State of the Art, Trends and Skill-gaps in Cybersecurity in Smart Grids

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 figures

List of Tables

Abbreviations

ACM	Association for Computing Machinery
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMI	advance metering infrastructure
BMI	German Federal Ministry of the Interior
NICE	National Initiative for Cybersecurity Education
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAE-CD	Centers of Academic Excellence – Cyber Defense
CC-RSG	Cybersecurity Curricula Recommendations for Smart Grids
CIA	Confidentiality, Integrity, and Availability
CPES	Cyber Physical Energy System
CPS	Cyber Physical System
DCSO	Deutsche Cyber- Sicherheitsorganisatio
DdoS	Distributed Denial of Service
DMZ	Demilitarized Zones
DoS	Denial of Service
ENISA	European Network and Information Security Agency
EU	European Union
EV	Electric Vehicle
FTP	File Transfer Protocol
GIAC	Global Information Assurance Certification
GICSP	Global Industrial Cyber Security Professional Certification
GOOSE	Generic Object Oriented Substation Events (GOOSE)
HAN	Home Area Network
HPC	Hardware performance counters
ICS	Industrial Control Systems
ICT	Information and Communications technology
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
KRITIS	Critical Infrastructure
KUs	Knowledge Units
ML	Machine Learning
MMS	Manufacturing Message Specification
MOOC	Massive online open courses
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIS	Network and information systems
NIST	National Institute of Standards and Technology
OT	Operational Technology
PV	Photovoltaic
R&D	Internet of Things
RTU	Remote Terminal Unit

SCADA	Supervisory control and data acquisition
SMEs	Small and medium-sized enterprises
SMV	Sampled Measured Values
TCIPG	Trustworthy Cyber Infrastructure for the Power Grid
TCP	Transmission Control Protocol
VET	Vocational education and training
WP	Work Pacakge

Executive summary

This document represents part of the project “Cybersecurity Curricula Recommendations for Smart Grids” work package 1 (WP) outcomes. The document aims to define the state of the art of education offering in smart grids cybersecurity. To explorethe state of the art of education in cybersecurity of smart grids, the following research methods were used: (1) systematic literature review; (2) analyze the cyber security curricula offered by universities and private education institutions. In the EU, there is a significant and persistent digital skills gap. The current education offer of specialized education programs does not addressall needs (especially for adults who want to re-skill or up-skill and new specialists). 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, as Higher education, Continuing education, MOOC. However, smart grid security topics are addressed relatively rarely.

Education must be accessible for different EU citizens groups (including enterprises, C-level managers, adults who want to up-skill and re-skill, and new specialists). It is recommended to provide cybersecurity distance, online and blended learning opportunities to make up-skilling and re-skilling more accessible to adults. The education must address general cybersecurity grounds and industry- specific topics (as energy supply chain cybersecurity and tools/methods and measures on monitoring and controlling it). The curricula must provide theoretical lectures and practical (i.e. hands-on) training, as the use of cybersecurity management tools (as SIEM, etc.) and virtual laboratories, perform simulations and experiments using digital twins and similar environments.

In smart grids cyber-security education, specific smart-grid-related cybersecurity tools, like energetic domain controllers monitoring tools, are essential. The need for real-time simulation capability and multi-domains are becoming essential to mimic “What if” scenarios to investigate security domain. To educate students and practitioners, the real-time laboratory must be set up and equipped with incorporated components and a realistic environment to carry out the multi-domain holistic experiment.

Cybersecurity topics should be integrated as a mandatory part of energy studies programs to enhance more interactive and attractive to students, it is recommended to integrate gamification elements, like, threat games, cyber ranges, and cybersecurity escape rooms.

1. Introduction

Cybersecurity is defined as one of EU strategic digital capabilities [1]; securing an IT environment is essential [2]. The EU has recently launched the EU Cyber- security strategy to bolster 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 [3]. The strategy covers the security of essential services, including energy grids and the ever-increasing number of connected objects in citizens homes, citizens' 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.

The IEEE European Public Policy Committee recommends that EU should [4]: 1. Strengthen cyber resilience and response to cyber-attacks; 2. Rationalise the European cybersecurity regime into a common framework; 3. Support the development of effective cybersecurity certification schemes; 4. Facilitate regulatory compliance by stakeholders; 5. Promote cybersecurity education, aware- ness, and 'hygiene' habits; 6. Support research and innovation in cybersecurity. Nowadays, technology innovations (as IoT, 5G networks, AI) contribute to new products and services development and raise new cybersecurity threats. In recent years, the energy sector has significantly expanded its digital maturity level by integrating various digital computing, communications, and industrial control systems and technologies into a modernized and advanced power grid. In addition, Europe is aiming for fully integrated internal energy market. EU strategic plans are to raise it more 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 computer networking, software, integrated systems, critical infrastructure security and security management as well as indicates the significant need for energy-specific cybersecurity skills. European Commission emphasizes the importance of raising awareness on (data) security of all the stakeholders involved in Smart Grids design and operation. European Commission states that education training is fundamental to counteract cybersecurity threats on the smart grids.

This document represents part of the project "Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)" WP1 outcomes. This work activity aims to define the state of the art of trends and education offering in smart grids cybersecurity. This document's research results will be used to identify current skill gaps in education programs that will provide grounds for a smart grids cybersecurity body of knowledge.

2. Objectives

The purpose of the “Cybersecurity Curricula Recommendations for Smart Grids” (CC-RSG) is to develop higher education to educate cybersecurity professionals for the field of smart grids. This purpose in the scope of this report is further analyzed in the following objectives:

- 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 needsbased on the above analysis

The identified skill gaps will be used by future reports in order to provide an educational strategy for Universities, VETs and employers and recommendations to relevant stakeholders (educational organizations, industry, policymakers).

The document is structured in accordance with the above objectives as follows:

- Section 3 presents the research methodology that been used in this study for collecting data and analyzing the result including the scope of thestudy.
- Section 4 illustrates the EU policy regarding cybersecurity in the smartgrid.
- Section 5 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 6 presents a summary of existing education programs in cybersecurity, including higher education, continuing education, and MOOC.
- Section 7 identifies with 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 8 presents useful tools for education in cybersecurity that is analyzed from the literature review and stakeholder survey.
- Section 9 is dedicated to the conclusion and initial requirements and recommendations regarding cybersecurity for smart grids education.

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

The research methodology of the WP 1 is shown in Figure 1. The research method starts with the desk-research literature review, the preliminary result from the literature review is presented and discussed in the stakeholder work-shop. The insightful information from the stakeholder workshop together with the desk research is used to develop the survey for specific gap analysis and further qualitative feedback.

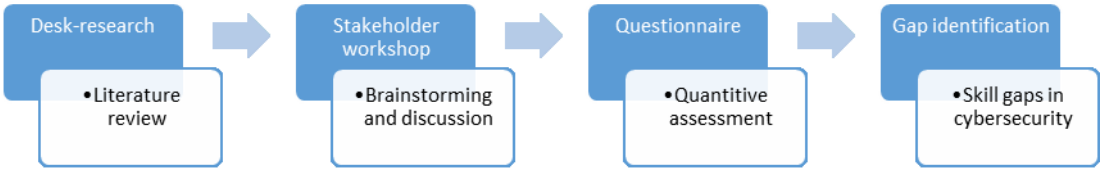

Figure 1 Research methodology of WP1

The literature review was conducted using Google scholar as a pool of sources. This choice was partly based on the article which found that Google scholar has broader search results that contain popular and reliable sources to a high degree. The keywords search terms are cybersecurity education, smart grids cybersecurity education, smart grids security. These selected keywords can gather the relevant literature that contains in their body including in thetitle pointing to education in the smart grid. There are approximately three hundred results by using the mentioned keywords shown in research articles, conference papers and theses. As a result, the literature from the years 2017 – 2020 is selected for a deep review of the latest development in smart grids.

In order to extract more information from the huge amount of the literature, the key research questions are used to analyze and categorize the state-of-the- art of cybersecurity research and development domain, teaching and learning method used during the classes and training including the level of education provided. The main research questions are:

- Q1 – What are EU strategic directions, requirements, and learning needstowards cybersecurity education?
- Q2 – How does the research overcome cyberattack prevention?
- Q3 – What are the state-of-the-art of tools and focused countermeasuresfor cyber-security research?
- Q4 – What are the technical and non-technical limitations for the researchand education in cybersecurity?
- Q5 – What is the current cybersecurity education offering (with a focuson smart grids cybersecurity)?
- Q6 – What have identified gaps in cybersecurity education and improvement areas?

In order to explore deeper the state of the art of education in cybersecurity of smart grids, the systematic literature review is used to identify key gaps from the primary sources:

- Universities and private education institutions study offering analysis;
- EU level political planning documents, regulations, and methodical materials (as ENISA recommendations, etc.) – published in institutions portals and web-pages;
- Industry associations requirements and recommendations – published in industry portals and web pages;
- Scientific articles regarding education in cybersecurity – published in scientific papers databases (IEEE digital library, etc.).

In the end, the different literature is categorized based on the security do- mains of the ACM Cybersecurity Curricular Framework and Cybersecurity curricula guidance [3], see Appendix 1:

- Data Security: focuses on the protection of data at rest, during processing, and in transit
- Software Security: focuses on the development of software with security and potential
- Component Security: focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems
- Connection Security: focuses on the security of the connections between components including both physical and logical connections
- System Security: focuses on the security aspects of systems that are com- posed of components and connections, and use software
- Human Security focuses on protecting individuals' data and privacy in the context of organizations (i.e., as employees) and personal life, in addition to the study of human behavior as it relates to cybersecurity
- Organizational Security focuses on protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission
- Societal Security focuses on aspects of cybersecurity that broadly impact society as a whole for better or for worse

4. Cybersecurity Policy in European Union

Cybersecurity has raised the cyber-threat concern to all critical infrastructure around the globe for example energy, transport, banking, financial, healthcare, residential sector, industrial sector. Cybersecurity policy can help the nation to address the essential aspects that are needed to be tackle to prevent the negative impacts caused by cyber vulnerabilities. The following section presentsthe cybersecurity policy in European Union (EU) including the recommendations from the industry and scientific research on essential education related to cybersecurity.

4.1 EU Policies and Strategic Directions

European Commission has conducted several types of research about EU digital capabilities where cybersecurity awareness, skills and competencies straightening has been identified as one of EU digital transformation strategic enablers. This section presents an overview of EU-level policies, strategic planning documentation and recommendations, addresses cybersecurity education to understand education requirements better, and acknowledges already defined plans and priorities.

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 secure digital system transformation against cyber threats. There are four pillars of the strategy for the implementation over the next five years as shown in Figure 2 which are 1) a future-proof security environment, 2) tacking evolving threats, 3) protecting Europeans from terror- ism and organized crime and 4) a strong European security ecosystem. These four pillars can help the EU member states to pave the way for digital system transformation and operation.

Figure 2 The four pillars of the strategy [3]

The EU Cybersecurity strategy [3] underlines the importance of energy grids cybersecurity, as it is part of essential services. Energy technologies embedding digital components and the associated supply chains security are crucial for the continuity of essential services and the strategic control of critical energy infrastructure (Cybersecurity strategy). 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 short- age of cybersecurity skills in the workforce. The EU lacks collective situational awareness of cyber threats. The strategy states that different types and forms of education (including vocational

education, understanding, and exercises) should focus and/on integrate cybersecurity topics to further increase cybersecurity and cyber defense skills at the EU level.

EU Revised Digital Education Action Plan [5] aims to raise cybersecurity awareness among individuals, especially children and young people, and organizations, especially SMEs. The plan has two priorities [5]: fostering a high- performing digital education ecosystem and enhancing digital skills and competencies for the digital transformation. The plan emphasizes the importance of education available for adults up-skilling and re-skilling, which can be achieved by education offering in online or a blended mode, at a time, place, and pace suited to the individual learner's needs.

Digital Europe program [1] defines cybersecurity as EU strategic digital capability. The program is focused on building the strategic digital capacities of the EU and on facilitating the broad deployment of digital technologies. The program aims to reinforce advanced skills and capabilities in EU member states for a uniformly high-security network and information systems level. The program has identified such primary cybersecurity digital skills strengthening actions: new master programs (co-created together with EU cybersecurity excellence centers), short-term specialized training courses for job seekers and employed people, especially SMEs and jobs placements. Similarly, as the EU Revised Digital Education Action Plan, the Digital Europe program stress the need not only for new higher education programs in cybersecurity but also for accessible continuing education courses for adults.

To define strategic priorities in digital skills straightening European Com- mission has researched academic offers and demand for advanced profiles in the EU: Artificial Intelligence, High-Performance Computing, and Cybersecurity [6]. Research finds that there is scope for increasing the EU-based master's programs in cybersecurity, and other education forms offering must be analyzed to understand issues and gaps.

European Parliamentary Research Service in their Briefing [7] indicates that the energy system has a number of particularities that necessitate a specialised sectoral approach to cybersecurity, above and beyond cybersecurity standards and measures applied to information technology systems:

- Real-time requirements: In an electricity grid, supply and demand must be balanced at any moment, meaning industrial control systems must react within fractions of a second, which leaves no time for sophisticated authentication procedures.
- Mix of advanced and legacy technologies: Energy system components have a very long lifespan, of several decades. It is consequently very likely that the grid will be controlled by a mix of advanced technologies with cybersecurity certification, and older devices which need to be protected in other ways.
- Cascading effects of disruption: Due to the interconnected nature of an electricity system, a serious disruption in one part of the grid can also spread to interconnected grids, potentially leading to a blackout over a wide area. This would also affect other services that depend on electricity, notably transport, telecommunications, water supply and finance.

European Commission Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids emphasizes the importance of raising awareness on (data) security of all the stakeholders involved in designing, manufacturing, system integration, and operating and using the European Smart Grids [8]. The report authors conclude that [8]: "cyber security in European Smart Grids requires well-trained proactive decision-taking operators of collaborating Smart Grid stakeholders to operate the next-generation Smart Grid infrastructure. Relevant stakeholders should generate the necessary expertise to design, build and maintain secure smart grid systems. To meet the increasing demand for ICT experts and ICT security experts with operational knowledge in electricity has become challenging and might require

updating engineering and ICT education curricula". The working group suggests educating and training stakeholders throughout the life cycle of new security solutions for Smart Grids. It states that education and training pro- grams 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. The document suggests to the curriculum should consist of four products (Figure 3).

