State of the Art, Trends and Skill-gaps in Cybersecurity in Smart Grids (Executive Report)

Authors:

Jirapa Kamsamrong, Björn Siemers, Shadi Attarha,
Sebastian Lehnhoff, Maria Valliou, Andrejs Romanovs,
Jana Bikovska, Janis Peksa, Ruta Pirta-Dreimane,
Janis Grabis, Nadezhda Kunicina, Julija Srebko,
Tero Vartiainen, Bahaa Eltahawy, Mike Mekkanen

Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)

Erasmus+ Strategic Partnership Project

Intellectual Output 1

April 2022

Reviewer: Foivos Palaiogiannis

Coordinator: University of Vaasa
Partners: University of Oldenburg, Riga Technical University, National Technical University of Athens

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

Contents

List of Tables

List of Figures

Abbreviations

ACM	Association for Computing Machinery
AES	Advanced Encryption Standard
CIA	Confidentiality, Integrity, and Availability
CPES	Cyber Physical Energy System
DdoS	Distributed Denial of Service
DMZ	Demilitarized Zones
DoS	Denial of Service
ENISA	European Network and Information Security Agency
EU	European Union
HPC	Hardware performance counters
ICS	Industrial Control Systems
ICT	Information and Communications technology
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP	Internet Protocol
KUs	Knowledge Units
MOOC	Massive online open courses
VET	Vocational education and training
WP	Work Package

1. Introduction

Inrecent years, the energy sector has significantly expanded its digital maturitylevel by integrating various digital computing, communications, and industrialcontrol systems and technologies into a modernized and advanced power grid.In addition, Europe is aiming for fully integrated by straightening cross-border real-time market data exchange. Due to the enormous amount of data and wide use of IoT, the energy sector has become more attractive to hackers. It requires a wide range of multidisciplinary knowledge, including energy systems, computer networking, software, integrated systems, critical infrastructure security, and security management.

European Commission (EU) has launched the EU Cyber- security strategy to booster Europe's collective resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The strategy covers the security of essential services, including energy grids and the ever-increasing number of connected objects in citizens homes and offices factories. The strategy indicates that current EU cybersecurity capabilities are not sufficient. For cybersecurity capabilities improvement, both the EU Cybersecurity Strategy and Digital Europe program highlight the need for society's cybersecurity awareness straightening and new specialist's cybersecurity skills improvement.

1.1 Objectives

The objectives of the WP1 report are the following:

- Analyze the current trends and state of the art in academia
- Analyze the current and future curricula in higher education in the EU
- Analyze the skill needs of the industry
- Identify the skill gaps between the higher education and the industry needs base on the above analysis

1.2 Structure of the document

The document is structured as follows:

- Section 2 presents the research methodology that has been used in this study for collecting data and analyzing the result including the scope of thestudy.
- Section 3 illustrates the EU policy regarding cybersecurity in the smartgrid.
- Section 4 gives the perspective of academia through a literature review. The literature review aims to find the state of the art and current trendsin the education of the combined field of smart grids and cybersecurity.
- Section 5 presents a summary of existing education programs in cybersecurity, including higher education, continuing education, and MOOC.
- Section 6 identifies the industry and the skill needs that they require for their staffing. The identification of skill needs is achieved through a stakeholder workshop and a dedicated survey that was conducted.
- Section 7 presents useful tools for education in cybersecurity that are analyzed from the literature review and stakeholder survey.
- Section 8 is dedicated to the conclusion and initial requirements and recommendations regarding cybersecurity for smart grids education.

This document is completed with the conclusions and the bibliography.

2. Research Methodology

To gain insight and state-of-art cybersecurity in smart grid, the literature review is the first step to collect the research trends and the developments as well as the education method and existing offered curricula. The research methodology of the WP 1 is shown in Figure 1.

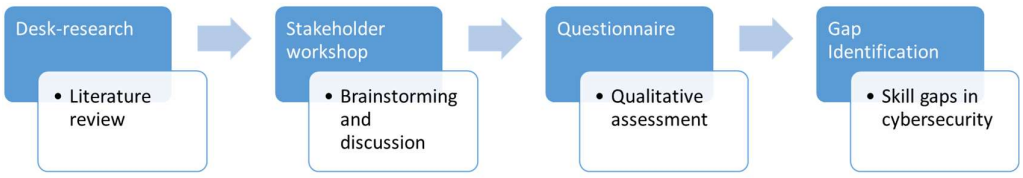

Figure 1 Research methodology of WP1

Desk research only provides information based on specific topics and domains depending on the research context and objective. To have a broader view of skill gaps in cybersecurity, especially from an industry perspective, the stakeholder workshop is essential for brainstorming and exchanging opinion between academia and industry.

