Towards A Massive Open Online Course for Cybersecurity in Smart Grids – A Roadmap Strategy

Towards A Massive Open Online Course for Cybersecurity in Smart Grids – A Roadmap Strategy

Bahaa Eltahawy
Computing Sciences Department
University of Vaasa
Vaasa, Finland
bahaa.eltahawy@uwasa.fi

Maria Valliou
School of Electrical and computer Engineering
National Technical University of Athens
Athens, Greece
mariavalliou@mail.nuta.gr

Jirapa Kamsamrong
OFFIS e.V.
Oldenburg, Germany
jirapa.kamsamrong@offis.de

Andrejs Romanovs
Department of Modelling and Simulation
Riga Technical University
Riga, Latvia
andrejs.romanovs@rtu.lv

Tero Vartiainen
Computing Sciences Department
University of Vaasa
Vaasa, Finland
tero.vartiainen@uwasa.fi

Mike Mekkanen
Computing Sciences Department
University of Vaasa
Vaasa, Finland
mike.mekkanen@uwasa.fi

***Abstract*— The major trends and transformations in energy systems have brought many challenges, and cybersecurity and operational security are among the most important issues to consider. First, due to the criticality of the energy sector. Second, due to the lack of smart girds' cybersecurity professionals. Previous research has highlighted skill gaps and shortage in cybersecurity training and education in this sector. Accordingly, we proceeded by crafting a roadmap strategy to foster cybersecurity education in smart grids. This paper outlines the methodology of teaching cybersecurity in smart grids to a large group of students in selected European universities via implementing a Massive Open Online Course. Unlike other solutions, this one focuses on hands-on practical skills without trading-off theoretical knowledge. Thus, flipped learning methodology and gamification practices were used to maximize retention rate. Also, a remote lab that includes a real-time simulator was established for training. Here, the process, outcome, and obstacles to overcome in future deployments, are presented.**

Keywords—MOOC, Cybersecurity, Curricula, Training, Smart Grids, Real-time Simulator

I. INTRODUCTION

The energy sector has recently witnessed major changes that resulted in the concept of smart grids. As defined, "a smart grid is an electricity network that can intelligently integrate the behavior and actions of all users connected to it such as generators, consumers, and those that do both, to efficiently deliver sustainable, economic and secure electricity supplies" [1] [2]. Accordingly, cybersecurity of the smart grid has become one of the most important issues to address, due to the increase in the attack surface, and the criticality of assets connected. Cybersecurity has long been identified as one of the European Union digital capabilities to achieve [3]. "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" [4]. Many tools and software packages from different vendors, e.g. [5] [6], already exist to cover security needs and to ensure grid robustness, however, the issue with cybersecurity is still prominent.

In Cybersecurity Curricula Recommendations for Smart Grid (CC-RSG) [1] project, this issue was investigated extensively using surveys, reviews and workshops, and results indicated the following:

1. Cybersecurity topics are not well addressed [7].
2. The lack of cybersecurity professionals in the smart grid field due to scarcity of education that covers this specific field [8] practically.
3. Existing educational offers do not meet the Smart power Security Professional (SPSP) requirements [7]
4. Lack of real-life scenarios [8] and connection with industry [9]

It is clear the critical need for educational offers that can strengthen skills and fill the above-mentioned gaps, especially in light of previous reports that indicate that 50% of cybersecurity incidents at least are merely human error [10]. In our project, the aim is to help post-secondary institutions include learning outcomes about cybersecurity in smart grids in their curricula. In this paper, we present our work in designing a course that can cover the required skills without compromising the theoretical knowledge. The remainder of this paper is organized as follows: Section II presents the research methods adopted. Section III introduces educational methodologies and the different learning approaches. Section IV is dedicated to the Massive Open Online Course (MOOC). In Section V, we present our approach and steps considered for the course design. Section VI is for discussion and faced challenges. Finally, Section VII concludes with summary and future work.

II. RESEARCH METHODS

This work adopts the practices of the Design Science Research (DSR) methodology specified in [11]. Processes are shown in Fig. 1. below.