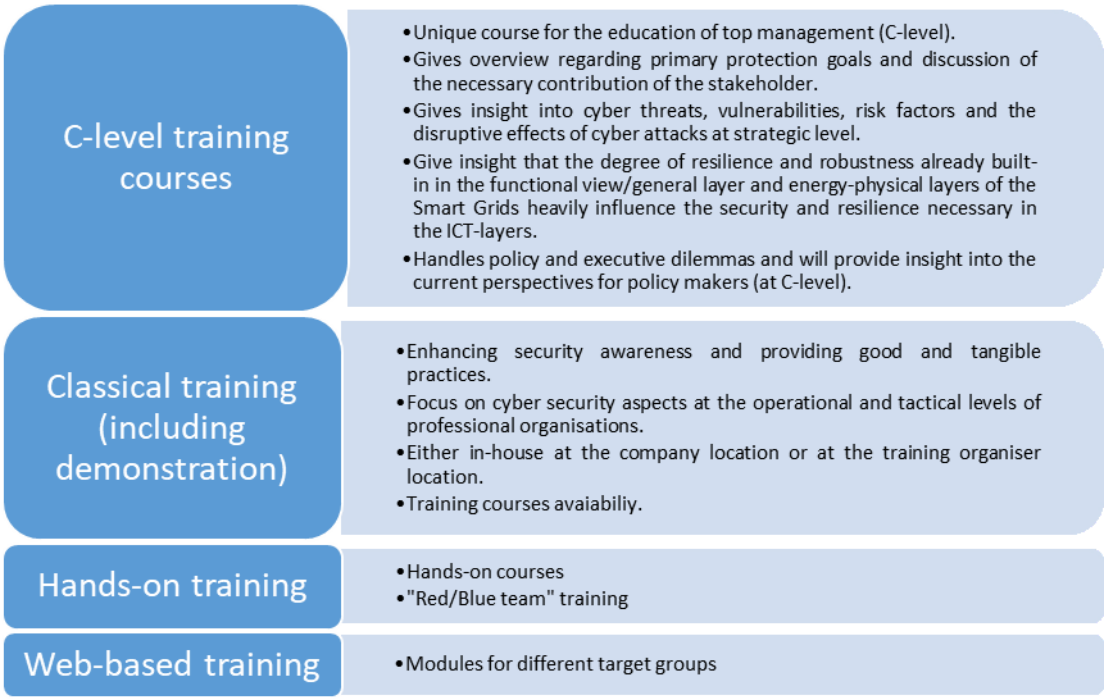

Figure 3. European Commission Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids curriculum recommendations

Cybersecurity is an important issue for the majority of energy companies, and a shortage of staff with specialized skills in cybersecurity is an obstacle to the successful implementation of cybersecurity technologies and procedures.

4.2 Organization related to cybersecurity

The EU Agency for cybersecurity (ENISA) is responsible for cybersecurity in the EU under the Cybersecurity Act [9]. 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 mandatedto provide supports to EU member states for cybersecurity implementationby setting up the European cybersecurity certification [10]. Businesses in the EU must comply with the specific requirement of their products and services according to the NIS directive.

National Institute of Standards and Technology (NIST) is a non-regulatory agency of the United States Department of Commerce. It is responsible for the activities related to in-formation technology and other aspects such as neutron research, material measurement, engineering, nanoscale science and technology. NIST has developed cybersecurity standards and best practices to meet the need in the U.S. context including the public and private sector. NIST also pro- vides a “Guide to Industrial Control Systems (ICS) Security” which outlines the threats to ICS and defense strategy [11]. In addition, NIST also provides work- force education and training which collaborate between government, academia and private sector to stimulate the ecosystem and workforce in this field. The National Electric Sector Cybersecurity Organization Resource (NESCOR) is an- other organization in the U.S that deals with cybersecurity especially in the electric sector. The NESCOR serves as the focal point for a public-private partnership to enhance cybersecurity in the electric domain.

International Electrotechnical Commission (IEC) is an organization for the international standards related to all electrical and electronics technologies. With the emergence of IT/OT convergence in the digitalized energy sector, cyber-threats also arise. The IEC standards such as ISO/IEC 27001 and IEC 62443 deal with testing and certification for holistic cybersecurity evaluation to ensure secure assets and their efficient performances.

For example, in Germany, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) was established in 2009. The BSI has played an important role in IT security on a national level through prevention, detection, testing and defense for the government, business and society [12]. In addition, the BSI also offers services to the private sectors such as IT manufacturers and commercial users. Currently, the BSI acts as the central cybersecurity authority in Germany. The public-private cybersecurity cooperation can be seen in Germany such as UP KRITIS which was founded in 2007 to secure the critical infrastructure in the country. Another form of public- private cooperation is the information exchange of vulnerabilities, defense plan, specific. The German Cybersecurity Organization (DCSO) was established by large companies which exchange information with BSI and the German Federal Ministry of the Interior (BMI). The cooperation between organizations in Germany can be seen between governmental agencies, public and private, government and industry and/or business [13].

4.3 Industry Studies and Recommendations

The importance of energy sector cybersecurity and related education offering availability has been highlighted both in energy and ICT sectors. Industry associations and interest groups have studied the art of existing cybersecurity education and prepared recommendations for cybersecurity curricula. However, suggestions about smart grids cybersecurity education are addressed limited. This section presents an overview of industry studies, what addresses cybersecurity education to explore industry requirements and recommendations.

Joint Task Force on Cybersecurity Education consists of several associations that have prepared Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity [14]. The Joint Task Force shares opinion that the world faces a current and growing workforce shortage of qualified cybersecurity professionals and practitioners and proposes cybersecurity education programs. The 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 author emphasizes that cyber- security is an interdisciplinary course of study, including law, policy, human factors, ethics, risk management, and computing. The proposed thought model consists of 8 knowledge areas (data, software, component, connection, system, human, organization, societal) and eight cross-cutting concepts (confidentiality, integrity, availability, risk, negative thinking, and systems thinking) (Figure 4).

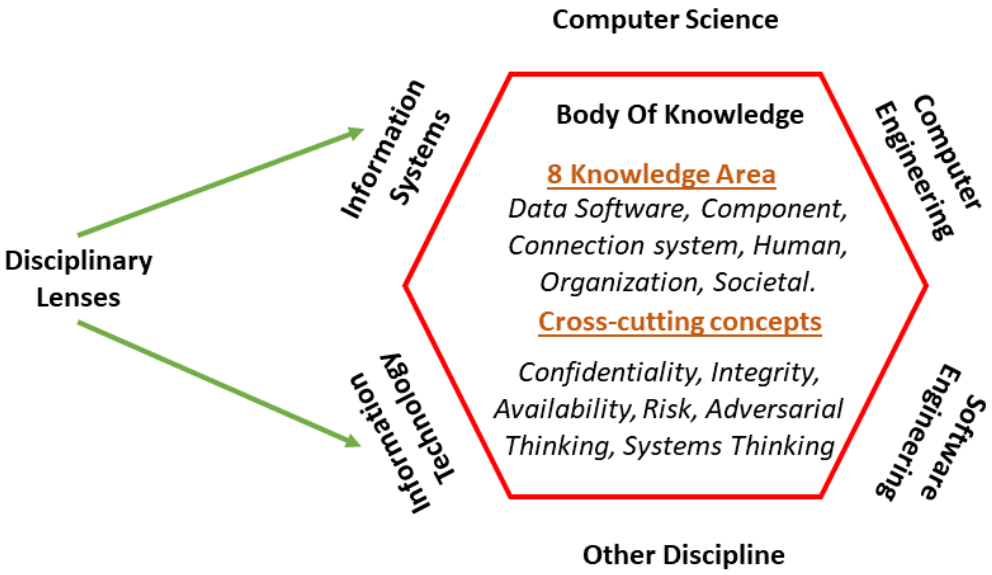

Figure 4 Cybersecurity education curriculum thought model [14]

Association for Computing Machinery Committee for Computing Education in Community Colleges has prepared Cybersecurity Curricular Guidance for Associate-Degree Programs [15]. The guidelines are based on Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity [14] and are adopted for two years programs. The policies focus on learning outcomes that are aligned to the NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [16] and Centers of Academic Excellence – Cyber Defense (CAE-CD) Two-Year Knowledge Units [17].

The framework serves as a reference model for describing and sharing in- formation about cybersecurity work and needed knowledge, skills, and abilities. It is designed for cybersecurity workforce development, education, and training purposes. The framework covers different audience needs, including educators who can use the framework to develop curriculum, certificate or degree pro- grams, training programs, courses, seminars, and exercises.

4.4 Scientific Research

Cybersecurity and smart grids cybersecurity education opportunities are quite rarely explored in scientific research; still, some research exists [18, 19]. Studies mainly focus on online education platforms development.

The energy sector recently has embarked on a digital transformational process introducing smart grids that triggers the need to re-educate the aging work- force and train the emerging workforce. To address training needs Yardley et al. proposes a modular, hands-on, and open Smart Grid cybersecurity educational training platform and supporting materials - TCIPG: Trustworthy Cyber Infrastructure for the Power Grid [18]. The research indicates that existing education offering not fully cover Smart Power Security Professional (SPSP) requirements, and they are monolithic what doesn't promote effective learning. Therefore, the authors present an education platform that is based on pillars of pedagogy of active learning, project-based learning, Piaget's learn by doing posture, and constructivism approaches. The main proposed learning topics are [20]:

- 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 (12) Robust control systems

Cybersecurity in smart grid systems as an engineering education tool has been investigated in [19]. The purpose of the study was to attract undergraduate students to cybersecurity by immersing them in a research experience that targets Smart Grid security. The lesson simulates cyberattacks to Smart grid systems and uses simulation for education purposes.

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

The Third Industrial Revolution that began in the middle of the twentieth century created the infrastructure to produce and store the digital tools to edit and share various formats of information (music, photos, news, social media, etc.). Klaus Schwab first used the

term “Fourth industrial revolution” in 2015 [21] to describe the revolution that follows the Third revolution and capitalizes on these tools and infrastructure creating cyber-physical systems (CPS) that continue being integrated into larger ones. The CPSs ensure the reliable operation of the electricity generation system, help the operators take important decisions and monitor the generators for abnormal behavior (due to human error, physical disasters, or cyber-attacks). In the distribution system, a large grid of sensors providing real-time data enables us to optimize the energy market operation, to make room in the existing grid for the electric vehicle (EVs from now on) charging stations and better plan the use of renewable that are weather-sensitive like photovoltaics and wind turbines. In homes, central units can plan the use of various devices for economic optimization and inform the customer about his/her current energy consumption profile.

The Fourth Revolution in power systems creates what is now widely known as a Smart Grid with the above characteristics. These characteristics require knowledge that is in the overlap between the power systems and the information and communications technology (ICT from now on). This broad use of data that can reveal personal information about the customer (energy consumption habits, bank information, etc.) and important information about a country’s critical infrastructure combined with the multiple points of access creates a need for protection from cyber-threats i.e., cyber-security. Traditional education has not yet caught up with the required changes it needs to make to create people adequately equipped to be employed in the cybersecurity of Smart Grids.

This section presents the state-of-the-art of cybersecurity in the smart grid to address the cyber vulnerabilities and countermeasures used. The past cyber- attack events can address the essential skill and training tools and/or laboratory needed to prepare the workforce for cybersecurity in the future.

5.1 Categorization

The search engines such as 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 cyber security framework of ACM as shown in Figure 5. Each selected study is reviewed in detail to identify the purpose, method, and result of the study. The higher number, the more studies focused on the area. However, one study can cover more than one aspect.

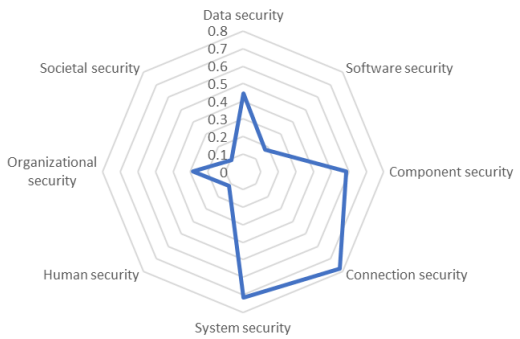

Figure 5 Categorization of skill gaps based on the literature review

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 CPES laboratories for the experiment and/or teaching students.

At the early stage of the emerging ICT in the energy sector, interoperability is considered a crucial technical concern on how to integrate it into the existing system. Most of the studies mainly focus on the new connection protocol especially proprietary ones which can cause vulnerabilities to the system. As a result, the focused security aspects on human, organization, and societal security are very low. An example of the smart meter deployment can indicate very well how policymakers overlook integrating the non-technical dimension at the early stage of the deployment. The non-technical factors are awareness, perception and understanding for example afraid of electromagnetic radiation, over-expectation on its benefit, privacy concerns. These non-technical factors may lead to the objection of smart grid technology deployment on the large scale. Both technical and non-technical aspects should be considered at the early stage of the deployment to prevent the opposition of the new technologies adoption. This can also be done by providing the information and facts of the technologies as well as raising awareness of its security and vulnerability.

5.2 Technology and Education Development

5.2.1 Cyber Security Threat in Smart Grid

The increasing IT/OT convergence has driven smart grid technology adoption. Integrating information and communication technology (ICT) into the existing system has two-fold effects; automatic control and operation, and vulnerabilities from cyberattacks. In the past, the testbeds were developed in the military domain which was only referred as to a national concern; currently, cybersecurity has been integrated into all sectors. The well-known cyber at- tack event in Ukraine in 2015 has driven more concern to the system operator in the energy sector. Cyber-Physical Energy System (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. The smart grid system is one of the key infrastructures and complex. It comprises two independent parts: power grids and communication networks as shown in Figure 6.

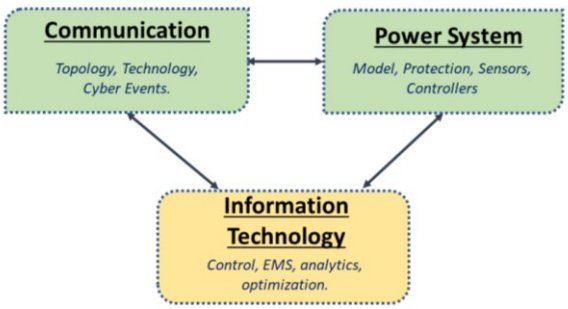

Figure 6 System Architecture in Compliance with IEEE 2030 [22]

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. Cyberattacks involve networked devices whose software becomes infected with malware. In recent years, there have been numerous cyberattacks against smart grid systems. A number of different malware types that are capable of infecting hosts exist. For example, in 2007, the Iranian nuclear power station attack slowed down the country's vital nuclear power development by using the Stuxnet virus. Also, in 2014, a hacker team called Dragonfly had attacked more than 1,000 energy companies in North America and Europe mainly through malware in emails, websites, and third-party programs. Table 1 shows the important cyberattacks in the energy sector.