3. Cybersecurity Policy in European Union

3.1 EU Policies and Strategic Directions

Cybersecurity policy can help the nation to address the essential aspects that are needed to prevent the negative impacts caused by cyber vulnerabilities. The European Commission and the high representative of the Union for Foreign Affairs and Security Policy has set a new 5-years EU cybersecurity strategy (2020-2025) to strengthen and secure digital system transformation against cyber threats. The strategy also emphasizes the importance of the cyber-skilled EU workforce. Cyber readiness and awareness among businesses and individuals remain low, and there is a significant shortage of cybersecurity workforce.

The EU cybersecurity strategy aligns EU Revised Digital Education Action Plan [1] which aims to raise cybersecurity awareness among individuals, especially children and young people, and organizations, especially SMEs. The plan has two priorities [1]: fostering a high- performing digital education ecosystem and [2] enhancing digital skills and competencies for the digital transformation. To meet the increasing demand for ICT workforce, the ICT security experts with operational knowledge in energy domains has become challenging and might require updating engineering and ICT education curricula. In addition, the education action plan has suggested educating and training stakeholders throughout the life cycle of new security solutions for Smart Grids. It states that education and training programs need to motivate stakeholders to think in different, innovative ways, and experience new approaches. The education and learning programs must focus on enhancing (and updating) awareness, providing insight and perspective into real-case scenarios, and developing, experimenting, and experiencing new (cybersecurity) concepts.

3.2 Organization related to cybersecurity

The EU Agency for cybersecurity (ENISA) is responsible for cybersecurity in the EU under the Cybersecurity Act [2]. The Cybersecurity Act enhances the ENISA body with the permanent mandate with concrete resources and tasks to increase the operational operation at the EU level. The ENISA is mandated to provide supports to EU member states for cybersecurity implementation by setting up the European cybersecurity certification [3]. Businesses in theEU must comply with the specific requirement of their products and services according to the directive.

3.3 Industry Studies and Recommendations

Industry associations and interest groups have studied the state of the art of existing cybersecurity education and prepared recommendations for cybersecurity curricula. However, thesuggestions about smart grids cybersecurity education are still limited. Joint Task Force on Cybersecurity Education consists of several associations that have prepared Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity [4]. The Joint Task Force shares opinion that the world faces a current and growing workforce shortage of qualified cybersecurity professionals, practitioners. The proposed cybersecurity education programs is shown in Figure 2.

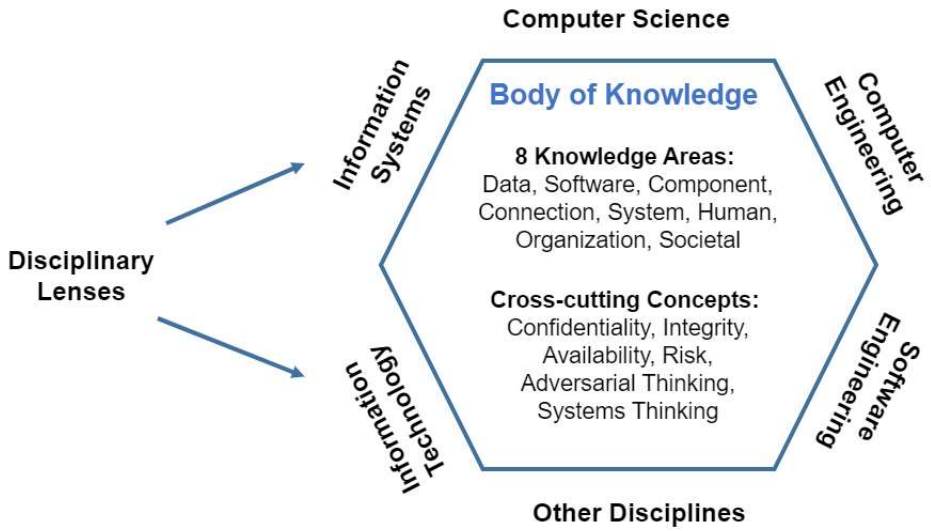

Figure 2 Cybersecurity education curriculum thought model [4]