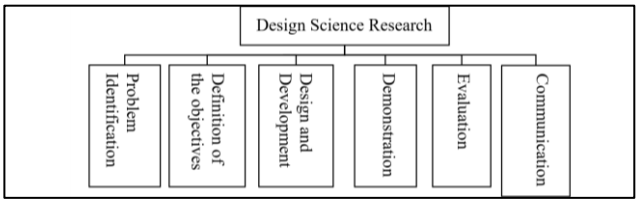

Figure 1: Design Science Research processes [11]

[1] CC-RSG is an Erasmus+ funded project focusing on cybersecurity from an educational perspective. The project has partners from Finland, Germany, Latvia, and Greece. More information: https://www.uwasa.fi/en/research/projects/cybersecurity-curricula-recommendations-smart-grids-cc-rsg

The primary resources that have been used are:

1. CC-RSG project reports [8] and [12]
2. Scientific papers in the field of education, from scientific paper databases (IEEE, AIS, etc.)
3. Technical papers and manuals from manufacturers websites

The main issue covered by this research is "How to design an effective MOOC course to raise knowledge and awareness of cybersecurity in smart grid systems?" Next, we take the steps to answer this question considering educational and technical perspectives and needs.

III. Educational Methodologies & Learning Approaches

As highlighted above, there is a lack of educational offers and educators that can cover theoretical and technical aspects of cybersecurity in smart grids. The educational methodology plays a vital role here as it specifies how learning objectives are met and validated. Depending on the level of retention targeted, different educational methodologies and approaches exist [8] [13] [14], e.g., lecture-based, experiential, active learning, cooperative learning, flipped learning, inquiry-based, problem and project-based learning, and gamification.

In brief, lecture-based learning [15] is the traditional model in which the instructor delivers the material, carries assessments, and is fully responsible for the educational experience. This approach is mostly passive and depends on memorization; however, as practiced in [16], by adding activities including, e.g., cold calling, discussions, learning cards, and so, this model can turn active and more effective. Experiential learning [17] is an active learning approach in which students engage in the learning process and learn by gaining and developing experience. Active learning [18], despite what the name implies, is not just about including activities and participating in the learning process but is rather the participation of all learners and processing of their responses before new information is presented. Cooperative learning [19] refers to an approach in which participants work in teams on a certain task or a project to meet certain criteria and take full responsibility for completing the task. Flipped learning [20] is a modern approach that enables participants to take full ownership of learning by distributing educational material beforehand, thus allowing more room for a dynamic interactive guided environment to take place in the classroom. Inquiry-based learning [21] is an approach in which students follow the same practices of professional scientists in order to build similar knowledge and experience. Problem and project-based learning [22] are approaches that actively engage participants in the learning process by exploring a specific problem/question with the aim of finding answers or developing a solution. Finally, gamification [23] is the use of features commonly found in games (e.g., storytelling, level-beating, badges) with the aim to encourage participation. About effectiveness and learning retention, as the given approaches promote different activities, they vary in their retention rates. Fig. 2 [24] shows these differences.

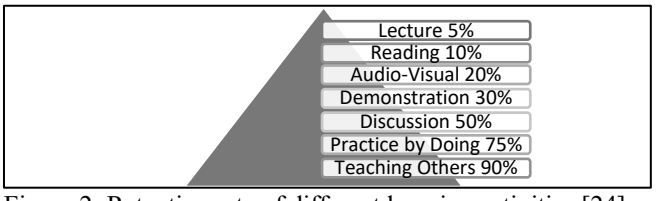

Figure 2: Retention rate of different learning activities [24]

From Figure 2, it is clear that the greater the number of activities, the shift towards the learners' space and the engagement an approach promotes, the higher the retention rate, and thus more knowledge and skills acquired.

Finally, the method of delivery itself has a significant impact on the educational process. Previous research [25] has revealed that although distant online courses feature higher flexibility, they have lower rates – 50 to 80% – to retain students compared to 80 to 90% with face-to-face courses. On the other hand, online learning, and blended learning [26] [27] [28], which combine face-to-face learning with computer-mediated instruction, showed better effectiveness in achieving the learning goals as well as higher performance since they allow for a semi-guided interactive environment between participants and instructors. To remove any ambiguity, it is worth mentioning that an online course can still be considered face-to-face if it has a synchronous live interaction [29].