Table 1 Cyber attacks events in energy sector

Event	Year	Method
Stuxnet - The Iranian nuclear power station	2007	An authoritative and structured virus
Energy firms in North America and Europe	2014	Emails, websites, and third-party programs
Electrical power station in Ivano-Frankivsk-Ukraine	2015	Spear-phishing and a 'BlackEnergy' Trojan horse to delete data, destroy hard disks, and control infected computers. Also, DoS attack on the phone numbers of companies running the power station.
The U.S., Saudi Arabia and South Korea (energy and petrochemicals)	2017	APT33 delivers its malware through targeted spear-phishing emails sent to employees.
Ukraine power system and the critical infrastructure in the U.S.	2017-2018	NotPetya - a malicious, permanent encryption;
Schneider Electric's Triconex safety instrumented system	2017	TRITON/Trisis/HatMan- by modifying in-memory firmware to add malicious functionality allowing an attacker to read/modify memory contents and execute custom code on demand by receiving specially crafted network packets from the attackers

In this regard, malware can spread either actively in the form of worms orin botnets, or passively in the form of viruses. Furthermore, they can utilize functional malware such as Trojan horses, spyware, adware, spammers, sniffers, crypto lockers, backdoors, logic bombs, and more in modular extensions. Al- though these malware types behave vastly differently, they all at some point utilize a payload that exploits a vulnerability to change

the host's behavior. Attackers may use any of a variety of infection vectors, e.g., software exploits, compromised removable drives, or manipulated emails.

Manipulation, sabotage and espionage are the three leading causes of smart grid attacks. These cyber-attacks can be happened consciously or unconsciously and influence confidentiality, integrity, and availability (CIA) which are the key elements of cybersecurity. Availability is the most important factor and must be ensured since smart grids must provide efficient use of electrical infrastructure. Integrity is considered as the second priority while confidentiality is third. Thecyberattack classification considering the CIA aspect is present in Table 2.

Table 2 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

In so-called man-in-the-middle attacks is one of the confidentiality attacks. The attacker is able to relay all the communication exchanged between some two devices. While the messages captured by the attacker can be altered, the communicating devices are convinced they communicate directly [22, 23, 24, 25,26]. Stuxnet is another example of confidentiality attacks which is a complex malware designed to change values of data sent and received by PLCs. The Stuxnet was exploited to the Iranian nuclear facility by an unaware insider orby a third-party contractor. The hackers are able to maintain connections within those networks and take control over remotely accessible devices by spreading malware within operators' networks [23, 27]. The attackers can also use the side-channel attack to compromise a system by analyzing the required time to execute cryptographic algorithms or escalate privilege such as scanning Metasploitable machine using nmap from Kali Linux, identifying an open TCP port, escalating privilege from daemon to root using the local privilege escalation exploit via netcat. Moreover, the attacker can also deploy AES cache-timing attack whichmay leak timing information during cache hits/misses. The cache-based timing attack is about reconstructing the key by observing the data flow of different cache levels [28].

The integrity attack aims to compromise the message. False data injection attack (FDIA) aims to hack the readings of multiple sensors and phasor measurement units (PMUs) to mislead the smart grid's decision-making process. Recent studies have shown that although the attackers are lack of knowledge on the power grid topology and transmission-line admittance values, they can adjust the false data injection attack vector. As a result, the attack remains un- detected and successfully passes the false data detection that is commonly usedin power system state estimation [29, 30, 31, 32, 33, 34]. A phishing

campaignis an email scam designed to steal personal information from victims. Cyber-criminals use phishing emails to obtain sensitive information such as credit card details and login credentials of a trustworthy organization or reputable personin an email communication [35].

A good example of an availability attack is the denial of service (DOS). A denial of service attack (DoS) aims to interrupt or take the communication system down. Please give the boundary/difference between Dos and DDoS. The distributed DoS (DDoS) attack is one of the device-based attacks that target interrupting the service availability for example advance metering infrastructure (AMI). The DDoS attack could cause a significant financial loss to the utility due to the large-scale blackout. The main objective of the attacker is to crushing the processing power and data bandwidth of the victims and then jamming its communication channel [24, 36, 22, 29, 31, 37].

5.2.2 Countermeasures

There is no standard 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.

The IDS is used to detect malicious activity before the real attack on the network. The IDS can be classified into three broad categories: signature-based, specification-based and anomaly-based. A signature-based IDS recognizes intrusions using a blacklist of known at-tack patterns. Whereas a specification-based IDS detects attacks using a set of constraints (rules) defining the correct operation of a program or protocol. An anomaly-based IDS recognizes deviations from what is considered by building a model of normal system behavior where any deviation from normal is identified as an intrusion [23, 27, 34, 38].

The IDS are used in several applications in the smart grid for example detection of tampered RTU for PV production, automatic controlled smart electric appliances. A trust algorithm can be integrated into the IDS to identify the state of the system. The IDS can be deployed at the RTU to check whether the data is not compromised. The DoS attack can be prevented by developing the IDSs in the network. The signature-based IDSs are not suitable for the smart grid due to lack of the detection the increasing number of new attacks which are often manifest themselves. On the other hand, specification-based and anomaly- based IDSs are a promising approach for the smart grid environment because of their dynamic capability [23].

While the IDS is used to detect the anomalies, the DMZ is used to provide the interface to an untrusted external network to secure the internal private net-work. The DMZ of operational technology (OT) aims to isolate the OT LAN from the corporate network, therefore it cannot access directly to the servers. For example, the DMZ can be deployed in the SCADA system to isolate the LAN network and prevent direct access to the SCADA server. The technical staff can access SCADA through the FTP server in the OT DMZ [24, 28]. The HPCs can also enhance cybersecurity by monitoring hardware events e.g. total instructions retired and branches are taken. The HPCs provides in- depth performance data with-out requiring source code modifications and with lower overhead than software profilers. The hardware events and the number of

available HPCs vary from one processor model to another. The interlocks man- age mutually dependent elements which can operate locally and independently from the central control room. However, for some applications, the distribution operators are concerned about its flexibility which cannot be performed locally but only in the central control room.

5.2.3 Cyber Physical Energy System (CPES) Laboratory

Up to date, universities, government and industry have set up testbeds to experiment on cybersecurity research and development. There is no standardized CPES testbed. Figure 7 shows testbed taxonomy categorized by domain which is 1) single domain testbed and 2) multi-domain testbed. The single-domain testbed only provides one domain investigation e.g. power system, network communication and cybersecurity. Multi-purposes and domains testbed has a greater advantage compared to the single purpose and/or single domain. Interconnection between domains enables practitioners to understand and have a broad overview of how different domains are connected as shown in Figure 8 . Several testbeds have been offered for several purposes e.g. education, training, services.

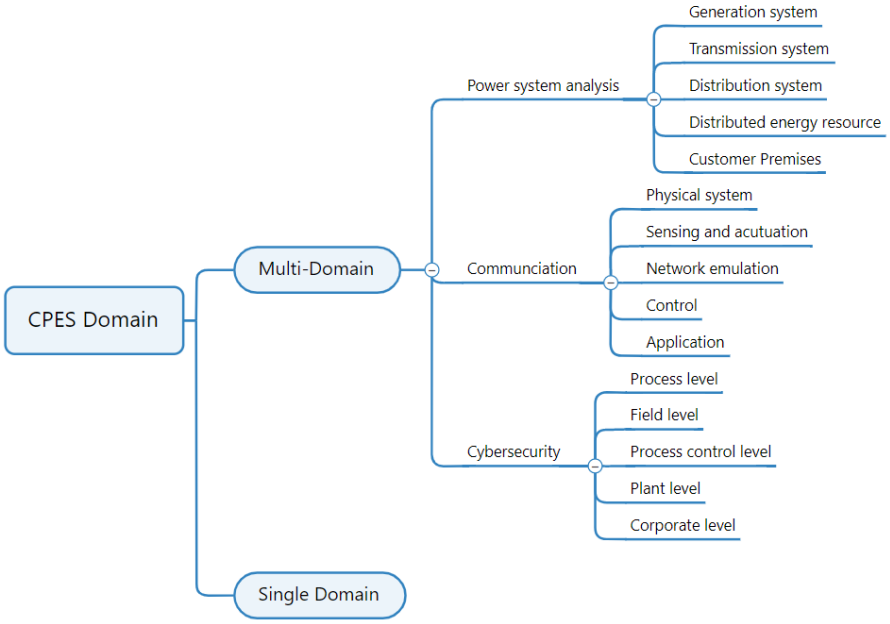

Figure 7 CPES testbed taxonomy

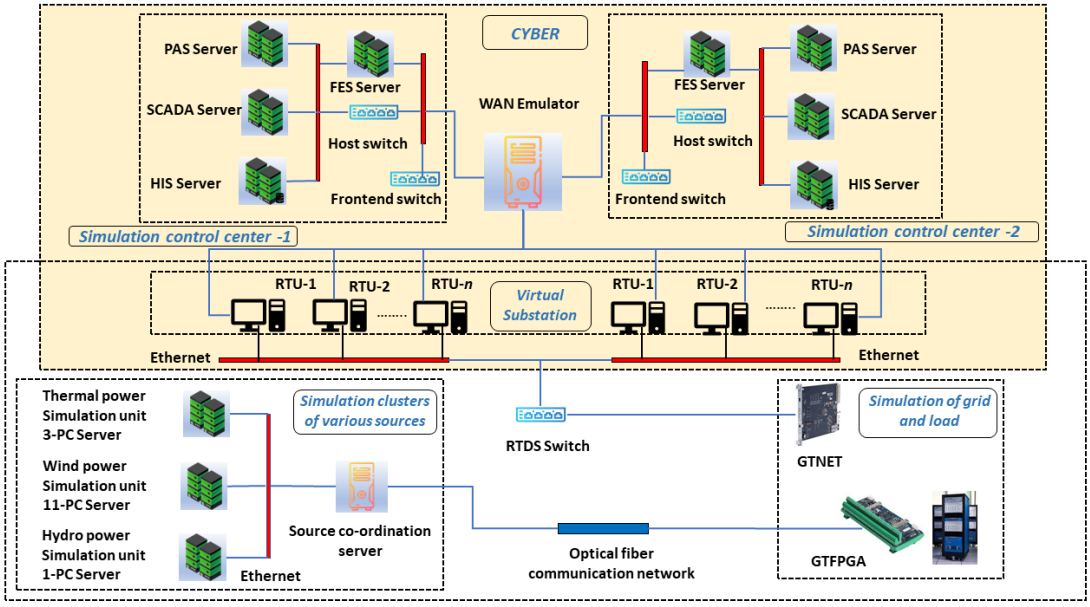

Figure 8 CPES Testbed Architecture [39]

Cyber security topics are complex and involving several knowledge back- grounds e.g. computer engineering, electrical engineering, industrial engineering. A simple and low-cost testbed allows undergraduate students to replicate and explore the fundamental principle of cyber security. For security research and development requires a more complex testbed that closes to reality to understand the interaction between cyber systems and physical systems i.e. power systems [40, 41, 34, 35, 42, 39, 43, 44, 45]. The university's testbed can also provide some of these services such as conceptual design, standard and protocol validation, and training for system operators.

Some industrial companies have their testbeds for providing services such as design, commissioning, validation, prototype, and deployment. The commercial testbed is a high-cost investment and required extensive experience to provide the services to the customers e.g. troubleshooting and in-field testing. It is essential for commercial testbeds to integrate cyber and physical components to provide to the customers as well as the security algorithm development of the products e.g. controlled testing, attack/defense experimentation [26, 46, 47, 30, 48, 49, 25]. It should be noted that some companies may not have their own testbeds for their product development. Collaboration between industry and university can accelerate state-of-the-art innovative research and product development.

5.2.4 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 a protocol that defines certain rules for communication. A communication protocol allows two or more devices to transmit information between them. The protocol defines the rules, syntax, semantics and synchronization of communication and possible recovery methods for the errors. The usage of communication protocols assures enhanced security to network communication among network nodes.

Intelligent devices (e.g. sensors, actuators) are used to collect and transmit the real-time information status of the energy network in the smart grid. The huge amount of heterogeneous information, which are collected by these intelligent devices, must be reliable and secure for optimization, management and control operations to make fast and effective decisions in the energy system. To support information collection, distribution and analysis, the smart grid communication system will rely heavily on communication infrastructure. The communication infrastructure consists of a set of communication technologies, net-works and protocols that: (i) support communication connectivity amongst devices or grid sub-systems, and (ii) enable the distribution of information and commands within the power system [50]. Furthermore, it is important to ensure secure and reliable operations of the smart grid communication system to protect the entire smart grid. However, the security solutions cannot be confined to a single component of the smart grid communication system but rather on a cross-layer because it is equally important to: (i) secure devices, information, and services, (ii) preserve data integrity, confidentiality and authenticity, and (iii) ensure very high availability of electricity provision.

There are several communication protocols that have been used in the smart grid depending on the latency, reliability, data rate, scalability and security. One of the widely-used protocols to connect the remote RTUs with a central supervisory computer is Modbus/TCP. Although Modbus is a generally accepted industrial process standard, especially popular in the oil and gas sector, it also plays an important role in power distribution. The IEC 61850 enables the interoperability between different components and functions from different manufacturers. It is mainly used for communication with IEDs in substation automation. The data model described in the IEC 61850 can be mapped to a protocol for example Manufacturing Message Specification (MMS), Generic Object Oriented Substation Events (GOOSE), and Sampled Measured Values (SMV). The MMS can also use at the higher level such as SCADA and RTU.

IEC 61850

There are several communication protocols that have been used in the smart grid depending on the latency, reliability, data rate, scalability and security. One of the widely-used protocols to connect the remote RTUs with a central supervisory computer is Modbus/TCP. Although Modbus is a generally accepted industrial process standard, especially popular in the oil and gas sector, it also plays an important role in power distribution. The IEC 61850 enables the interoperability between different components and functions from different manufacturers. It is mainly used for communication with IEDs in substation automation. The data model described in the IEC 61850 can be mapped to a protocol for example Manufacturing Message Specification (MMS), Generic Object Oriented Substation Events (GOOSE), and Sampled Measured Values (SMV). The MMS can also use at the higher level such as SCADA and RTU.