3.4 Industry Studies and Recommendations

The energy sector recently has embarked on a digital transformational process introducing smart grids that triggers the need to reeducate the aging workforce and train the emerging workforce. An education platform to foster active learning topics should be provided as follows [5]:

- Cyber-infrastructure in the electric power grid;
- Monitoring and situational awareness;
- Advanced metering infrastructure;

- Smart grid guidance documents;
- Electric sector capability maturity model;
- Privacy in the smart grid;
- Critical infrastructure security examples and impact;
- A perspective on security;
- Security challenges in distribution automation;
- Embedded assessment;
- SCADA fundamentals and Robust control systems

4. State of the art and trends in cybersecurity in smart grids

4.1 Categorization

Google Scholar and Microsoft Academic are used to collect the relevant studies from 2017-2020 by using keywords “cyber security” and “smart grid”. The results have been shown in the title and also the content of the studies accounted for approximately 164 papers. All of these studies are reviewed at a high level to select the relevant studies related to cyber security and smart grid. Then, the selected studies are categorized by using the cybersecurity framework of ACM as shown in Figure 3. Each selected study is reviewedin detail to identify the purpose, method, and result of the study. The higher number, the more studies focused on the area. It should be noted that one study can cover more than one aspect.

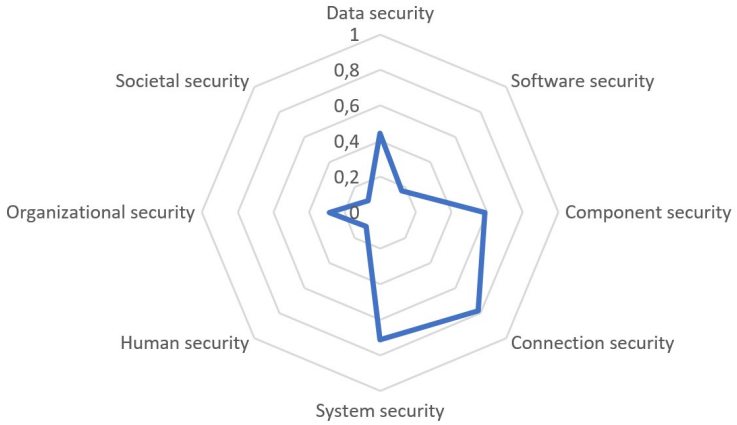

Figure 3 Categorization of skill gaps based on the literature review

It is clear that the focus on organization, human and societal security is very low compared to system security, connection security, and component security. Investigating on technical, system and components security is performed by using specific testbeds and/or cyber physical energy system (CPES) laboratories for the experiment and/or teaching students.

4.2 Technology and Education Development

4.2.1 Cyber Security Threat in Smart Grid

A CPES involves multiple domains in engineering and communication disciplines that require relevant curricula and essential tools to identify the vulnerabilities. To prevent previous and new cyberattack events in the future, passive and active countermeasures are highly needed. System operators and practitioners require a realistic environment testbed to examine real-life scenarios and countermeasures. Cyberattacks involve networked devices whose software becomes infected with malware. In recent years, there have been numerous cyberattacks against smart grid systems. These cyberattacks can be happened consciously or unconsciously and influence confidentiality, integrity, and availability (CIA). Thecyberattack classification considering the CIA aspect is present in Table 1.

Table 1 Cyberattacks classification considering CIA

Cyber Attack type	Short-description	Example
Confidentiality	Protection of data by preventing the unauthorized disclosure of information	Man-in-the-Middle, Stuxnet, Phishing campaign, SQL injection attack, Side-channel- attack, escalate privilege, AES Cache-Timing Attack
Integrity	Intercepted and altered the message	False data injection, Load Altering attack, Phishing campaign, Tampering
Availability	Either block or delay the message/traffic	DoS/DDoS, Ransomware, Blocking attack, Escalate privilege, AES Cache-Timing Attack, Buffer overflow

4.2.2 Countermeasures

There is no single countermeasure to encounter all the attacks. Each attack requires countermeasures depending on the attack context. Several types of research on cybersecurity in the smart grid have suggested common counter- measures such as intrusion detection system (IDS), demilitarized zones (DMZ), hardware performance counters (HPC), interlock, log management, multi-factor authentication, active network monitoring, IP address, and application whitelisting, network segmentation and smart switches/routers, security awareness training.