Based on the explained methodologies and the several factors that affect the educational process, and to meet with CC-RSG project main goals of promoting knowledge of cybersecurity in smart grid and covering existing gaps, a MOOC has been designed. In the next section, a justification of this method is given, in addition to more details about MOOCs design models.

IV. Massive Open Online Course Approach

A. Introduction

According to [30], a MOOC is an "online course designed for large numbers of participants, that can be accessed by anyone anywhere as long as they have an internet connection, is open to everyone without entry qualifications, and offers a full/complete course experience online for free". By this definition, the main pillars and benefits of a MOOC are accessibility, flexibility, being affordable and not requiring much knowledge beforehand. While these are great benefits, MOOCs face two main concerns. First [31], the lack of guidance, structure and support that traditional courses offer. Second [32] [33], issues related to less reliability, pedagogical structure, homogeneity, and depersonalization of course offerings. Fortunately, with academic institutions entering the MOOCs market [34], e.g., Stanford university with Coursera Platform and MIT with edX, some of these issues – especially the second set – were fixed, after adopting academic guidelines.

In terms of coverage, MOOCs mostly cover diverse topics with less emphasis on specialization and advanced courses [34]. Accordingly, several types and formats of MOOCs exist to cater to unique needs and goals of different topics. In Table I, the main types of MOOCs are briefly highlighted.

TABLE I. Main MOOC Types Explained [34] [35]

Type	Definition	Focus
Extended, xMOOC	"Traditional e-learning courses organized by universities"	Knowledge duplication
Connective, cMOOC	Courses that "emphasize creation, creativity, autonomy, and social networking learning"	Knowledge creation
Social, sMOOC	"Social courses characterized by interactivity using social networks"	Active participation and engagement
Transfer, tMOOC	Courses "generating interest towards action and professional interaction	Transfer of learning and Pedagogical transformation

From Table I, although there is a clear distinction between the types of MOOCs, in practice a MOOC offering may combine more than one format to effectively cover its curriculum. Chapter V explains and exemplifies this clearly.

B. MOOC Instructional Design Models

As mentioned, MOOCs combine eLearning approaches and tools with pedagogical learning methodologies. Thus, to successfully design a MOOC, general Instructional Design (ID) models should be referred to. In brief, ID [36] is the "principles and procedures by which instructional materials, lessons, and whole systems can be developed in consistent and reliable fashion", or as described in [37], it is "the planning, creation, refinement, selection sequencing, managing and evaluating activities and resources in support of targeted goals and objectives". ID is thus the application of learning theories [37] [38], e.g., behaviorism (gradual attempt and error, reinforcement, and stimulus-response sequence), cognitivism (formation of cognitive structure), constructivism (learner-centered, collaboration and communication, appropriate resources), and connectivism (creating networks – the role of social and cultural context). Various ID models exist to provide guidance and direction on developing course content, the most famous of which are [38] [39]:

1) Bloom's Taxonomy: A model for measuring learning progress, in which levels of learning and related activities are represented in a hierarchical order that includes remembering at the bottom, then understanding, applying, analyzing, evaluating, and finally creating at the top. Depending on the expected outcome, the activities can be designed accordingly.

2) Gagne's Nine Events Model: A description of instructional events required for effective learning, i.e., gain attention, inform objectives, recall prior knowledge, present the content, provide guidance, practice, provide feedback, assess performance, and finally enhance retention/transfer.

3) ADDIE Model: A framework of the processes required for course design/development, which include: Analyze, Design, Develop, Implement, and Evaluate phases. The framework supports continuity by including revision instances between different processes.

4) Merrill's Principles: Identified principles common to effective ID models, which are: task/problem-centered, activation of prior knowledge, demonstration of new knowledge, application, and encouraging integration.