The first versions of the standard IEC61850 in parts 8 and 9 have described data exchange between logical nodes of different IEDs within the same substation, especially the use of GOOSE and SV messages. Goose is a layer-2 message used to fast communications between IEDs in the substation (e.g. send commands and receive status data); whereas SV is used by IED to collect digital measurement data from master units or optical current transformers. The additional part IEC61850-90-x is intended to extend these two types of messages to exchange data between IEDs located in different substations, i.e over Wide Area Network, and that's why they are termed as "routable" (R-GOOSE and R-SV). These are layer-3 messages (i.e. over IP) and could be mapped using either TCP or UDP. These routable inter-substations messages have two main use

cases: teleprotection schemes (e.g. line differential protection schemes) and wide area protection and control schemes (WAPAC). The part IEC61850-90-5 (published in 2012) has been developed to standardize the synchrophasor data measurements, i.e. data exchange between PMUs and PDCs. This focus only on the communications part of synchrophasor data (similar to IEEE C37.118-2 standard) and refers to IEEE C37.118-1 in regard to PMU concept and requirements. The data structure of IEC 61850 has been extended to cover the PMU measurements; the PMU itself has been considered as a MMXU logical node with additional data objects and attributes to describe all synchrophasor measurements and PMU-classes. Additional attributes have been also added to the control blocks of the normal GOOSE/SV to enable layer-3 implementations [93].

IEC 62351

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. For example, GOOSE and SV messages are modified to trip circuit breakers which can be further fabricated to the control center. 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. Figure 9 shows the security mechanism between IEC 62351 and IEC 61850.

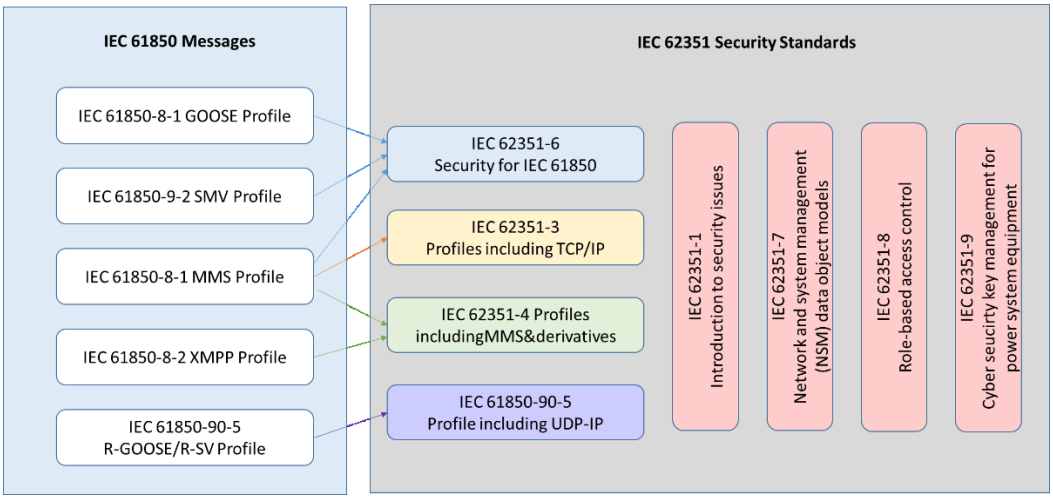

Figure 9 IEC 62351 security mechanisms corresponding to the different IEC 61850 messages [94]

For example, GOOSE and SV messages apply digital signatures (DS) generated by SHA256 and RSA public keys algorithms to strengthen security. The processing time of IED is high with limited computation capacity, therefore it poses vulnerabilities by modification of data, tampering, replay, and man-in-the-middle attacks. Every GOOSE/SV message will be extended with generated DS which is indicated by “extension” as shown in Figure 10. For R-GOOSE and R-SV messages, IEC62351-1 has defined security model and recommend encryption algorithm such as AES-128 and AES-256 [94].

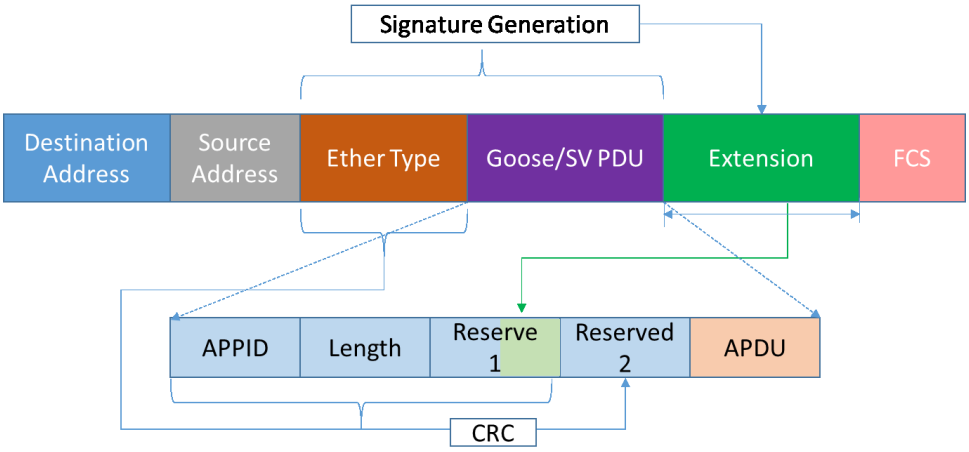

Figure 10 Extended GOOSE/SV frame format [94]

For communication with SCADA devices such as RTU, the IEC 60870-5-101 is also used. But, the security of this protocol has been proven to be problematic such as the lack of proper data encryption, remote attacker to spoof network communications, exploit input validation flaws on a vulnerable system. The HSR/PRP protocol is used for persistent communication under a single network component failure so that the PLC/SCADA can continue to access the IEDs [34, 25, 51].

Other protocol

Recent smart home device development in the market has also raised cyber- security concerns for home users. ZigBee is the most popular network protocol used in the HAN which is suitable for high-level communication protocols with a sufficient data rate for smart home network communication and less power consumption. ZigBee is also used for reliable communication between the smart meter and the home appliances ZigBee provides a sufficient data rate for smart home network communication. The experiment of protocols related to smart home devices have been investigated for cybersecurity matters in the CPES laboratory [22, 52, 53].

5.3 Gaps analysis

The power system is complex and dealing with different devices and protocols. The testbed developed by the university is mostly lacking real-world practice from the industry. Students and researchers often work with simplified assumptions and high-level scenarios. Integrating practical experiences from the industrial is recommended for setting up the testbed. Close to a real-life industrial environment testbed allows students and practitioners to replicate a real industrial process; however, the high investment cost and extensive knowledge are the main challenges. The need for real-time simulation capability and multi- domains are becoming essential because the offline simulation can perform for the simplification which cannot reflect the security domain. 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 existing CPES laboratory and/or testbed is shown in Table 3.

Table 3 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
Knowledge	Lack of cross-disciplinary background, only have computer engineering or electrical engineering

The home IoT devices can be seen and reachable in the market which can stipulate the cyber security awareness and engagement of students by using learning projects in the curricula. For example, how to connect the smart device with the hub and protect them from malicious attacks. Students can examine different test scenarios to assess the vulnerabilities of the IoT device. In addition, the IoT gateway should be included in the CPES testbed that enables the communication between ICS components internally and externally for developing intrusion detection systems and countermeasures. Few testbeds have set up the low-cost Cyber-Physical Systems (CPS) IoT with physical infrastructure such as sensors, actuators and communication devices [52, 43, 22, 54]. This can also be done by using virtual components through communication protocols. Education and research on cyber security of IoT devices has been a focus recently due to lack of policy orientation whereas the cyber attack and privacy issues were reported [52, 55].

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 able to detect and recover from a cyber-attack. Table 4 identifies cybersecurity gaps of the CPES according to the CPES application.

Table 4 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

Users often lack flexibility for configuration and examination due to thelimitation of the real device which mainly because of high investment costs. Remote access is not only a trend but it is a need to achieve holistic testing due to the limited resources, thus, sharing the infrastructure between the testbeds is the solution. Collaborating between research infrastructures can overcome this limitation through virtual and remote access which also can avoiding the interaction of the costly incident with the real system.

Regarding the inconsistency between the technical and non-technical skill areas, we will work more on the areas which are be neglected. In these domains, the role of humans is a common part of them, and neglecting that can imply a superficial knowledge of human behavior and how significant it is in cybersecurity. Since it is showed that most cyberattacks have happened from namely “disgruntled employees” or via human error like misuse of resources, it is necessary to determine this research gap. From the industry point of view, one reasonfor neglecting this area can be that preventing an attack from human errors can-not be directly linked to profit. Authors in [56] show the results from 2015 that50% of the main cyber incidents originated by human errors. In this regard, the students or

professionals must be educated about their behaviors such as managing sensitive data and credentials, maintaining backups, and checking the email reputation which affect the security of the company.

Furthermore, it is important to show the priority of security over productivity by managers. By considering cybersecurity to study human behavior, designers (e.g. of a smart meter) can make it easier for the clients of the end product to maintain data privacy. Virtual simulations can be easily integrated by these skills. The cur- rent study shows the proposed countermeasures in case of cyberattacks include keeping historical data to check for abnormalities (although they do not pre- vent zero-day attacks), using Intrusion Detection Systems and checking every command against the safety of the end state of the system (command is not executed if it sends the system in an unsafe state).

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

There are several ways to secure state of the art in smart grid and cyber security through the three elements are higher education programs, continuing education programs, and massive open online courses (MOOC). This section summarizes the main findings from the available literature, internet resources within EU and USA study programs.

6.1 Higher education study programs

A total of 84 universities offering security-related Information Technology study programs were examined. Starting with undergraduate study programs that offer Cyber Security, Ethical Hacking, Security Management, Cryptography & Data Security, and Information Assurance Track with different word combinations, it should be emphasized that all strictly adhere to a familiar concept. The concept can be compared to the set of study courses required for Cyber Security study programs. Starting with a basic knowledge of Information Technology and Computer Architecture, gradually with an in-depth understanding of data, cryptography, networks, forensics, information systems, operating systems, algorithms, and finally with computer security study courses. Also, it is observed that study courses are offered that give practical examples as professional bachelor study programs.

Providing the study course with useful security testing tools and skills for testing systems, their networks, and surrounding equipment that affect the existing infrastructure. Moving from theory and practice allows the acquisition of various competencies, skills, and knowledge. 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 go deep enough into the current topic of Cyber Security. The technical evolution in the cyber security education world are ever accelerating but, in general, adapting the curricula in a university is a rather slow process. The evolution in the industry and the research in the academic world do not always correlate well. This implies that bridging the gap between industry needs and educational output, in terms of the prospective researchers and engineers, is always a challenge. In this context, one of the main goals is the introduction of new up-to-date curricula to avoid outdated curricula and teaching contents by reviewing with graduated study programs that are predominantly.

Master's level study programs that most emphasize Cyber Security with a certain degree of knowledge, which already indicates that graduates have specific experience,

competencies, skills, and abilities to apply practically specific Cyber Security sub-topics. Examples include Privacy Engineering, which emphasizes 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 different aspects of the proceedings which come from jurisprudence. The next section presents human-based security aspects such as Computer Forensics, Information Security Management, Physical, Operations, and Personnel Security and Human Aspects of Cybersecurity. The next division is both national and SME relevant, consisting of various specific study courses. Such as Security Practices in the Enterprise, Secure Information System Governance, Regulation, and Compliance, Enterprise Security Threats, Enterprise Security Technologies, Organizations, Management, and Work: Theory and Practice and Critical Infrastructure Protection, in Theory, Policy and Practice. As already mentioned in several titles of study courses, practice is the keyword that also indicates practical skills and the practical application of these study courses. The last subdivision is the specific sub-topics, the application of which is mostly already directed to doctoral study programs. Cryptography, Cyber Defense, Information Security Risk Management, Digital Transformation, and more.

That already known higher level of study are doctoral study programs that are also based on Cyber Security. Of all the universities surveyed that are valid at the end, there are 70 in Cyber Security, of which only 1 offer doctoral studies with the following title: Cyber Security and Software Technology Doctoral Programme. As the university itself proudly acknowledges: “At De Montfort University (DMU), we are recognized as world leaders in cyber security and software technology research. We advise governments on it; we help develop the leading international standards in the field. Deliver the most prestigious cyber security and software engineering courses, publish our exciting research in world renowned journals, and organize ground-breaking international conferences in the area students into the global research community. The Cyber Security and Software Technology Doctoral Training Programme run at DMU is led by a world-class team of academics from many disciplines across all faculties, including Psychology, Law, English, and Computer Science. This unique program will meet the public and private sector’s needs and provide skilled, flexible, and knowledgeable researchers. Who will be fully able to meet the challenges associated with providing a safe, secure and prosperous environment that encompasses smart systems, critical infrastructures, as well as cyberspace.”[57].

As mentioned above study levels, it must be emphasized that the smartgrid is stressed only in one study program, which is at the Master’s level atthe University of Turku. This concludes that the higher education system hasnot yet fully implemented smart grids study courses. It drives and makes the necessary improvements that will be filled over time. The universities covered are available in Appendix 2.

6.2 Continuing education programs

Across the globe, many national institutions have embarked on a transformational process to augment the over-a-century-old power grid under an umbrella term of the Smart Grid. Worldwide Smart Grid investment rose to 15 billion euro in 2013, according to Bloomberg Energy News Finance. This vast infrastructural upgrade involves integrating various digital computing, communications, and industrial control systems and technologies into a modernized and advanced power grid. A vital constituent of the smart grid effort lies in incorporating the bidirectional flow of power (for distributed and renewable energy sources) and the two-way communications and control capabilities.

With the enhanced automation, computing, communications, and control characteristics of the Smart Grid, a crucial need becomes apparent to address the plethora of security and privacy-related challenges. The general term to refer to the dimensions mentioned above of the Smart Grid is cyber security. Cyber security becomesan indispensable component and critical enabler for success [58]. The authors emphasize the pedagogical framework, such as Active Learning, Project-based Learning, Piaget's learn-by-doing posture, and constructivism [58].