4.2.3 Cyber Physical Energy System (CPES) Laboratory

Up to date, universities, government, and industry have set up testbeds to experiment with cybersecurity research and development. Cyber security topics are complex and involve several knowledge backgrounds e.g. computer engineering, electrical engineering, industrial engineering. Interconnection between domains enables practitioners to understand and have a broad overview of how different domains are connected. Multi-purposes and domains testbed has a greater advantage compared to the single purpose and/or single domain. A simple and low-cost testbed allows undergraduate students to replicate and explore the fundamental principle of cyber security. A sophisticated laboratory is high cost, a collaboration between industry and university can accelerate state-of-the-art innovative research.

4.2.4 Communication protocols

Cybersecurity research and education also focus on the communication protocols between the devices and/or the systems. The protocols are tested within the laboratory and specific testbed. For any data transmission within a network, it is essential to have standard protocols that defines certain rules for communication. There are several communication protocols that have been used in the smart grid depending on the latency, reliability, data rate, scalability and security. The IEC 61850 enables the interoperability between different components and functions from different manufacturers.

As IEC 61850 gains popularity in the power automation systems because of the ease of connection via ethernet and standardized message structures, vulnerabilities have been pointed out for gaining access to confidential data and disrupting service caused by the integrity of data exchange. To strengthen cybersecurity for power communications, IEC 62351 can provide end-to-end information security for power systems control operations. It defines the different requirements for secure data communication and processing in power systems. The IEC 62351 standard focuses on the security of IEC TC 57 protocols that can support authentication and encryption. IEC 62351 can secure IEC61850 messages such as GOOSE, SV, R-GOOSE, R-SV.

4.3 Gaps analysis

The power system is complex and deals with different devices and protocols. The testbed developed by the university is mostly lacking real-world practice from the industry. To educate students and practitioners, the testbed must be set up and equipped with incorporated components and a realistic environment to carry out the multi-domain holistic experiment. The summary of gap analysis for the existing CPES laboratory and/or testbed is shown in Table 2.

Table 2 Gap analysis for existing CPES laboratory/testbed

Aspect	Gap analysis
Purpose	Limited only single domain analysis either power system or communication network
Fidelity	Pure simulation testbed Lack of intensive knowledge of ICS component, physical process and practical realization
Accessibility	Only physical access Lack of interface platform support
Flexibility	Inflexibility to choose between simulation and physical processes Unable to configure the real component due to the proprietary protocol Lack of ability to integrate different simulators
Scalability	Lack of ability to scale up the experiment due to the limited resources
User-friendliness	Several programming tools Lack of GUI
Cost-effective	High investment cost for real/physical device and components
Repeatability	Low granularities of testbed architecture design for repeatability and reliability Uncertainty of the measurement Unrepeatable because of proprietary real-life industrial process
Standard and protocol	Lack of support for various hardware and communication protocols Require a novel ICS testbed that combined new and old protocols Absence of IoT gateway and real devices

Aspect	Gap analysis
Knowledge	Lack of cross-disciplinary background, only have computer engineering or electrical engineering

From the cyber-events the world has experienced thus far, the technical capabilities of threat actors have evolved significantly. Hence, the critical infrastructures in the smart grid must be able to detect and recover from a cyber-attack. Table 3 identifies cybersecurity gaps in the CPES according to the CPES application.

Table 3 Cybersecurity Risks in the CPES

Area/Application	Cybersecurity Risk
Boundary Protection	- Undetected unauthorized activity in critical systems - Weaker boundaries between ICS and enterprise networks.
Allocation of Resources	- No backup or alternate personnel to fill a position if the primary is unable to work - Loss of critical knowledge of control systems
Account Management	- Compromised unsecured password communications - Password compromise could allow trusted unauthorized access to systems
Identification and Authentication	- Lack of accountability and traceability for user actions if an account is compromised - Increased difficulty in security accounts as personnel leave the organization, especially sensitive for users with administrative access.
Physical Access Control	- Unauthorized physical access to field equipment and locations provides increased opportunity to: o Maliciously modify, delete, or copy device programs and firmware o Access the ICS network o Steal or vandalize cyber-assets - Add rogue devices to capture and retransmit network traffic
Least Functionality	- Increased vectors for malicious party access to critical systems. - Rogue internal access established

5. State of the art in education in smart grids and cyber security

5.1 Higher education study programs

A total of 84 universities offering security-related Information Technology study programs were examined. From the list, 14 out of 84 universities do not fit into the general criteria. Specific study program criteria with cyber security; however, Information Technology, Computer Science, or Computer Systems study programs do not provide deep knowledge for the cyber security. The technical evolution in the cyber security education is accelerating but, in general, adapting the curricula in a university is slow. To bridge the gap between industry needs and educational output, in terms of the prospective researchers and engineers, is always a challenge. One of the main actions is to review the curriculum regularly to improve up-to-date e context and teaching methods.