5) Dick and Carey Model (Systems Approach Model): A model for planning lessons through defining instructional goals, conducting instructional analysis, defining entry requirements, specifying performance objectives as well as test items, developing instructional strategy and material, and finally conducing a formative and summative evaluation.

The processes and practices of these or other ID models should be adopted and modified to meet the desired outcomes of a MOOC, especially since MOOCs need a specific ID curriculum [40]. Next, we present our approach on designing a MOOC for cybersecurity in smart grid.

V. MOOC For Cybersecurity in Smart Grid

A. Course Elements

First, MOOCs that cover general topics of cybersecurity already exist. However, as our previous research [7] [12] revealed, specific topics such as cybersecurity in smart grids are rarely if not at all covered. This was the motivation for initiating this course. Second, by performing the reviews presented in Chapters II and III, and by following guidelines of [41], the elements and approach needed to design an effective course, were identified, adopted, and adjusted. In Table II, the proposed approach is presented.

TABLE II. Course Design Approach

#	Element	Description
1	Learning Objectives	To cover the gap of cybersecurity knowledge related to smart grids
2	Prerequisites to join this course	The course is **ONLY** open to students and professionals with pre-knowledge in the fields of cybersecurity and smart grids
3	Retention level projected by this course	60% to 75%, aiming at active discussions and simple practice by doing tasks
4	Type of MOOC adopted	xMOOC, with practices of tMOOC
5	Instructional Design methodologies adopted	ADDIE and Dick and Carey models for design and targeting the third level – applying – of Bloom's Taxonomy for retention.
6	Approaches used	Flipped learning and gamification, with tasks that promote cooperative learning
7	Method of delivery	Supervised recorded sessions (lectures and tutorials) with online face-to-face mediation by instructors
8	Criteria to increase attention and engagement	Bonus points, the use of games, and discussion forums
9	Assessment and Measurement	Regular quizzes and a final exam
10	Credits	5 credit points (ECTS = 125-140 hours of lectures, exercises, and self-study material)

Regarding the selection of specific criteria, the justifications are:

1. Point 2: the course covers a specific topic, which is the reason pre-knowledge is mandatory.
2. Point 3: as the main aim is active participation, discussions, and simple practice by doing tasks can fulfill such criterion.
3. Point 5: with MOOC offers and the substantial number of participants, resources cannot match the needs to analyze, evaluate or create levels. These levels require higher engagement and fewer participants.
4. Points 9 and 10: according to general academic standards, 1 credit point is 25 to 28 study hours.

B. Real-Time Simulation for Education

Real-time simulation [42] [43] is a technique in which a computer model simulates a physical system in approximately the same amount of time it takes in real time. Unlike other simulation techniques, real-time simulators are powerful computer platforms that allow a code to execute near the real-time it would take with minimum delay. These systems can solve overly complex equations and consider many attributes simultaneously that typical simulation systems cannot provide. Accordingly, real-time simulation systems are used for applications [43] that include large scale systems, control

of actual operating conditions, automotive simulation, automation, robotics, and power systems.

Here, to cover the practical part of the course, a real-time simulator is used to create a cyber-physical testbed to simulate power systems and events that may emerge. Such a testbed can be used for [44], e.g., vulnerability analysis, disturbance scenarios, assessment metrics, impact analysis, and training. In Fig. 3, a typical testbed consisting of Intelligent Electronic Devices (IEDs) controller connected to a Real-Time simulator (OPAL-RT) and a communication and network simulator (EXATA Server), is shown. Such a testbed can be connected with other systems, e.g., SCADA, to run one of the mentioned tests, or used individually to develop attack and mitigation scenarios.