Professional training courses exist [58] that attempt to prepare students and professionals for careers in the emerging Smart Grid cyber security domain. This includes the Global Information Assurance Certification (GIAC) newly launched certification program known as the Global Industrial Cyber Security Professional Certification (GICSP) [59], which is designed to assess a specific body of knowledge thought to be representative of the necessary expertise in this sector. To accomplish training in this sector, various approaches exist, including 1) Samurai SCADA security course [60]; 2) Cybati's Critical Infrastructure and Control System Cyber security course [61]; 3) SCADA hacker's Industrial Control System Cyber Security Training course [62]; 4) SANS ICS410 ICS/SCADA Security Essentials [63], and 5) Cimation's ICS/SCADA Security courses [64]. Various specialized certification courses allow to increase the competencies, abilities, and skills of specialists and present a specific knowledge range.

However, the knowledge skills and opportunities of K12 and secondary high schools in the EU and USA should also be emphasized. The authors [65] have already started building CS and cyber security foundation in Florida K12 school systems by exposing teachers to basic CS concepts as the first step.

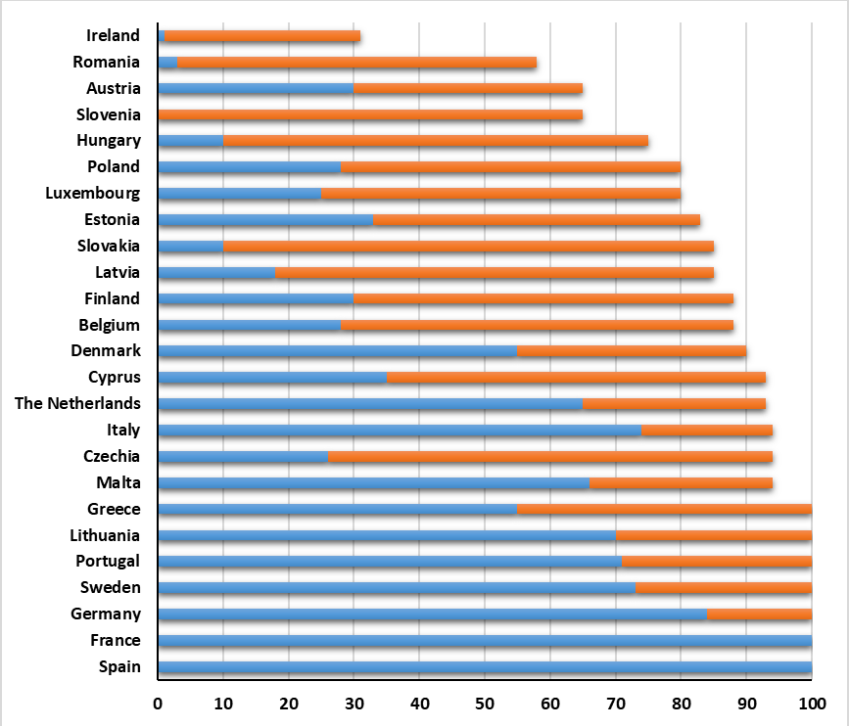

Figure 11 The percentage of the KUs that each country covers with mandatory courses (blue) and other courses (orange) [66]

The next step would be to continue with the instructions to introduce cyber security activities that can be used as stand-alone or as part of the AP CS curriculum, depending on the teacher population. Cyber security is an interdisciplinary area. So, naturally, cross-disciplinary skills, such as finding business solutions to social problems, are necessary to build an effective, efficient, and diverse workforce.

EU research also shows clear divisions in knowledge, competencies, and precise national divisions. Unsurprisingly, large countries offer a higher coverageof the knowledge units (that is, there is at least one education program covering each knowledge unit in the country). 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 [66]. Some smaller countries have good coverage as well (Figure 11 and Figure 12).

Looking at the EU and the USA's experience, it can be concluded that the direction is set correctly and study courses are improved centrally. Study programs are introduced in different countries and states. 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 both the state and SMEs and industry in general.

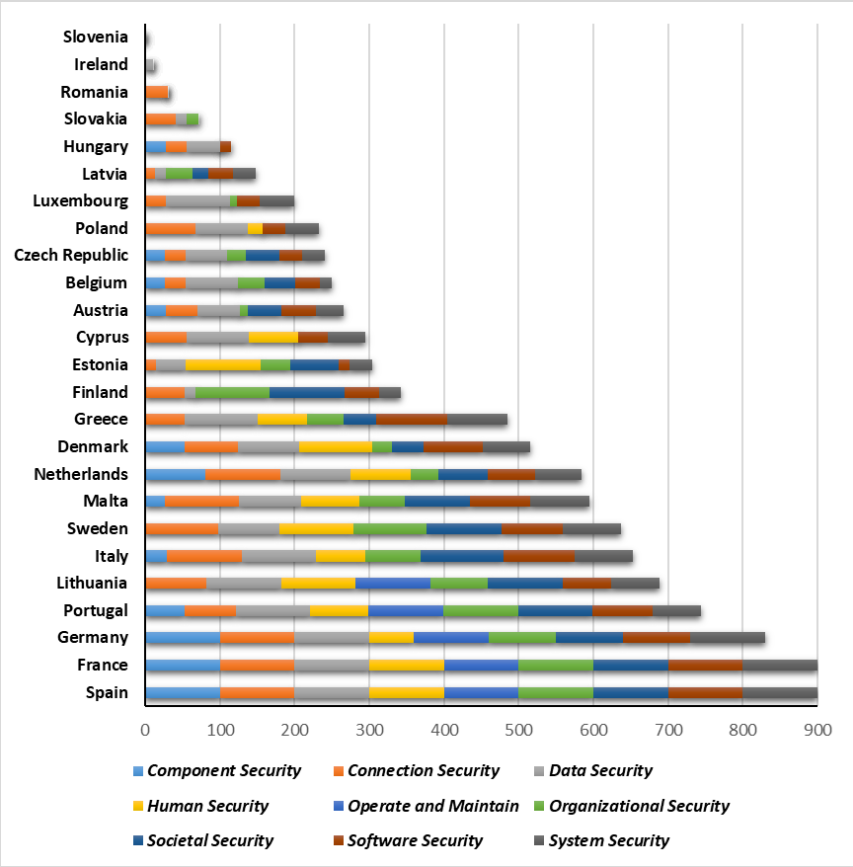

Figure *12* The percentage of each knowledge areas and knowledge units covered with mandatory courses for each country [66]

Looking at the EU and the USA's experience, it can be concluded that the direction is set correctly and study courses are improved centrally. Study programs are introduced in different countries and states. 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 both the state and SMEs and industry in general.

6.3 Massive open online courses (MOOC)

There is a current demand for cyber security professionals, and many courses have been developed to address this issue. Online courses are exciting as they reach out to more people. Authors [67] present 35 cyber security online courses concerning NICE framework to help in selecting topics while preparing a cyber security course. Results show that there are gaps to patch, thus place for many more new courses. Additionally, guidelines on how to prepare a cyber security course are presented, all of them based on the analysis of a cyber security edX MOOC with +2,000 active users. A framework for the study of edX courses has also been released to promote the research in this direction [67].

The authors [67] addresses both topic choice and course preparation issues. Concerning the first aspect, the current coverage of the NICE framework is studied. For this purpose, 35 free online courses are surveyed. This leads authorsto detect gaps between what is taught and what is required in cyber security work roles – those parts of NICE that have received less attention from training designers. Concerning course preparation, the authors analyze students' performance and commitment to a Massive Online Open Course (MOOC) in the edX platform in 2017. This MOOC counted on +10,000 worldwide enrolled students, among which +2,000 were initially active. This analysis leads authors to propose a set of recommendations for course preparation. Moreover, to foster further research in this area, an open-source framework to analyze student results in edX courses is released [67]. One of the main results is shown in Figure 13.

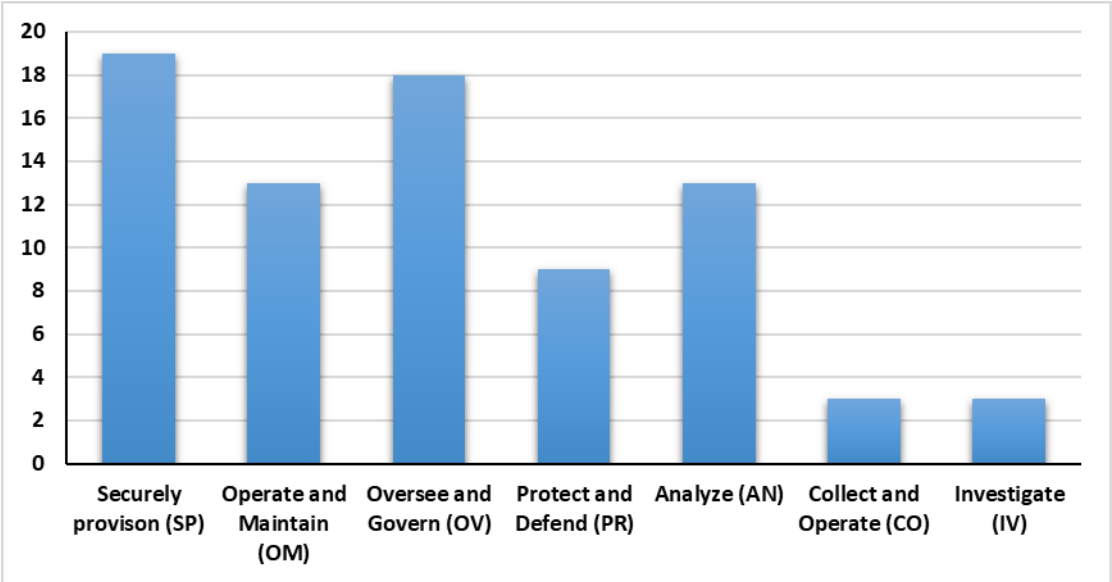

Figure 13 Coverage of cyber security domains from training courses [67]

The authors [68] investigate the machine learning (ML) techniques changing both the offensive and defensive aspects of cyber security. The implications are powerful for privacy, as ML approaches provide unprecedented opportunities to use collected data. Thus, education on cyber security and AI is needed. To investigate how AI and cyber

security should be taught together, we look at previous studies on cyber security MOOCs by conducting a systematic literature review. The initial search resulted in 72 items, and after screening for only peer-reviewed publications on cyber security online courses, 15 studies remained. Three of the studies concerned multiple cyber security MOOCs, whereas 12 focused on individual courses. The number of published works evaluating specific cyber security MOOCs was small compared to all available cyber security MOOCs.

Analysis of the studies revealed that cyber security education is, in almostall cases, organized based on the topic instead of used tools, making it difficult for learners to find focused information on AI applications in cyber security. Furthermore, there is a gap in the academic literature on how AI applicationsin cyber security should be taught online [68] The authors highlight followingthe literature search, the resulting 15 papers were observed in detail. The reports were divided into two groups based on whether they considered a single cyber security course or multiple. The preliminary information regarding the courses was obtained from the studies. They were expected to contain meta-level details about the course's purpose, its design philosophy, and possible reasons for involving or not involving AI. Secondary information regarding the coursewas obtained from the actual course page when available, where the course's learning goals and topics were retrieved. The aim was to look at how many of the courses involve AI [68].

From a large study to focused research, it can be seen that the results are welland finely described. However, it should be emphasized that MOOCs cannot give 100 percentage of the results as it would be possible on-premise, but it should also be measured, or the online options are not similar. As can be seen from the authors' results that MOOC still has room to grow and developits capabilities in Cyber Security and Smart Grids training, giving practical examples with which learners can operate in real-time situations.

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

7.1 Stakeholder workshop

To achieve a better understanding into the real-world situation of industry and academia, a virtual workshop were conducted by us to inform both parties about the results of literature review and provide a context for discussing the necessarytools and skills for cybersecurity topic in the energy domain. The duration of this workshop was 2.5 hours. The number of participants are approximately 23 which are selected from the associations, universities and industries. The technique which was used to choose and invite the key stakeholders in this workshop is snowball sample [69]. The first part of the stakeholder workshop started with a preamble and the expected goals of the project. The result of the literature review was also mentioned in this part. The workshop was continued throughout the open discussion and stakeholders were divided into four small groups, led by a moderator. Each group discussed the same questions whichare mainly focused on what skills students learn in academia for the industrial job and what does the industry needs from the young professional. To show comments and ideas for further discussion, a virtual concept board was provided. Finally, each group reported their results, and afterward, participants discussed the open questions across the groups

7.2 Recommendations from the workshop

To summarize the ideas from discussions and come up with a practical solutions, the result of discussions from each group stakeholders provided their insights. Classifying the ideas from the workshop can help to align the Industry expectations from the university graduates. Table 5 shows the result of the stakeholder work-shop. All in all, the ideas 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 want to work in the industry in future.

Table 5 Recommendation from the stakeholder workshop [70]

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.	——

The commonly used tools that are presented in the workshop and the literature have some differences. Regarding cyberattacks and countermeasures, designing testbeds to assess the systems, connection and component are currently the main focus on literature. While, the results of discussion in the work- shop showed that the use of platforms, tools, and standards such as shodan, IEC62443, kali linux and ISO27001) which provide the security professional are very high in the daily activity. This helps to keep informed about actual threats and adversarial issues.

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

This section presents tools for education in cyber security in the smart grid context. Common tools are collected from the literature that has been used in the research and education for cybersecurity. There is no single tool that can fit all purposes, it depends on the education goals whether to focus on providing knowledge for active learning or specialize in vulnerabilities investigation. This section presents existing tools into two aspects which are 1) basic tools for active learning about cybersecurity, and 2) advanced tools for vulnerabilities experiments.

8.1 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. These approaches focus mainly on building deep knowledge and understanding of the main concepts related to the field as well as the analytical skills required for further development. In addition, hands-on skills are also considered since

they provide the means for practicality and ability to apply the knowledge being gained in this sector. From [71], approaches of education that are suitable for cyber security field are highlighted in Table 6 below.

Table 6 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

In more details, remote and virtual labs [72] are one of the most useful approaches for education in cyber security related fields. The approach and its associated tools provide active and effective means for interaction between students and instructors that is similar to classroom environment. Regarding virtual lab tools, they create a computer-based virtual environment that is used for testing and experimenting. These tools are helpful for upgrading personal skills, especially since they do not connect to actual devices, and thus allowing for trial-and-error problem solving methodology without compromising or affecting systems' functionality. In contrast, remote lab tools use ICT technologies to connect to physical labs and devices at different locations. This provides convenience to learners since they can access devices remotely, thus allowing testing and collecting data. However, since remote lab tools connect to devices still, experimenting should be supervised, as systems can be affected. Some of the remote lab tools include Labview, OMWeb, and NI ELVIS. As well, for virtual labs tools include but not limited to the following such as Labster and LabAlive.