5.2 Continuing education programs

Professional training courses exist [6] that attempt to prepare students and professionals for careers in the emerging Smart Grid cyber security domain. Various specialized certification courses allow to increase the competencies, abilities, and skills of specialists and present a specific knowledge range. A study [7] has shown that, many countries offer a higher coverage of the knowledge units. For example, when considering the strictest coverage metric, Spain, France, Germany, and Italy cover 75% of the knowledge units (KUs) with mandatory courses. However, the size of the country is not a decisive factor [7]. The availability and promotion of various professional practices can be observed, which allows to expand the knowledge and strengthen the technical specific experience required by industry in general.

5.3 Massive open online courses (MOOC)

Online courses are becoming more popular as they reach out to more people. There are available online courses related to cyber security via edX. However, the available cyber security education courses are organized based on the topic instead of used tools, making it difficult for learners to practice specific knowledge in cyber security. Massive open online course (MOOC) still has room to developits capabilities in Cyber Security and Smart Grids training, this can be done by giving practical examples which learners have opportunities to experiences in real-life laboratories i.e. real-time simulations.

6. Identification of skill gaps in cyber security in smart grids

To achieve a better understanding into the real-world situation of industry and academia, a virtual workshop were conducted by us to disseminate the results of literature review and provide a context for discussing the necessarytools and skills for cybersecurity topic in the energy domain. Table 4 shows the result of the stakeholder workshop. The suggestions gathered from the workshop show the basic knowledge about cybersecurity in different domains (e.g. communication networks, critical infrastructure), more practical experience and working with different tools for cybersecurity are necessary for the academy. It is important to mention that teaching and presenting the theory in the cybersecurity curricula is not enough for students who pursue to work in the industry in future.

Table 4 Recommendation from the stakeholder workshop [8]

Domain	Start	Continue	Do more	Less of
Academia	• Bridging between powersystem and communication infrastructure knowledge. •Designing , developing and monitoring cyber security measures and policies proactively. •Allocate more budget for research.	•Testbud. •Essential development and testing tools •Knowledge about cyber security in multi domain (e.g. critical infrastructure , communication system, power system. •Practical experience.	• Knowledgeof the component in the power system (RTU,IED,PMU). • Conduct international research in cyber security. •Professional training. •Certificates (e.g. CISM/CISSP/CISA/CEH)	•Only theory
Industrial	• Deep understanding on the different types of security threats	•Self teaching. •Understanding of multi domain (e.g. power system, communication network). •Zero trust	•Self teaching. •Knowledge on the vulnerebalities on power system and communication network. •Workable softskills. •Learn new technologies. •Knowledge of most popular SCADA platforms. •Practical use cases •Basic tools for threat analysis.	—

7. Identification of useful tools for education in cyber security in smart grid

7.1 Basic tools for active learning about cybersecurity

There are many approaches for knowledge dissemination that can be used in the fields of cyber security generally and smart grids in specific. Table 5 shows education approaches in smart grid and cyber security for building deep knowledge and understanding of the main concepts related to the field as well as the analytical skills required for further development.

Table 5 Educational Approaches in Smart Grids and Cyber Security

Approach	Purpose	Example tools
Remote and virtual laboratories	self-learning and to create a close-to-reality interaction as in the classroom	Labview, OMWeb, NI ELVIS, Labster, LabAlive
Augmented reality	interactive learning	Worklink, CoSpaces, Merge Cube
Data visualization	visualization and analytics	Tableau, Microsoft Power Bi, IBM Congos Analytics
Cloud computing	advanced algorithms and functionalities such as data mining and deep learning	Google Classroom, Microsoft Education Center, Amazon Web Services
Flipped learning	active engineering learning	Massive Open Online Courses (MOOC)
Gamification and game theory	analyzing probabilities and cybersecurity scenarios	Kahoot, Gimkit
Simulation	practicing and testing different cases	MATLAB, Simulink

7.2 Advanced tools for vulnerabilities experiments

Smart grid system is complex by incorporting power grid and communications networks. There have been several cyberattacks on smart grid systems in recent years that have caused significant consequences. The disturbances are inherently complex and can be attributed to a wide range of sources, including natural and man-made events. Table 6 shows advanced tools categorized by their functionalities for tackle and experiments vulnerabilities.