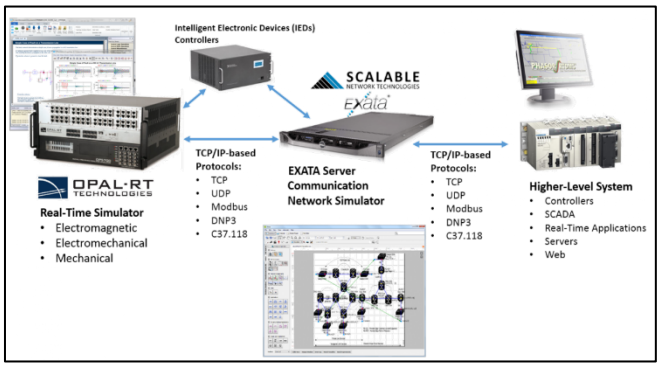

Figure 3: Cyber-physical testbed (adopted from [45])

The shown testbed is used to show students the actual work using the Real-Time simulator and its capabilities to simulate power systems and attack scenarios, and to train students to use the general components and settings of the system. As mentioned in the next section, pre-designed models will be used to perform this task efficiently.

C. Course Syllabus

Teaching and supporting material were selected to reflect on the goals of the course and to cover the gaps found previously. In Table III, the course structure in the form of modules that cover the different topics, is presented. Noting that one module is typically covered in two lectures.

TABLE III. COURSE STRUCTURE

Module and Goals	Material
Module #1 **Fundamentals of Smart Grids** To learn about: 1. Smart Grid Infrastructure 2. Cyber-physical Systems	• **Pre-reading material** 1. "Ready or not, here comes the smart grid!" 2. "Smart grids: A cyber–physical systems perspective" 3. "Smart grid for a sustainable future" • **Main Material and handouts** "Smart Grids Infrastructure Technology and Solutions"
Module #2 **Cybersecurity and Operational Security in Smart Grids** To learn about: 1. Cybersecurity fundamentals 2. Operational security 3. Smart Grid Security	• **Pre-reading material** 1. "Cyber-security in smart grid: Survey and challenges" 2. "Cyber-security on smart grid: Threats and potential solutions" 3. "Cyber-physical systems security: Limitations, issues and future trends" • **Main Material and handouts** "Applied Cyber Security and The Smart Grid"
Module #3 **IEC 61850 and IEC 62351** To learn about: 1. IEC 61850 grid communication standard 2. IEC 62351 security standard for IEC 61850	• **Pre-reading material** 1. "Overview of IEC 61850 and Benefits" 2. "IEC 61850 for power system communication" 3. "Iec tc57 wg15: Iec 62351 security standards for the power system information infrastructure" • **Main Material and handouts** "IEC 61850 Communication Protocol Manual"
Module #4 **Fundamentals of Real-Time simulation systems** To learn about: 1. Real-Time simulation systems	• **Pre-reading material** 1. "Review of real-time simulator and the steps involved for implementation of a model from MATLAB/SIMULINK to real-time." 2. "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed" 3. "Cyber security of a power grid: State-of-the-art" • **Main Material and handouts** "Real-time simulation technologies: Principles, methodologies, and applications"
Exercises and Lab #1 **Opal RT Simulator** To learn about: 1. Real-Time simulation systems	• **Main Material and handouts** "Opal RT user manual"
Exercises and Lab #2 **Exercises and case scenarios** To learn about: 1. Implementation and simulation	• **Main Material and handouts** Pre-designed models to run and test

D. Delivery Strategy

About the actual and detailed strategy of delivering the course, it goes as follows:

1. Course objectives and schedule are announced and communicated to participants.
2. A MOOC course page is created and hosted by one of the course hosting platforms (Moodle platform [46] is selected for this purpose following its rich features).
3. Guest access is enabled to allow enrollment of participants from other institutions, and continuing education professionals. Access will be approved by instructors after assessing pre-knowledge.
4. A repository of the course content is created and divided into modules that cover the different topics.
5. For each module, there is a section for a pre-reading material list that contains 2 to 3 general articles about the topic to be covered. This should be available and announced one week at least before the scheduled lecture.
6. Lectures' materials, e.g., presentations, handouts, and other supporting materials, are also designed and uploaded to the lecture's section one week beforehand.
7. A set of 3 to 4 short videos – 15 to 20 minutes each – covering the main topic of the lecture, is recorded, and published on the scheduled day of the lecture.
8. Simple pre-lecture quizzes consisting of 3 to 4 multiple choices, match, and true and false questions that cover the pre-reading material list, are designed.
9. Pre-lecture quizzes open on the scheduled lecture's time and last for 10 to 15 minutes.
10. To avoid any sort of plagiarism, it is advised to create a questions bank, thus questions would differ from one participant to another.