Augmented reality AR [73] [74] is an advanced form of virtual reality technology that is used to enhance learning throughout sharing learning concepts and allowing interactive sessions. With augmented reality, students can view a specific scenario that is provided by instructors combined with data, so that to form a better experience. AR tools are used in several industries including medical, manufacturing, and service; additionally, they suitable for higher education and are used to provide training in different fields [75]. Some of the typical AR tools include in Worklink, CoSpaces, and Merge Cube.

Data visualization [76] is a technique that deals with representation of data in different forms graphically for the sake of creating informative figures that are better understood by other parties. Data visualization has long been known via simple charts and so, but with the proliferation of data, different tools came to exist, as they can provide more details and insights

about data. Currently, some of the famous tools for data visualization such as Tableau, Microsoft Power Bi, and IBM Congos Analytics.

Cloud computing [77] [78] technology is used to provide resources and computing power that can be used for different operations and purposes, including education. Apart of their use for keeping information secure and to perform complex computations on demand, cloud computing and storage platforms provide easy access to material and data, also allows sharing and collaboration, and thus provide seamless communication experience to learners and all needed tools to teachers. Famous tools to be used with cloud computing include in Google Classroom, Microsoft Education Center, and Amazon Web Services

Flipped learning [79] is not a tool by itself but is rather a general instructional strategy that combines traditional classroom practices with technology innovation tools that are suited for the given course. In this strategy, educational materials are handed to students beforehand, and the educational process is mainly student-based with general guidance from teachers and instructors. Flipped learning [80] is currently used in many institutions since it provides a rich and seamless experience to students, and that it can be used to deliver a certain course to a higher number of students, which is referred to as Massive Open Online Courses (MOOC).

Gamification [81] is an innovative approach to ensure engagement of students and learners in a certain course by introducing material in the form of interactive games and in a style that promotes game thinking. This approach is used to draw expectations about a certain problem, thus enhance problem solving skills among learners. Game theory provides the basis of this technique, and it helps to solve problems that include different paths and choices, in other words probability and statistics. Many tools exist to support this approach, in which some of the most used are Kahoot and Gimkit.

Finally, simulations [82] [83] are one of the old techniques that are used for education. In this approach, cases and scenarios that simulate the real ones are created, thus, to be used for students' training before moving to actual practice. Depending on the industry, many simulation tools exist, from physical simulators to virtual ones. Moreover, with current computation capabilities, many tools are even used to create cases of real scenarios, thus, to study different factors and gather measurements that are difficult to do in reality. For instance, and related to the topic of this report, real-time simulator [84] [85] tools have computation power that allows them to simulate real-time situations, thus provide means for design and testing before moving models to actual practice. Many tools exist to provide simulations, which typically include in MATLAB and Simulink.

8.2 Advanced tools for vulnerabilities experiments

Smart grid systems and due to their architecture [86] [87] [88], unlike traditional power grids, are accompanied by an increased number of vulnerabilities and threats. For instance, the use of intelligent devices; physical security of devices out of premises; smart meter and end-customer security; established trust between conventional and intelligent devices; the use of IP protocols and associated risks; insider attacks as well as other forms of attacks as Man in the Middle MitM, Denial of Service DoS attacks, and malicious data injection; are all examples of vulnerabilities that should be considered. Accordingly, several cyber security tools are used to provide an adequate level of protection to smart grids by means of performing vulnerability assessment, threat detection and mitigation processes. In Table 7, a list of the typical tools that are used for these processes is presented and classified into different categories according to their functionality [89] [90] [91].

Table 7 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
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

Depending on the assets to be protected and the level of protection required, some of the tools given should be used to protect against potential cyber incidents. Moreover, advanced tools with advanced capabilities and protection schemes should also be used when it comes to protecting critical infrastructure components.

The existing tools cover mostly the technical-related issues associated with physical cyber systems. However, as breaches continue despite the existence of such tools, it is clearly noticed that these tools solely are not sufficient enough for the protection scheme required. Two issues have been raised here. First, the human factor is clearly one of the most critical issues to consider, and it has been noticed the lack of awareness tools. Accordingly, education approaches and tools mentioned in the first section should be considered when designing curricula suitable for cyber security and threat mitigation. Moreover, continuous education as a key point to ensure updated knowledge and skills to deal with new techniques and forms of cyber incidents, should be planned on a regular basis. Second, many of the tools used to detect vulnerabilities and threats use signature-based and anomaly-based detection techniques, and it has been noticed also the lack of a common platform or a tool for vulnerability and threat reporting. Existing advanced tools should be able to tackle 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.

9. Conclusion and recommendation

The CPES testbed has been used to conduct extensive cybersecurity research on component, system, and connection domains; however, there is still a shortage of study on software security as well as data security on how to secure, transfer, and process data. Students and practitioners would get a deeper understanding and awareness of cybersecurity by integrating real-world experiences. This can be done by introducing a simple testbed to the high school and undergraduate students, such as an IoT system in a smart house. The CPES laboratory and specific testbeds can be used for teaching for higher education to investigate thevulnerabilities and countermeasures.

In addition, non-technical dimensions should be more considered for teaching and researching for cyber security in the smart grid to prevent the opposition ofnew technologies deployment as well as prevent and/or reduce the severity of the cyberattack. In order to meet the industry's expectations, students should havea deeper knowledge of interdisciplinary power systems and communication to understand the interdependence of smart grid technology to perform real-world tasks.

The importance of cyber security (including smart grids cyber security) skills straightening is stressed in EU policy documents and industry studies and recommendations. Documents highlight the need for accessible cyber security education availability. The topic has also been addressed in some related scientific searches.

The main conclusions from the literature review are following:

- In the EU, there is a significant and persistent digital skills gap. The current education offer of specialized education programs does not address all needs (especially for adults who want to re-skill or up-skill and new specialists).
- Cyber security education has been identified as one of the strategic dig- ital 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.
- Cyber security is represented in different education forms, as Higher education, Continuing education, MOOC. However, smart grid security topics are addressed relatively rarely.
- Cyber security programs include various topics; organizational security(security operations and personal security) and the knowledge unit system retirement are the least covered [92].
- The main findings coming from the literature review and university Cyber security offer in both the EU and the USA are quite similar and yet, the technical reporting coming from the universities is more theoretical, while the MOOC and continuing learning provide with specific knowledge witha greater emphasis on the practical side.
- Slim divisions from the literature on EU countries indicate that study courses are strong, but students are not as well prepared at lower levels.
- Explicit Smart Grids study courses are not currently available in university study pro-grams but in MOOC they are available and are also availablein continuing education programs with certificate supporting documents.

EU policies and industry research includes several requirements that must be considered in cyber security curricula recommendations for smart grids development. The main requirements and recommendations are following:

- Education must be accessible for different EU citizens 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 on monitoring and controlling it).
- It must provide theoretical lectures and practical training, as the use of cyber security management tools (as SIEM, etc.) and virtual laboratories, 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 [8]: 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 [8].
- 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 simulations 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.

Reference

[1] The European Commission, *Europe investing in digital: the Digital Europe Programme — Shaping Europe's digital future*. The European Commission, 2020.

[2] European Union agency for cybersecurity, *A trusted and cyber secure Europe. ENISA Strategy*. European Union agency for cybersecurity, 2020.

[3] The European Commission, *The EU Cybersecurity Strategy for Digital decade*. The European Commission, 2020.

[4] IEEE, *Cybersecurity for a stronger and more resilient digital Europe. An IEEE European Public Policy Committee Position Statement*. IEEE, 2020.

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

[6] J. R. Center, *Academic offer and demand for advanced profiles in the EU: Artificial Intelligence, High Performance Computing and Cybersecurity*. European Commission Joint Research center, 2020.

[7] European Paliament, *Cybersecurity of critical energy infrastructure- Briefing of European Parliamentary Re-search Service*. European Palia- ment, 2019.

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

[9] The European Paliament, "Cybersecurity act," 2019.

[10] The European Commission, *The EU cybersecurity certification framework*.

[11] The National Institute of Standards and Technology (NIST), "Nist cybersecurity and privacy program."

[12] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Act on the federal office for information security."

[13] M. Schallbruch and I. Skierka, "The organisation of cybersecurity in ger- many," 2018.

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

[15] Association for Computing Machinery (ACM) Committee for Comput-ing Education in Community Colleges (CCECC), *Cybersecurity Curricular Guidance for Associate-Degree Programs*. Association for Computing Machinery, 2017.

[16] National Initiative for Cybersecurity Careers and Studies (NICCS), *Cybersecurity Workforce Framework*. https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework, 2020.

[17] Centers of Academic Excellence – Cyber Defense (CAE-CD), Two-Year Knowledge Units.https://www.nsa.gov/Portals/70/documents/resources/students-educators/centers-academic-excellence/Cyber2020.

[18] T. Yardley, S. Uludag, K. Nahrstedt, and P. Sauer, "Developing a smart grid cybersecurity education platform and a preliminary assessment of its first application," Oct. 2014.

[19] D. Navarro, J. C. Mendez, K. Berrios, E. Ortiz-Rivera, and E. Arzuaga, "Using cybersecurity as an engineering education approach on computer engineering to learn about smart grid technologies and the next generation of electric power systems," Oct. 2014.

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

[21] K. Schwab, *The Fourth Industrial Revolution*. USA: Crown Publishing Group, 2017.

[22] E. Hammad, M. Ezeme, and A. Farraj, "Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification," International Journal of Electrical Power & Energy Systems, vol. 104, pp. 817–826, Jan. 2019, doi: 10.1016/j.ijepes.2018.07.058.

[23] J. J. Chromik, A. Remke, and B. R. Haverkort, "An integrated testbed for locally monitoring scada systems in smart grids," *Energy Informatics*, vol. 1,

no. 1, pp. 1–29, 2018.
[24] N. Jamil, Q. Qassim, M. Daud, N. Jaaffar, I. Z. Abidin, and W. A. Wan, “Electrical power scada testbed for cyber security assessment,”
[25] F. Sauer, M. Niedermaier, S. Kießling, and D. Merli, “Licster–a low- cost ics security testbed for education and research,” *arXiv preprint arXiv:1910.00303*, 2019.
[26] A. Siddiqi, N. O. Tippenhauer, D. Mashima, and B. Chen, “On practical threat scenario testing in an electric power ics testbed,” in *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security*, pp. 15–21, 2018.
[27] V. K. Singh, S. P. Callupe, and M. Govindarasu, “Testbed-based evaluation of siem tool for cyber kill chain model in power grid scada system,” in *2019 North American Power Symposium (NAPS)*, pp. 1–6, IEEE, 2019.
[28] C. Konstantinou, “Cyber-physical systems security education through hands-on lab exercises,” *IEEE Design & Test*, vol. 37, no. 6, pp. 47–55, 2020.
[29] C. Lee, “Discovering cyber vulnerabilities in scada control system via examination of water treatment plant in laboratory environment,” *The UNSW Canberra at ADFA Journal of Undergraduate Engineering Research*, vol. 9, no. 1, 2018.
[30] X. Li, M. Liu, R. Zhang, P. Cheng, and J. Chen, “Demo abstract: An industrial control system testbed for the encrypted controller,” in *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*, pp. 343–344, IEEE, 2018.
[31] Z. O’Toole, C. Moya, C. Rubin, A. Schnabel, and J. Wang, “A cyber-physical testbed design for the electric power grid,” in *2019 North American Power Symposium (NAPS)*, pp. 1–5, IEEE, 2019.
[32] S. Haghani, “Development of a new course on smart-grid communication and security for senior undergraduate and graduate students,” in *2018 ASEE Annual Conference & Exposition*, 2018.
[33] Y. Wang, Z. Zhang, and L. Xie, “A semi-physical simulation testbed for cybersecurity,” in *2018 37th Chinese Control Conference (CCC)*, pp. 6423–6428, IEEE, 2018.
[34] J. Xie, J. C. Bedoya, C.-C. Liu, A. Hahn, K. J. Kaur, and R. Singh, “New educational modules using a cyber-distribution system testbed,” *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5759–5769, 2018.
[35] J. Jones and P. Brouse, “T2-f: A remotely accessible, configurable, instrumented ics lab for attack, defend, and forensics research and education,” 2018.
[36] H. Neema, B. Potteiger, X. Koutsoukos, G. Karsai, P. Volgyesi, and J. Sztipanovits, “Integrated simulation testbed for security and resilience of cps,” in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*,pp. 368–374, 2018.
[37] J. D. Kollmer, *A Hardware-In-The-Loop Experimental Testbed for the Evaluation of Power Grid Stability and Security*. PhD thesis, Temple University, 2020.
[38] J. J. Chromik, C. Pilch, P. Brackmann, C. Duhme, F. Everinghoff, A. Giberlein, T. Teodorowicz, J. Wieland, B. R. Haverkort, and A. Remke, “Context-aware local intrusion detection in scada systems: a testbed and two showcases,” in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 467–472, IEEE, 2017.
[39] H. Zhang, D. Ge, J. Liu, and Y. Zhang, “Multifunctional cyber-physical system testbed based on a source-grid combined scheduling control simulation system,” IET Generation, Transmission & Distribution, vol. 11, no. 12, pp. 3144–3151, Feb. 2017, doi: 10.1049/iet-gtd.2016.1853.
[40] M. Frank, M. Leitner, and T. Pahi, “Design considerations for cyber security testbeds: A case study on a cyber security testbed for education,” in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, pp. 38–46, IEEE, 2017.

[41] J. Achara, M. Mohiuddin, W. Saab, R. Rudnik, and J.-Y. Le Boudec, "T-recs: A software testbed for multi-agent real-time control of electric grids," in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1–4, IEEE, 2017.

[42] O. Salunkhe, M. Gopalakrishnan, A. Skoogh, and Å. Fasth-Berglund, "Cyber-physical production testbed: literature review and concept development," *Procedia manufacturing*, vol. 25, pp. 2–9, 2018.

[43] M. Kaouk, F.-X. Morgand, and J.-M. Flaus, "A testbed for cybersecurity assessment of industrial and iot-based control systems," in *Congrès Lambda Mu 21 Maîtrise des risques et transformation numérique: opportunités et menaces*, 2018.

