2020. Available online: https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy (accessed on 11 April 2024).

3. Jelo, M.; Helebrandt, P. Gamification of cyber ranges in cybersecurity education. In Proceedings of the 20th Anniversary of IEEE International Conference on Emerging eLearning Technologies and Applications, ICETA 2022—Proceedings, Stary Smokovec, Slovakia, 20–21 October 2022. [CrossRef]
4. ISC2. ISC2_Cybersecurity_Workforce_Study_2023. 2023. Available online: https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap (accessed on 11 April 2024).
5. Sadik, S.; Ahmed, M.; Sikos, L.F.; Najmul Islam, A.K.M. Toward a sustainable cybersecurity ecosystem. *Computers* **2020**, *9*, 74. [CrossRef]
6. Dawson, J.; Thomson, R. The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Front. Psychol.* **2018**, *9*, 284332. [CrossRef]
7. Petersen, R.; Santos, D.; Smith, M.; Witte, G. *Workforce Framework for Cybersecurity (NICE Framework)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
8. European Union Agency for Cybersecurity, E. European Cybersecurity Skills Framework. 2022. Available online: https://WwwEnisaEuropaEu/Publications/European-Cybersecurity-Skills-Framework-Role-Profiles (accessed on 11 April 2024).
9. Neigel, A.R.; Claypoole, V.L.; Waldfogle, G.E.; Acharya, S.; Hancock, G.M. Holistic cyber hygiene education: Accounting for the human factors. *Comput. Secur.* **2020**, *92*, 101731. [CrossRef]
10. Pirta-Dreimane, R.; Brilingaitė, A.; Majore, G.; Knox, B.J.; Lapin, K.; Parish, K.; Sütterlin, S.; Lugo, R.G. Application of intervention mapping in cybersecurity education design. *Front. Educ.* **2022**, *7*, 998335. [CrossRef]
11. European Commission. *Shaping Europe's Digital Future*; Digitalisation of the European Energy System; European Commission: Luxembourg, 2023.
12. Tajalli, S.Z.; Mardaneh, M.; Taherian-Fard, E.; Izadian, A.; Kavousi-Fard, A.; Dabbaghjamanesh, M.; Niknam, T. DoS-Resilient Distributed Optimal Scheduling in a Fog Supporting IIoT-Based Smart Microgrid. *IEEE Trans. Ind. Appl.* **2020**, *56*, 2968–2977. [CrossRef]
13. Directorate-General for Communications Networks Networks C and T. Digital Skills & Jobs Platform. Cybersecurity Skills Academy. 2023. Available online: https://digital-skills-jobs.europa.eu/en (accessed on 11 April 2024).
14. Cyber2yr2020 Task Group. *Cybersecurity Curricular Guidance for Associate-Degree Programs*; Association for Computing Machinery: New York, NY, USA, 2020. [CrossRef]
15. Joint Task Force on Cybersecurity Education. Curricula 2017 Cybersecurity Curriculum—Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. 2017. Available online: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf (accessed on 11 April 2024).
16. NSA and DHS. 2020 CAE Cyber Defense (CAE-CD) Knowledge Units. 2020. Available online: https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf (accessed on 11 April 2024).
17. Romanovs, A.; Bikovska, J.; Peksa, J.; Vartiainen, T.; Kotsampopoulos, P.; Eltahawy, B.; Lehnhoff, S.; Brand, M.; Strebko, J. State of the art in cybersecurity and smart grid education. In Proceedings of the EUROCON 2021—19th IEEE International Conference on Smart Technologies, Proceedings, Lviv, Ukraine, 6–8 July 2021. [CrossRef]
18. Brezhniev, E.; Kharchenko, V. Smart GRID Safety and Security: Educational and Research Activities. *Inf. Secur. Int. J.* **2016**, *35*, 165–178. [CrossRef]
19. Siemers, B.; Attarha, S.; Kamsamrong, J.; Brand, M.; Valliou, M.; Pirta-Dreimane, R.; Grabis, J.; Kunicina, N.; Mekkanen, M.; Vartiainen, T.; et al. Modern trends and skill gaps of cyber security in smart grid: Invited paper. In Proceedings of the EUROCON 2021—19th IEEE International Conference on Smart Technologies, Proceedings, Lviv, Ukraine, 6–8 July 2021. [CrossRef]
20. Hevner, A.R.; March, S.T.; Park, J.; Ram, S. Design science in information systems research. *MIS Q.* **2004**, *28*, 75–105. [CrossRef]
21. Hevner, A.R. A Three Cycle View of Design Science Research. *Scand. J. Inf. Syst.* **2007**, *19*, 4.
22. Leventon, J.; Fleskens, L.; Claringbould, H.; Schwilch, G.; Hessel, R. An applied methodology for stakeholder identification in transdisciplinary research. *Sustain. Sci.* **2016**, *11*, 763–775. [CrossRef]
23. De Montfort University. Cyber Security and Software Technology Doctoral Programme. Available online: https://WwwDmuAcUk/Study/Technology/Doctoral-Training-Programme/Cyber-Security-Doctoral-ProgrammeAspx (accessed on 11 April 2024).