11. Quizzes' results should be considered as bonus points or count only for up to 5% of the course's grade.
12. At the scheduled time of the lecture, recorded videos are played and facilitated/supervised by course instructors who are present online. After each video, 10 to 15 minutes are given to questions and any discussions.
13. A game, simple competition, or a similar activity that is related to the lecture's topic, could be created on one of the gaming platforms, e.g., Kahoot [47] or similar ones, and played in the middle of the lecture. Points received are considered bonus points as well.
14. A forum that hosts different topics open for discussion is created. Topics can be defined beforehand or emerge as needed.
15. For assessment, like points 8, 9 and 10, a questions bank is created to cover the main material of the lecture. Questions should be of auto-graded type, i.e., multiple-choice, multiple selection, true and false, fill in the blank and so on.
16. 15 to 20 questions are randomly selected from the questions bank for the weekly quizzes.
17. Weekly quizzes are available one day after the lecture and for a period of a week. Once a quiz is open, it can be completed within a certain timeframe, e.g., 30 minutes. After that, the quiz cannot be taken or opened again.
18. Weekly quizzes should count for 60 to 70% of the course's final grade.
19. Regarding exercises and practical skills, 2 to 3 exercise sessions based on study cases and to conduct a supervised remote connection with the lab, are given at the second part of the course once theoretical background is established and covered.
20. Students are encouraged to try pre-designed models, to learn the general concepts and criteria regarding the system in place.
21. Finally, after the course completion, questions already existing in the questions bank can be reused to design an exam covering the whole content of the course, e.g., 50 to 60 questions that can be answered in 2 to 3 hours. The final exam contributes 30 to 40% of the course's final grade.

VI. Discussion and Challenges

Knowledge and awareness of cybersecurity operations are essential for the energy sector to mitigate incidents and disruption scenarios. Although many courses exist on different fields of cybersecurity, such specific domains are not well covered. The key issues that current courses face are, either they are more academic or more practical, however, offers that combine both are rarely found. To fix this gap by designing a MOOC course that covers this topic, it was found that the topic has more perspectives than the technical one. First, MOOC types were investigated carefully to find out which type is more suitable to deliver the content and how to adjust it to meet the objectives of the course. Second, back to basics, instructional design models provide the foundation for designing an effective course, therefore, before embarking on course design – whether traditional, online, or a MOOC – the ID model should be selected carefully. After defining the MOOC type and the ID type, designing a course is quite a straightforward process following the available guidelines.

Regarding implementation, we have encountered the following challenges:

1. Resources: MOOCs by default are open to a large number of students, therefore all side tasks of the course, e.g., evaluation, should be automated, to optimize resources and provide time for the more important tasks, e.g., mediation, discussion, and so.
2. Retention rate: Depending on the assigned resources, the targeted rate of retention should be adjusted. However, typically for courses with no contact teaching, it is difficult to achieve higher retention rates that match with analyzing and creating criteria.
3. Retaining students: One of the key issues online courses face is the low completion rate which is due to lack of interest, interaction, and assistance. This was solved by opting for supervised sessions, discussion forums, and the use of simple gamification practices to encourage engagement.
4. Technical challenges regarding exercises and tutorials: Real-Time simulators are not available in every organization as they are very costly. Moreover, they have limited user licenses so they cannot be used remotely by several users. Therefore, a Virtual Private Network (VPN) connection is being established, and time slots are being distributed upon needs to participants who want to connect remotely to the cyber-physical lab for practicing. To make the process more efficient and to allow more students to practice, pre-designed models are provided, thus participants can move forward to running models and trying the different configurations.

As of the time of this writing, the course is yet to be completed and deployed. After that, results of the last two phases of the DSR – evaluation and communication – methodology will be available, and accordingly any measures needed to improve the course will be considered.