[44] M. Otte, D. Pala, C. Sandroni, S. Rohjans, and T. Strasser, "Multi-laboratory cooperation for validating microgrid and smart distribution sys- tem approaches," 2018.

[45] D. Assante, C. Capasso, and O. Veneri, "Internet of energy training through remote laboratory demonstrator," *Technologies*, vol. 7, no. 3, p. 47, 2019.

[46] Q. Qassim, N. Jamil, I. Z. Abidin, M. E. Rusli, S. Yussof, R. Ismail, F. Abdullah, N. Ja'afar, H. C. Hasan, and M. Daud, "A survey of scada testbed implementation approaches," *Indian Journal of Science and Technology*, vol. 10, no. 26, pp. 1–8, 2017.

[47] Y. Xie, W. Wang, F. Wang, and R. Chang, "Vtet: A virtual industrial control system testbed for cyber security research," in *2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pp. 1–7, IEEE, 2018.

[48] H. Hui, P. Maynard, and K. McLaughlin, "Ics interaction testbed: a plat- form for cyber-physical security research," in *6th International Symposium for ICS & SCADA Cyber Security Research 2019 6*, pp. 89–96, 2019.

[49] P. Shukla, T. Akther, Z. Nedic, and A. Nafalski, "Design of a microgrid laboratory for electrical power education,"

[50] C. J. Du Plessis, *A framework for implementing Industrie 4.0 in learning factories*. PhD thesis, Stellenbosch: Stellenbosch University, 2017.

[51] M. Thornton, H. Smidt, V. Schwarzer, M. Motalleb, and R. Ghorbani, "Internet-of-things hardware-in-the-loop simulation testbed for demand re- sponse ancillary services," *Materials for Energy, Efficiency and Sustainabil- ity, TechConnect Briefs*, pp. 66–69, 2017.

[52] B. Pearson, L. Luo, C. Zou, J. Crain, Y. Jin, and X. Fu, "Building a low-cost and state-of-the-art iot security hands-on laboratory," *IFIPIoT 2019: Internet of Things. A Confluence of Many Disciplines*, 2020.

[53] M. Kuzlu and O. Popescu, "Upgrading of a data communication and com- puter networks course in engineering technology program," in *2020 ASEE Virtual Annual Conference Content Access*, 2020.

[54] S. Hutchinson, Y. H. Yoon, N. Shantaram, and U. Karabiyik, "Internet of things forensics in smart homes: Design, implementation, and analysis of smart home laboratory," in *2020 ASEE Virtual Annual Conference Content Access*, 2020.

[55] L. González-Manzano and J. M. de Fuentes, "Design recommendations for online cybersecurity courses," *Computers & Security*, vol. 80, pp. 238–256, 2019

[56] B. Arora, "Teaching cyber security to non-tech students," *Politics*, vol. 39, no. 2, pp. 252–265, 2019.

[57] "Cyber security and software technology doctoral programme."

[58] T. Yardley, S. Uludag, K. Nahrstedt, and P. Sauer, "Developing a smart grid cybersecurity education platform and a preliminary assessment of its first application," in *2014 IEEE Frontiers in Education Conference (FIE) Proceedings*, 2014.

[59] Global Information Assurance Certification (GIAC), *Global Industrial Cyber Security Professional Certification (GICSP)*. 2014.

[60] Utilisec, "Assessing and exploiting control systems with samuraistfu," 2014.

[61] Cybati, "Critical infrastructure and control system cybersecurity," 2014.

[62] SCADAhacker, "Industrial control system cyber security training," 2014.

[63] SANS, "Ics410 ics/scada security essentials," 2014.

[64] Cimation, "Ics/scada security courses," 2014.

[65] G. Javidi and E. Sheybani, "K-12 Cybersecurity Education, Research, and Outreach," 2018 IEEE Frontiers in Education Conference (FIE), 2018, pp. 1-5, doi: 10.1109/FIE.2018.8659021
[66] 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
[67] L. González-Manzano and J. M. de Fuentes, "Design recommendations for online cybersecurity courses," *Computers & Security*, vol. 80, pp. 238–256, 2019.
[68] S. Laato, A. Farooq, H. Tenhunen, T. Pitkamaki, A. Hakkala, and A. Airola, "Ai in cybersecurity education-a systematic literature review of studies on cybersecurity moocs," in *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)*, pp. 6–10, IEEE, 2020.
[69] J. Leventon, L. Fleskens, H. Claringbould, G. Schwilch, and R. Hessel, "An applied methodology for stakeholder identification in transdisciplinary research," *Sustainability science*, vol. 11, no. 5, pp. 763–775, 2016.
[70] 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.
[71] Mogoş, Radu-Ioan, et al. "Technology enhanced learning for industry 4.0 engineering education." Rev. Roum. Sci. Techn.–Électrotechn. et Énerg 63.4 (2018): 429-435.
[72] Athauda, Rukshan, et al. "Design of a Technology-Enhanced Pedagogical Framework for a Systems and Networking Administration course incorporating a Virtual Laboratory." 2018 IEEE Frontiers in Education Conference (FIE). IEEE, 2018.
[73] Kommera, Nikitha, Faisal Kaleem, and Syed Mubashir Shah Harooni. "Smart augmented reality glasses in cybersecurity and forensic education." 2016 IEEE Conference on Intelligence and Security Informatics (ISI). IEEE, 2016.
[74] Seo, Jinsil Hwaryoung, et al. "Using virtual reality to enforce principles of cybersecurity." The Journal of Computational Science Education 10.1 (2019).
[75] Tashko, Rizov, and Rizova Elena. "Augmented reality as a teaching tool in higher education." International Journal of Cognitive Research in Science, Engineering and Education 3.1 (2015).
[76] Telea, Alexandru C. Data visualization: principles and practice. CRC Press, 2014.
[77] González-Martínez, José A., et al. "Cloud computing and education: A state-of-the-art survey." Computers & Education 80 (2015): 132-151.
[78] Yadav, Kiran. "Role of cloud computing in education." International Journal of Innovative Research in Computer and Communication Engineering 2.2 (2014): 3108-3112.
[79] Bergmann, Jonathan, and Aaron Sams. Flipped learning: Gateway to student engagement. International Society for Technology in Education, 2014.
[80] Wang, Kai, and Chang Zhu. "MOOC-based flipped learning in higher education: students' participation, experience and learning performance." International Journal of Educational Technology in Higher Education 16.1 (2019): 1-18.
[81] Kiryakova, Gabriela, Nadezhda Angelova, and Lina Yordanova. "Gamification in education." Proceedings of 9th International Balkan Education and Science Conference, 2014.
[82] Rutten, Nico, Wouter R. Van Joolingen, and Jan T. Van Der Veen. "The learning effects of computer simulations in science education." Computers & education 58.1 (2012): 136-153.
[83] Keys, Bernard, and Joseph Wolfe. "The role of management games and simulations in education and research." Journal of management 16.2 (1990): 307-336.

[84] Chlela, Martine, et al. "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks." 2016 IEEE Power and Energy Society General Meeting (PESGM). IEEE, 2016.
[85] Choi, Jinchun, et al. "A Real-Time Hardware-in-the-Loop (HIL) Cybersecurity Testbed for Power Electronics Devices and Systems in Cyber-Physical Environments." 2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG). IEEE, 2021.
[86] Aloul, Fadi, et al. "Smart grid security: Threats, vulnerabilities and solutions." International Journal of Smart Grid and Clean Energy 1.1 (2012): 1-6.
[87] Khurana, Himanshu, et al. "Smart-grid security issues." IEEE Security & Privacy 8.1 (2010): 81-85.
[88] Deng, Yi, and Sandeep Shukla. "Vulnerabilities and countermeasures–a survey on the cyber security issues in the transmission subsystem of a smart grid." Journal of Cyber Security and Mobility (2012): 250-276.
[89] Young, Susan, and Dave Aitel. The hacker's handbook: the strategy behind breaking into and defending networks. Auerbach publications, 2003.
[90] Vacca, John R., ed. Managing information security. Elsevier, 2013.
[91] Stewart, James Michael. CompTIA Security+ Review Guide: Exam SY0-501. John Wiley & Sons, 2017
[92] Cybersecurity for Europe project deliverables, “D6.2 education and training review,” 2020.
[93] S. M. S. Hussain, T. S. Ustun, and A. Kalam, “A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges,” IEEE Transactions on Industrial Informatics, vol. 16, no. 9. Institute of Electrical and Electronics Engineers (IEEE), pp. 5643–5654, Sep. 2020. doi: 10.1109/tii.2019.2956734.
[94] I. ALI, M. A. AFTAB, and S. M. S. HUSSAIN, “Performance comparison of IEC 61850-90-5 and IEEE C37.118.2 based wide area PMU communication networks,” Journal of Modern Power Systems and Clean Energy, vol. 4, no. 3. Springer Science and Business Media LLC, pp. 487–495, Jul. 2016. doi: 10.1007/s40565-016-0210-y.

Appendix 1: ACM Cybersecurity Curricula framework and Cybersecurity curricula Guidance

To identify essential cybersecurity skills, we consider the following:

- The ACM Cybersecurity Curricula framework (CSEC2017 Joint Task Force, 2017), developed by the Association for Computing Machinery (ACM) in collaboration with the IEEE Computer Society (IEEE-CS), the Special Interest Group on Information Security and Privacy of the Association for Information Systems (AIS SIGSEC), and the Committee on Information Security Education of the International Federation for Information Processing Technical (IFIP WG 11.8) [9].
- The ACM Committee for Computing Education in Community Colleges (CCECC) Cybersecurity Curricular Guidance for Associate-Degree Programs (Cyber2yr2020) [10].

Each knowledge area encompasses several knowledge units with assigned skills (see Table A1). Skills ("know-how") are defined as qualities that people develop and learn over time with practice and through interaction with others.

Knowledge area	*Knowledge unit*	*Skills*
Data Security	Cryptography	• Apply cryptographic protocols, tools, and techniques are appropriate for providing confidentiality, data protection, data integrity, authentication, non-repudiation, and obfuscation • Apply symmetric and asymmetric algorithms as appropriate for a given scenario. • Investigate hash functions for checking integrity and protecting authentication data. • Use historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, Hill cipher, and Enigma machine simulator, to encrypt and decrypt data • Contrast trust models in PKI, such as hierarchical, distributed, bridge, and web of trust. • Apply symmetric and asymmetric cryptography, such as DES, Twofish, AES, RSA, ECC, and DSA for a given scenario.
	Digital Forensics	• Perform fundamental incident response functions including detecting, responding, and recovering from security incidents. • Examine legal issues, authorities, and processes related to digital evidence. • Carry out forensically sound acquiring and handling of digital evidence following chain of custody best practices. • Analyze digital evidence from non-PC devices, such as smartphones, tablets, GPS, game consoles, Smart TVs, and IoT devices. • Apply documentation techniques and reporting of findings using industry standard and technically accurate terminology and format. • Carry out verification and validation of evidence during forensic acquisition, preservation, and analysis, including the use of hashes.
	Data Integrity and Authentication	• Apply the concepts and techniques to achieve data integrity, authentication, authorization, and access control. • Execute one or more password attack techniques, such as dictionary attacks, brute force attacks, rainbow table attacks, phishing and social engineering, malware-based attacks, spidering, off-line analysis, and password cracking tools. • Apply basic functions associated with storing sensitive data, such as cryptographic hash functions, salting, iteration count, password-based key derivation, and password managers.

Knowledge area	*Knowledge unit*	*Skills*
		• Implement multifactor authentication using tools and techniques, such as cryptographic tokens, cryptographic devices, biometric authentication, one-time passwords, and knowledge-based authentication • Illustrate the use of cryptography to provide data integrity, such as message authentication codes, digital signatures, authenticated encryption, and hash trees.
	Access Control	• Apply access control best practices, such as separation of duties, job rotation, and clean desk policy. • Apply physical security controls, such as keyed access, man traps, key cards and video surveillance, rack-level security, and data destruction. • Implement data access control to manage identities, credentials, privileges, and related access. • Apply different access control models, including role-based, rule-based, and attribute-based.
	Secure Communication Protocols	• Apply end-to-end data encryption method. • Apply different communication security protocols, such as HTTP, HTTPS, SSH, SSL/TLS, IPsec and VPN technologies. • Illustrate attacks and countermeasures on TLS, such as downgrade attacks, certificate forgery, implications of stolen root certificates, and certificate transparency • Apply privacy preserving protocols, such as Mixnet, Tor, Off-the-record message, and Signal.
	Cryptanalysis	• Identify various cryptanalysis attacks, such as ciphertext only, chosen plaintext, chosen ciphertext, man-in-the-middle, and brute force. • Apply the following algorithms: RSA, ElGamal, and the Digital Signature Algorithm. • Apply different techniques for attacks against public key ciphers, such as Pollard's p-1 and rho methods, quadratic sieve, and number field sieve.
	Information Storage Security	• Apply storage device encryption at the hardware and software levels. • Apply techniques for data erasure and their limitations in implementation.
Software Security	Fundamental Principles	• Apply fundamental design principles, including least privilege, open design, and abstraction, to system and application software. • Execute access decisions and permissions based on explicit need. • Diagram a simple secure application design.

Knowledge area	*Knowledge unit*	*Skills*
		• Modify the levels of abstraction in a given piece of software to provide single layer abstraction whenever possible. • Implement software as a system of secure co-operating components. • Test authorization and access control for a given class. • Develop software for a specific process among multiple secure modules. • Write software specifications that include security specifications infused in the design and implementation specifications. • Diagram a software design that is adjustable to environmental changes. • Decompose a software design to reduce the common mechanism among system components. • Decompose a software design to reduce the common mechanism among system components • Investigate an object's access authorization following the principle of complete mediation. Applying
	Design	• Translate software security requirements into written formal, informal, and testing specifications.
	Implementation	• Write secure code which implements input validation and prevents buffer overflow, integer range violations, and input type violations. • Apply appropriate restrictions to process privileges. • Implement appropriate error and exception handling and user notification. • Develop a secure application or script using defensive programming techniques. • Use an API to detect errors and implement security policy • Implement process and resource checking. • Use cryptographic randomness appropriately for a given scenario. • Implement process isolation.
	Analysis and Testing	• Carry out security-related testing procedures, for a given piece of software. • Apply different methods of static and dynamic software analysis and testing. • Test software components as they are integrated. • Test software as a whole while incorporating unit testing and software testing. • Test the security of a given piece of software, including granting access one OSI model layer at a time while reducing access points.