24. Cabaj, K.; Domingos, D.; Kotulski, Z.; Respício, A. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Comput. Secur.* **2018**, *75*, 24–35. [CrossRef]
25. Pirta-Dreimane, R.; Brilingaite, A.; Roponena, E.; Parish, K. Multi-dimensional Cybersecurity Education Design: A Case Study. In Proceedings of the 2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Falerna, Italy, 12–15 September 2022; pp. 1–8. [CrossRef]
26. Hajny, J.; Ricci, S.; Piesarskas, E.; Levillain, O.; Galletta, L.; de Nicola, R. Framework, Tools and Good Practices for Cybersecurity Curricula. *IEEE Access* **2021**, *9*, 94723–94747. [CrossRef]
27. Morrison, G.; Ross, S. *Designing Effective Instruction*, 7th ed.; John Wiley & Sons: Hoboken, NJ, USA, 2013.
28. Marron, J.; Gopstein, A.; Bartol, N.; Feldman, V. *Cybersecurity Framework Smart Grid Profile*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019. [CrossRef]
29. Pirta-Dreimane, R.; Romānovs, A.; Bikovska, J.; Pekša, J.; Valliou, M.; Kotsampopoulos, P.; Eltahawy, B.; Vartiainen, T.; Mekkanen, M.; Kamsamrong, J. *The CYBERSECURITY Education in Smart Grids Body of Knowledge Development and Implementation Roadmap*; University of Vaasa: Vaasa, Finland, 2023.

30. Bret Fund. 16 Soft Skills You Need to Succeed in Cyber Security. 2021. Available online: https://FlatironschoolCom/Blog/Soft-Skills-Cyber-Security/ (accessed on 11 April 2024).
31. Frederick Scholl. Developing Your Portfolio of Soft Skills for Cybersecurity. 2020. Available online: https://wwwQuEdu/Quinnipiac-Today/Developing-Your-Portfolio-of-Soft-Skills-for-Cybersecurity-2020-01-29/ (accessed on 11 April 2024).
32. Steinke, J.; Bolunmez, B.; Fletcher, L.; Wang, V.; Tomassetti, A.J.; Repchick, K.M.; Zaccaro, S.J.; Dalal, R.S.; Tetrick, L.E. Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. *IEEE Secur. Priv.* **2015**, *13*, 20–29. [CrossRef]
33. Goulden, M.; Bedwell, B.; Rennick-Egglestone, S.; Rodden, T.; Spence, A. Smart grids, smart users? the role of the user in demand side management. *Energy Res. Soc. Sci.* **2014**, *2*, 21–29. [CrossRef]
34. Sauer, P.W.; Sanders, W.H. A project to develop a trustworthy cyber infrastructure for the power grid (TCIPG). In Proceedings of the IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 22–26 July 2012. [CrossRef]
35. Liu, R.; Srivastava, A. Integrated simulation to analyze the impact of cyber-attacks on the power grid. In Proceedings of the 2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2015—Held as Part of CPS Week, Proceedings, Seattle, WA, USA, 13 April 2015. [CrossRef]
36. Xie, J.; Bedoya, J.C.; Liu, C.C.; Hahn, A.; Kaur, K.J.; Singh, R. New educational modules using a Cyber-Distribution system testbed. *IEEE Trans. Power Syst.* **2018**, *33*, 5759–5769. [CrossRef]
37. Zayapragassarazan, Z.; Kumar, S. Active Learning Methods. *NTTC Bull.* **2012**, *19*, 3–5.
38. Hamer, L.O. The Additive Effects of Semistructured Classroom Activities on Student Learning: An Application of Classroom-Based Experiential Learning Techniques. *J. Mark. Educ.* **2000**, *22*, 25–34. [CrossRef]
39. Deterding, S.; O'Hara, K.; Sicart, M.; Dixon, D.; Nacke, L. Gamification: Using game design elements in non-gaming contexts. In Proceedings of the Conference on Human Factors in Computing Systems—Proceedings, Vancouver, BC, Canada, 7–12 May 2011. [CrossRef]
40. Markopoulos, A.P.; Fragkou, A.; Kasidiaris, P.D.; Davim, J.P. Gamification in engineering education and professional training. *Int. J. Mech. Eng. Educ.* **2015**, *43*, 118–131. [CrossRef]
41. Shivapurkar, M.; Bhatia, S.; Ahmed, I. Problem-based Learning for Cybersecurity Education. *J. Colloq. Inf. Syst. Secur. Educ.* **2020**, *7*, 6.
42. Sherman, A.T.; Peterson, P.A.; Golaszewski, E.; LaFemina, E.; Goldschen, E.; Khan, M.; Mundy, L.; Rather, M.; Solis, B.; Tete, W.; et al. Project-Based Learning Inspires Cybersecurity Students: A Scholarship-for-Service Research Study. *IEEE Secur. Priv.* **2019**, *17*, 82–88. [CrossRef]
43. Junqueira, B.S.; de Souza, M.V.; Lima, V.B.; Lepikson, H.A. Learning Proposal for Cybersecurity for Industrial Control Systems Based on Problems and Established by a 4.0 Didactic Advanced-Manufacturing-Plant. In Proceedings of the VII Simpósio Internacional de Inovação e Tecnologia, Online, 20–22 October 2021. [CrossRef]
44. Malik, K.M.; Zhu, M. Do project-based learning, hands-on activities, and flipped teaching enhance student's learning of introductory theoretical computing classes? *Educ. Inf. Technol.* **2023**, *28*, 3581–3604. [CrossRef] [PubMed]
45. Carranza, A.; DeCusatis, C. Hybrid implementation of flipped classroom approach to cybersecurity education. *Natl. Cybersecur. Inst. J.* **2015**, *2*, 45–54.
46. Celeda, P.; Vykopal, J.; Svabensky, V.; Slavicek, K. KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems. In Proceedings of the SIGCSE 2020—51st ACM Technical Symposium on Computer Science Education, Portland, OR, USA, 11–14 March 2020. [CrossRef]
47. Eltahawy, B.; Valliou, M.; Kamsamrong, J.; Romanovs, A.; Vartiainen, T.; Mekkanen, M. Towards A Massive Open Online Course for Cybersecurity in Smart Grids—A Roadmap Strategy. In Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference Europe, Novi Sad, Serbia, 10–12 October 2022; Volume 2022. [CrossRef]