VII. Conclusion and Future Work

This paper presents the roadmap for designing an effective MOOC that can fill the cybersecurity knowledge gap in the field of smart grids. It was found that:

1. MOOC are resource intensive if they try to imitate traditional contact courses, especially in specific topics as the one of this paper. Therefore, measures were taken to automate the educational process and to optimize resources, thus, to give more time for interaction and engagement.
2. Techniques such as flipped learning and gamification if well adjusted, they can provide such optimization and engagement required.
3. The retention rate cannot be the same as contact teaching.
4. By using techniques such as remote access and VPN, participants could practice and gain practical knowledge, thus creating a richer MOOC experience.

In continuation of this work and as a part of CC-RSG project, this course is generalized and a framework for cybersecurity education in smart grids will be developed.

Acknowledgment

CC-RSG project is funded by the Erasmus+ Strategic Partnership program. The European Commission is not responsible for the content of this publication.

REFERENCES

[1] European Technology Platform, European Commission, “Strategic deployment document for Europe electricity networks of the future”, April 2010.

[2] Elzinga, David. "Electricity system development: A focus on smart grids. overview of activities and players in smart grids." UNECE. www. unece. org/fileadmin/DAM/energy/se/pdfs/eneff/eneff_h. news/Smart. Grids. Overview. pdf, (2015).

[3] European Commission (2020). Europe investing in digital: the Digital Europe Programme.
https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[4] ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). https://www.itu.int/rec/T-REC-X.1205-200804-I/en

[5] Young, Susan, and Dave Aitel. The hacker's handbook: the strategy behind breaking into and defending networks. Auerbach publications, 2003.

[6] Vacca, John R., ed. Managing information security. Elsevier, 2013.

[7] Romanovs, Andrejs, et al. "State of the Art in Cybersecurity and Smart Grid Education." IEEE EUROCON 2021-19th International Conference on Smart Technologies. IEEE, 2021.

[8] Valliou, Maria, et al. "Strategy for Cybersecurity Education in Smart Grids." (2022).

[9] González-Manzano, Lorena, and Jose M. de Fuentes. "Design recommendations for online cybersecurity courses." Computers & Security 80 (2019): 238-256.

[10] Arora, Bela. "Teaching cyber security to non-tech students." Politics 39.2 (2019): 252-265.

[11] Peffers, Ken, et al. "A design science research methodology for information systems research." Journal of management information systems 24.3 (2007): 45-77.

[12] Kamsamrong, Jirapa, et al. "State of the Art, Trends and Skill-gaps in Cybersecurity in Smart Grids." (2022).

[13] Merriam, Sharan B., and Lisa M. Baumgartner. Learning in adulthood: A comprehensive guide. John Wiley & Sons, 2020.

[14] Becker, S. Adams, et al. NMC horizon report: 2017 higher education edition. The New Media Consortium, 2017.

[15] Shi, Yinghui, et al. "Examining interactive whiteboard-based instruction on the academic self-efficacy, academic press and achievement of college students." Open Learning: The Journal of Open, Distance and e-Learning 33.2 (2018): 115-130.

[16] Hall, Steven R., et al. "Adoption of active learning in a lecture-based engineering class." 32nd Annual frontiers in education. Vol. 1. IEEE, 2002.

[17] Kolb, David A. Experiential learning: Experience as the source of learning and development. FT press, 2014.

[18] Felder, Richard M., and Rebecca Brent. "Active learning: An introduction." ASQ higher education brief 2.4 (2009): 1-5.

[19] Felder, Richard M., and Rebecca Brent. "Cooperative learning." Active learning: Models from the analytical sciences 970 (2007): 34-53.

[20] Bergmann, Jonathan, and Aaron Sams. Flipped learning: Gateway to student engagement. International Society for Technology in Education, 2014.

[21] Keselman, Alla. "Supporting inquiry learning by promoting normative understanding of multivariable causality." Journal of Research in Science Teaching 40.9 (2003): 898-921.

[22] English, Mary C., and Anastasia Kitsantas. "Supporting student self-regulated learning in problem-and project-based learning." Interdisciplinary journal of problem-based learning 7.2 (2013): 6.