Knowledge area	*Knowledge unit*	*Skills*
	Deployment and Maintenance	• Perform software installation, configuration, maintenance, and patching tasks in a secure manner.
	Documentation	• Write appropriate security notations within software documentation. • Use available documentation to resolve security-related issues throughout the software life cycle. • Write documentation for software installation and configuration. • Write user documentation emphasizing user security dangers.
	Ethics	• Apply ethical approach, including legal aspects and regulations, to software development.
Component Security	Component Design	• Apply various secure component design principles
	Component Procurement	• Evaluate security threats and risks to both hardware and software in component procurement, such as malware attached during manufacturing or transportation.
	Component Testing	• Perform component security testing. • Use tools and techniques, such as fuzz testing, for testing the security properties of a component beyond its functional correctness.
Connection Security	Physical Media	• Diagram transmission flow in a medium. • Examine characteristics of common networking standards including frame structure, including IEEE 802.3 and 802.11.
	Hardware and Physical Component Interfaces and Connectors	• Manipulate physical components of an organizational network and their interfaces, such as network cables, motherboards, memory, current CPU chips, and buses. • Apply various standards for network connector hardware, such as RJ-11, RJ-45, ST, and SC. • Perform installation and configuration of device drivers for network components in an organization.
	Distributed Systems Architecture	• Apply commonly used network protocols based on the layers of the OSI model. • Apply common protocols used in the world-wide-web and the TCP/IP Internet protocol suite, including HTTPS, DNS, DHCP, ARP, etc. • Classify various cloud system implementations, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Knowledge area	*Knowledge unit*	*Skills*
		• Perform the setup and configuration of a virtual machine in a hypervisor environment
	Network Architecture	• Diagram common architecture models for simple secure systems, including components and interfaces of internetworking devices, according to current standards.
	Network Implementations	• Prevent different connection attacks, such as SYN-scanning, and associated vulnerabilities. • Prevent different transmission attacks, such as Ping of Death and Denial of Service, and associated vulnerabilities. • Analyze the various fields available in Internet Protocol packets at various layers of the Open Systems Interconnection (OSI) and TCP/IP models.
	Network Services	• Apply methods by which components connect, including procedure calls, IPC requests, Interface Definition Languages with stub code, and private protocols over a socket. • Apply specific services and their protocols, including SMTP, HTTP, SNMP, REST, CORBA, and Application layer protocols for specialty devices. • Apply service virtualization as a method to emulate the behavior of specific components, such as cloud-based applications and service-oriented architecture. • Write a security policy that provides guidance and requirements for the services provided by the network along with the measures to be used to see that the policies are followed.
	Network Defense	• Explain how network defenses should be structured using layering, segmentation, and other controls to achieve maximum confidentiality, integrity, and availability (CIA). • Implement configuration settings on devices throughout an enterprise to harden the network against attackers. • Demonstrate how intrusion detection and intrusion prevention services can be used to protect a network and audit network traffic. • Implement a simple virtual private network. • Operate commonly used monitoring network tools and devices. • Analyze logs associated with commonly used monitoring network tools and devices. • Manipulate a commonly used network protocol analyzer to capture and analyze packets flowing through the network • Apply threat hunting, attack pattern detection, and similar network traffic analysis techniques.

Knowledge area	*Knowledge unit*	*Skills*
		• Use tools and techniques for finding and mitigating vulnerabilities through looking at potential weaknesses. • Diagram a Demilitarized Zone (DMZ) and its components, including isolated networks and special servers, such as proxy servers, mail servers, and web servers. • Develop procedures that are used to operate the network in light of applicable security policies and business requirements. • Use penetration testing tools and techniques to test the network by attempting to exploit vulnerabilities.
System Security	System Thinking	• Apply a security threat model to a given scenario.
	System Management	• Carry out elements of an automation plan, such as data mining, machine learning, and related techniques. • Examine reasons for commissioning, decommissioning, and disposing of a system under attack • Apply various system monitoring tools and mechanisms. • Evaluate various system recovery methods. • Implement defenses to protect a system against an insider threat. • Apply a process to document baseline system functions.
	System Access and Control	• Apply various system-related methods for authentication, authorization, and access control. • Write documentation for a system with security considerations in mind. • Differentiate among types of malware. • Detect malicious activity, including the use of intrusion detection systems. • Analyze logs to detect intruders. • Carry out a penetration test on a system. • Analyze system requirements for performing forensic analysis. • Apply recovery and resilience mechanisms that help ensure system availability.
	System Testing	• Execute system security test protocols. • Examine system requirements to determine whether they meet system objectives. • Develop plans for testing secure systems in a given scenario.

Knowledge area	*Knowledge unit*	*Skills*
	Common System Architectures	• Construct virtual environments including disk and memory structures. • Describe the components of a SCADA industrial control system. • Diagram an Internet of Things system.
Human Security	Identity Management	• Compare various methods of identity management, identification, authentication, and access authorization, such as roles, biometrics, and multifactor systems. • Apply various physical assets access controls, such as Network Access Control (NAC), Identity Access Management (IAM), Rules-based Access Control (RAC), and Roles-based Access Control (RBAC).
	Social Engineering	• Detect various social engineering attacks, such as phishing, vishing, email compromise, and baiting, along with suitable mitigations. • Use various tools and approaches to detect and/or mitigate different social engineering threats, such as using email filtering and blacklists.
	Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms	• Debate methods and techniques to persuade individuals to follow rules, policies, and ethical norms related to cybersecurity. • Summarize methods and techniques to employ when an individual is uncertain how to respond to a given cybersecurity situation. • Debate various organizational rules and policies, and ethical norms related to personal social media privacy and security.
	Awareness and Understanding	• Compare various mental models and their impact on how users perceive, judge, communicate, and respond to cybersecurity risks. • Assess individual responsibilities related to cyber hygiene, such as password creation, maintenance, and storage; mitigation tools; identification and use of safe websites; and identifying and using appropriate privacy settings.
	Personal Data Privacy and Security	• Evaluate potential risks to personal data privacy and security for a given scenario. • Examine various types of sensitive personal data (SPD) and associated risks and impact of misuse. • Evaluate how personal tracking techniques and an individual's digital footprint impact privacy and security.
	Usable Security and Privacy	• Describe human factors which impact privacy and security, such as the psychology of adversarial thinking, resistance to biometric authentication, and the economics of security.

Knowledge area	*Knowledge unit*	*Skills*
		• Describe the benefits and challenges of following cybersecurity design guidelines, such as providing secure defaults, and reducing unintentional security and privacy errors.
Organizational Security	Risk Management	• Classify organizational risk factors due to security failure, such as financial loss, operational disruption, and reputational damage. • Describe the components that contribute to an organization's security posture. • Distinguish information assets in an organization and threats to those assets. • Analyze risks in an organization including the potential for both accidental and intentional losses. • Apply a risk management model to measure, evaluate, and communicate risk to stakeholders.
	Security Governance & Policy	• Perform tasks in compliance with information security governance and policy. • Summarize relevant independent and government-sponsored cybersecurity frameworks. • Examine the cost of cybersecurity to an organization.
	Analytical Tools	• Use tools to collect and analyze data to generate security intelligence including threats and adversary capabilities.
	Systems Administration	• Describe components that secure the operating system and system database from vulnerabilities. • Demonstrate administrative functions, such as using group membership to assign permissions. • Discuss security features that are embedded within a cloud environment. • Decompose administrative procedures for protecting the physical system from attack. • Assess processes that ensure availability of system access and functions. • Implement hardening techniques to protect the operating system.
	Cybersecurity Planning	• Apply Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis in an organization.
	Business Continuity, Disaster Recovery, and Incident Management	• Explain the components of a business continuity plan, such as contingency planning, incident response, emergency response, backup, and recovery efforts. • Describe a disaster recovery plan that ensures minimal down time and quick recovery.

Knowledge area	*Knowledge unit*	*Skills*
	Security Program Management	• Perform project management tasks that provide for security of data. • Analyze the meaning and use of various security metrics used in protecting the network. • Apply quality assurance and quality control techniques to prevent mistakes and increase the quality of a system.
	Personnel Security	• Classify components of third-party security services. • Develop components that ensure the protection of personally identifiable information.
Societal Security	Cybercrime	• Describe the proper use or avoidance of fear, uncertainty, and doubt (FUD) as an awareness tool in various contexts, such as physical security, password security, and social engineering • Classify components of third-party security services • Discuss components that ensure the protection of personally identifiable information.
	Cyber Law	• Apply global, national, and international cyber law such as HIPAA, FERPA, and those which relate to fraud, digital contracts, copyrights, and intellectual property. • Apply case law and common law to current legal dilemmas related to computer hacking.
	Cyber Ethics	• Analyze given cyber ethics scenarios, including topics on codes of conduct and professional ethics.
	Cyber Policy	• Discuss cyber policies and related liability issues. • Examine the cost of cybersecurity to a nation.
	Privacy	• Contrast privacy and transparency from a societal perspective, including goals and tradeoffs. • Analyze potential solutions that address circumstances when data privacy is compromised in a societal context.

Appendix 2: Cyber Security universities in the EU and USA

Universities	Study Programs
Abertay University	Master's in Ethical Hacking & Computer Security
	BSc in Ethical Hacking
Bellevue University	Cyber security Degree
	Master of Science in Cybersecurity Degree
Boston University	Bachelor's in Computer Science with Concentration in Cryptography & Data Security
	MS with Specialization in Cyber Security
California State Polytechnic University, Pomona	CIS Undergraduate Program with Information Assurance Track
California State University, San Bernardino	Master of Science in National Cyber Security Studies
Carnegie Mellon University	Master's in Information Security and Assurance
	Master's in Information Security & Assurance
	Master's in Information Security
	Master's in Information Technology - Information Security
	Master's in Information Technology - Privacy Engineering
Colorado Technical University	Bachelor of Science in Cyber Security
	Master of Science in Information Technology - Security Management
De Montfort University	Master's in Cyber Security
	Doctorate in Cyber Security and Software Technology
	Master's in Cyber Technology
Eindhoven University of Technology	Master's in Information Security Technology
	Master's in Cyber Security
ETH Zurich	Master's in Information Security
Fordham University	Master's in Cyber security
George Mason University	Master's in Management of Secure Information Systems
George Washington University	Master's in Cyber security in Computer Science
	Master's in Cyber security Policy and Compliance
	Master's in Cyber security Strategy and Information Management
Iowa State University	Master's in Information Assurance
Johns Hopkins University	Master of Science in Cyber security
Kennesaw State University	Bachelor's in Information Security Assurance
New York University	Master's in Cyber security

Nova Southeastern University	Master's in Information Security
Pennsylvania State University	Master of Professional Studies in Information Sciences - Cyber security Analytics and Operations
	Bachelor of Science in Security and Risk Analysis - Information and Cyber Security Option
	Master of Professional Studies in Homeland Security - Information Security and Forensics Option
Queen's University Belfast	MSc Cyber Security
Southern New Hampshire University	Msc in Information Technologies - Cyber Security
	Bachelor's in Cyber Security
St. John's University	Bachelor's in Cyber Security Systems
	MS in Cyber and Information Security
Stevens Institute of Technology	Master's in Cyber security
Syracuse University	Master of Science in Cyber security (Online)
Tallinn University of Technology	Master's in Cyber Security
	Bachelor of cyber security engineering
University of Birmingham	Master's in Cyber Security
University of Maryland College Park	Master of Engineering in Cyber security
University of Maryland University College	Bachelor's Computer Networks and Cyber security
	Bachelor's Cyber security Management and Policy
	Bachelor's Software Development and Security
	Master's Cyber security Management and Policy
	Master's Cyber security Technology
	Master's Digital Forensics and Cyber Investigation
	Master's Information Technology: Information Assurance
University of Maryland, Baltimore County	Master's in Cyber security
University of North Carolina at Charlotte	Bachelor of Arts in Software and and Information Systems with Concentration in Cyber Security
	Master's of Science Information Technology with Cyber Security Focus
University of Oxford	Centre for Doctoral Training in Cyber Security program
University of South Florida	Master's in Cyber security
	Bachelor's Cyber security
University of Southern California	Master's in Cyber security Engineering
University of Surrey	Master's in Information Security
University of Washington	Master's in Cyber Security Engineering
Utica College	Bachelor's of Science in Cyber security
	Master's in Cyber security
Virginia Polytechnic and State University	Cyber security Minor
Middlesex University London	Network Security and Pen Testing MSc

Cranfield University	MSc in Cyber-secure Manufacturing
Ferris State University	MSc in Information Security and Intelligence
Webster University Leiden	MS Cyber security
Northumbria University London Campus	MSc Cyber Security -London Campus-
John Jay College of Criminal Justice	Master of Science in Digital Forensics and Cyber security
Indiana University	Master of Science Secure Computing
Drexel University	Masters in Cyber security
Mercy College	Masters in Cyber security
Sacred Heart University	Masters in Cyber security
	BS in Cyber security
Villanova University	Master of Science in Cyber Security Engineering
University of Denver	INFORMATION SYSTEMS SECURITY (MASTER'S)
Davenport University	CYBER DEFENSE, BS
Western Governors University	Master of Science, Cyber security and Information Assurance
GISMA, The University of Law	MSc Cyber Security and Data Governance
EIT Digital Master School	Master in Cyber Security
Harbour.Space University	Master in Cyber Security
University of Turku	Master's Degree Programme in Information and Communication Technology: Cyber Security
St. Pölten University of Applied Sciences	Master in Cyber Security and Resilience
University of Padova	Master in Cyber security
Antwerp Management School	Executive Master in IT Risk & Cyber Security Management
Leiden University	Master in Cyber security
INISEG Instituto Internacional de Estudios en Seguridad Global	Master in Cyber security, Analysis and Engineering
King's College London Online	MSc/PG Dip/PG Cert in Advanced Cyber Security
University of Central Lancashire	MSc Cyber security
Northumbria University London Campus	MSc Cyber Security
University of Klagenfurt - Faculty of Technical Sciences	MSc in Artificial Intelligence and Cyber security
AUM American University of Malta	MS in Cyber Security
Eötvös Loránd University	MSc in Computer Science - Cyber security
Manchester Metropolitan University	MSc Cyber Security
University of Bradford	MSc in Cyber Security
University of Westminster	MSc in Cyber Security and Forensics
Universidad de Leon	Master in Research in Cyber security