Table 6 Cybersecurity tools for smart grids

Tool	Functionality
Security platform	Unified security management to provide centralized control and actions over threats affecting an organization's infrastructure
Network monitoring	To monitor the quality of the network against any failure or disruption, thus, to ensure continuity and performance level
Vulnerability scanning	To scan different systems and software components in trial of identifying flaws and weaknesses that can be exploited
Penetration testing	To evaluate systems' security by means of exploiting found vulnerabilities

Tool	Functionality
Packet sniffers and port scanners	To monitor network traffic, identify running services and evaluate security policies
Encryption	To maintain confidentiality and consistency of information, thus protecting data from unauthorized access
Antivirus	To detect and take action against malware and other illicit software such as ransomware, works, trojan horses, etc.
Firewalls	To provide protection against attacks by preventing malicious traffic entering a certain network or smart device
Wireless security	To prevent unauthorized access to the wireless network, as well as protecting transmitted traffic by ensuring a high level of data encryption
Password management	To control accounts securely

The existing advanced tools cover mostly the technical-related issues associated with physical cyber systems. The advanced tools should be able to cope such incorrect and misidentified threats as well as slower detection and response time. This would help to educate the students to have hands-on experiences through active learning.

8. Conclusion and recommendations

Cybersecurity education has been identified as one of the strategic digital skills in the EU that needs to be straightened by providing formal and informal education (including VET, continuing education) and topics practical application (practicing) in organizations' R&D projects. Cybersecurity is represented in different education forms, such as Higher education, Continuing education, and MOOC. The main requirements to improve cyber security curricula for smart grids development are as follows:

- Education must be accessible for different EU citizen groups (including enterprises, C-level managers, adults who want to up-skill and re-skill, and new specialists).
- It is recommended to provide cyber security distance, online and blended learning opportunities to make up-skilling and re-skilling more accessible to adults.
- The education must address general cyber security grounds and industry-specific topics (as energy supply chain cyber security and tools/methods and measures for monitoring and controlling it).
- It must provide theoretical lectures and practical training, as the use of cyber security management tools and virtual laboratories, and perform simulations and experiments using digital twins and similar environments. In smart grids cyber security education, specific smart-grid-related cyber security tools, like energetic domain controllers monitoring tools, are essential.
- Education and training programs must be developed in collaboration with relevant partners (like universities and industry representatives).
- In cyber security of smart grids programs, attention should be paid to all these domains [9]: Confidentiality, Integrity, and Availability (including performance and timeliness) as well as data privacy (the combination of organization, integrity, and confidentiality) and non-repudiation (e.g., electronic contracts). So, the scope is broader than only data security since data security is only one of the security aspects (though important) while implementing the smart grids in Europe.

- Cyber security topics should be integrated as a mandatory part of energy studies programs.
- To make cyber security education more interactive and attractive to students, it is recommended to integrate gamification elements, like, threat games, cyber ranges, and cyber security escape rooms.
- Real-time simulation infrastructures and hands-on scenarios should be provided to the students as well as the availability of basic and advanced tools for active learning.
- In the context of relevant higher cyber security education, student mobility should be considered as part of programs

9. Bibliography

[1] The European Commission, The Revised Digital Education Action Plan. The European Commission, 2020.

[2] The European Parliament, “Cybersecurity act,” 2019.

[3] The European Commission, The EU cybersecurity certification framework.

[4] J. T. F. on Cybersecurity Education, Curriculum Guidelines for Post- Secondary Degree Programs in Cybersecurity. Association for Computing Machinery, 2017.

[5] Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) https://tcipg.org/.

[6] T. Yardley, S. Uludag, K. Nahrstedt, and P. Sauer, “Developing a smartgrid cybersecurity education platform and a preliminary assessment of its first application,” in 2014 IEEE Frontiers in Education Conference (FIE) Proceedings, 2014.

[7] N. Dragoni, A. Lluch Lafuente, F. Massacci and A. Schlichtkrull, "Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs [Education]," in IEEE Security & Privacy, vol. 19, no. 1, pp. 81-88, Jan.-Feb. 2021, doi: 10.1109/MSEC.2020.3037446

[8] B. Siemers et al., "Modern Trends and Skill Gaps of Cyber Security in Smart Grid: Invited Paper," IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, 2021, pp. 565-570, doi: 10.1109/EUROCON52738.2021.9535632.

[9] The European Commission, European Commission Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids. European Commission, 2019.