[23] Deterding, Sebastian, et al. "From game design elements to gamefulness: defining" gamification"." Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments. 2011.

[24] Lalley, J., and R. Miller. "The learning pyramid: Does it point teachers in the right direction." Education 128.1 (2007): 16.

[25] Carr, Sarah. "As distance education comes of age, the challenge is keeping the students." Chronicle of higher education 46.23 (2000).

[26] Means, Barbara, et al. "The effectiveness of online and blended learning: A meta-analysis of the empirical literature." Teachers college record 115.3 (2013): 1-47.

[27] Ward, Barbara. "The best of both worlds: A hybrid statistics course." Journal of Statistics Education 12.3 (2004).

[28] Ryan, Sarah, et al. "The effectiveness of blended online learning courses at the community college level." Community College Journal of Research and Practice 40.4 (2016): 285-298.

[29] Boelens, Ruth, et al. "Blended learning in adult education: towards a definition of blended learning." (2015).

[30] Jansen, Darco, and Robert Schuwer. "Institutional MOOC strategies in Europe." Status Report Based on a Mapping Survey Conducted in October-December 2014 (2015).

[31] L17 Kim, Sung-Wan. "MOOCs in higher education." Virtual learning (2016): 121-135.

[32] Fischer, Gerhard. "Beyond hype and underestimation: identifying research challenges for the future of MOOCs." Distance education 35.2 (2014): 149-158.

[33] Vardi, Moshe Y. "Will MOOCs destroy academia?." Communications of the ACM 55.11 (2012): 5-5.

[34] Palacios Hidalgo, Francisco Javier, Cristina A. Huertas Abril, and M. Gómez Parra. "MOOCs: Origins, concept and didactic applications: A systematic review of the literature (2012–2019)." Technology, Knowledge and Learning 25.4 (2020): 853-879.

[35] Osuna-Acedo, Sara, Carmen Marta-Lazo, and Divina Frau-Meigs. "From sMOOC to tMOOC, learning towards professional transference: ECO European Project [De sMOOC a tMOOC, el aprendizaje hacia la transferencia profesional: El proyecto europeo ECO]." Comunicar ART-2018-105258 (2018).

[36] Reigeluth, Charles M. "Instructional design: What is it and why is it." Instructional-design theories and models: An overview of their current status 1 (1983): 3-36.

[37] Spector, J. Michael. Foundations of educational technology: Integrative approaches and interdisciplinary perspectives. Routledge, 2015.

[38] Huang, Ronghuai, J. Michael Spector, and Junfeng Yang. Educational technology a primer for the 21st century. Springer, 2019.

[39] Brown, Abbie H., and Timothy D. Green. The essentials of instructional design: Connecting fundamental principles with process and practice. Routledge, 2015.

[40] Kopp, Michael, and Elke Lackner. "Do MOOCs need a special instructional design." EDULEARN14 Proceedings 71387147 (2014).

[41] Dietz-Uhler, Beth, Amy Fisher, and Andrea Han. "Designing online courses to promote student retention." Journal of Educational Technology Systems 36.1 (2007): 105-112.

[42] Faruque, MD Omar, et al. "Real-time simulation technologies for power systems design, testing, and analysis." IEEE Power and Energy Technology Systems Journal 2.2 (2015): 63-73.

[43] Popovici, Katalin, and Pieter J. Mosterman, eds. Real-time simulation technologies: Principles, methodologies, and applications. CRC Press, 2017.

[44] Poudel, Shiva, Zhen Ni, and Naresh Malla. "Real-time cyber physical system testbed for power system security and control." International Journal of Electrical Power & Energy Systems 90 (2017): 124-133.

[45] “SCALABLE and OPAL-RT Innovate Cyber-Physical Solution.” *Scalable Network Technologies,* 5 July 2017, www.scalable-networks.com/news/scalable-and-opal-rt-innovate-cyber-physical-solution.

[46] Rice, William, and H. William. Moodle. Birmingham: Packt publishing, 2006.

[47] Dellos, Ryan. "Kahoot! A digital game resource for learning." International Journal of Instructional technology and distance learning 12.4 (2015): 49-52.