




Review

Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes

Madhav Mukherjee , Ngoc Thuy Le, Yang-Wai Chow  and Willy Susilo 

Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2522, Australia; johnle@uow.edu.au (N.T.L.); caseyc@uow.edu.au (Y.-W.C.); wsusilo@uow.edu.au (W.S.)

* Correspondence: madhav@uow.edu.au

Abstract: As the demand for cybersecurity experts in the industry grows, we face a widening shortage of skilled professionals. This pressing concern has spurred extensive research within academia and national bodies, who are striving to bridge this skills gap through refined educational frameworks, including the integration of innovative information applications like remote laboratories and virtual classrooms. Despite these initiatives, current higher education models for cybersecurity, while effective in some areas, fail to provide a holistic solution to the root causes of the skills gap. Our study conducts a thorough examination of established cybersecurity educational frameworks, with the goal of identifying crucial learning outcomes that can mitigate the factors contributing to this skills gap. Furthermore, by analyzing six different educational models, for each one that can uniquely leverage technology like virtual classrooms and online platforms and is suited to various learning contexts, we categorize these contexts into four distinct categories. This categorization introduces a holistic dimension of context awareness enriched by digital learning tools into the process, enhancing the alignment with desired learning outcomes, a consideration sparsely addressed in the existing literature. This thorough analysis further strengthens the framework for guiding education providers in selecting models that most effectively align with their targeted learning outcomes and implies practical uses for technologically enhanced environments. This review presents a roadmap for educators and institutions, offering insights into relevant teaching models, including the opportunities for the utilization of remote laboratories and virtual classrooms, and their contextual applications, thereby aiding curriculum designers in making strategic decisions.

Keywords: cybersecurity; information applications in education; teaching models; pedagogical models; learning objectives; curriculum design



Citation: Mukherjee, M.; Le, N.T.; Chow, Y.-W.; Susilo, W. Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information* **2024**, *15*, 117. <https://doi.org/10.3390/info15020117>

Academic Editors: Raúl Igual and Inmaculada Plaza

Received: 15 January 2024

Revised: 31 January 2024

Accepted: 6 February 2024

Published: 18 February 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The cybersecurity skills gap is a widely acknowledged concern that has prompted extensive efforts to address it through reforms in the education sector, particularly through the adoption of advanced information applications like remote laboratories and virtual classrooms (e.g., Massive open online courses (MOOCs)). Yet, according to the International Information Systems Security Certification Consortium's (ISC2) Cybersecurity Workforce Study 2022 [1], the cybersecurity workforce skills gap has grown by 26% year on year to 3.4 million, while the workforce has grown by half of that rate at 11% year on year, standing at 4.7 million, making it a profession in dire need. The leading cause, indicated by 43% of respondents, is a lack of qualified talent [2]. Over 57% of organizations aim to mitigate this gap by investing in training and certifications. We have seen an increase in funding for courses, digital platforms and online learning environments related to cybersecurity and subjects related to cybersecurity awareness across all classrooms in higher education. Yet, there seems to be little done to address the underlying issues contributing to this skills gap.

The interdisciplinary nature of the field, along with the lack of standardization in the recent past, has been a deterrent to many entering the field. A lack of clearly defined learning pathways, job roles and requirements has made cybersecurity unattractive to potential professionals and learners. Furthermore, there is a discernible lack of unified comprehension around the makeup of the cybersecurity workforce and the skills associated with it, often addressed through interactive and flexible online modules. Notably, analogous cybersecurity job profiles ought to encompass an identical skillset [3,4]. This has been sought to be addressed by a multitude of organizations, esteemed universities and national bodies [5–7] via the deployment of cybersecurity education frameworks. Major frameworks [8,9] propose a standardization and taxonomy for key skills and competencies for a professional. Some frameworks go as far as to outline specific education pathways [10], often incorporating online learning tools.

Despite the abundance of established frameworks for cybersecurity education and their application, including online and remote learning technologies, there is a noticeable absence of research offering a comprehensive approach to tackling the root of the skills gap. In addition, research on the proponents of this skill gap is still not conclusive, yet various frameworks identify the requirements and shortcomings of the cybersecurity workforce, like retention, interest and career clarity to name a few. Establishing these causal factors is essential for identifying and implementing mitigators, which could be effectively addressed through educational reform at varying scales, including the integration of digital learning environments. While we have encountered numerous studies that have been conducted to guide educators in developing effective cybersecurity education models and curricula, to the best of our knowledge, these studies did not specifically tackle the misalignment with framework standards, nor did they consider different learning contexts in their meta-analysis, reviews and recommendations. Additionally, they failed to clearly explain how they addressed causal factors.

This research aims to review, restructure and modernize the knowledge available to education providers, assisting them in the pedagogical and instructional design of cybersecurity subjects. We accomplish this while being cognizant of the causal factors and optimal learning objectives, taking into account the unique constraints and barriers within each institution's learning context for the application of practical, real-time experiences in a controlled, virtual environment. This review offers an insight into teaching models that have demonstrated success in enhancing student outcomes. The previously mentioned cybersecurity skills frameworks serve as a foundation, providing insight into the causal factors of the skill shortage and highlighting the desired learning outcomes and objectives. They also offer context regarding topics, skill levels and industry demands, all geared toward addressing the recognized skill gap.

To inform our selection of models, we infer the learning objectives from cybersecurity skills and development frameworks from Europe, the European Cybersecurity Skills Framework [10], the National Institute of Standards and Technology, the National Initiative for Cybersecurity Education's Framework (NIST/NICE) [9] and other well-established cybersecurity educational frameworks. Each identifies the roles and skills required of a professional, and moreover, they provide guidance to support the identification of learning outcomes for teaching professionals.

Our research on the literature for teaching models for cybersecurity education helped us categorize different models based on their successful application in specific learning contexts, their aptitude to address the identified learning outcomes and objectives and their inclusion of features such as virtual and online classrooms and learning environments or platforms that resulted in positive outcomes. We analyzed multiple learning contexts and identified both the unique and common features of each model that contribute to positive learning outcomes. Additionally, we identified the models that address the desired learning objectives.

This research aims to present a context-aware roadmap for educators and educational institutions for cybersecurity curriculum design. It identifies the relevant educational objectives and presents various educational models in widely generalized learning contexts, making their applicability to education systems and online learning platforms more apparent and accessible. Each have shown success to a higher degree than traditional classroom approaches in addressing the framework-derived objectives. With further research, it can provide educators a context-aware roadmap for developing the appropriate education models and methods of instruction informing curriculum design aligned to popular cybersecurity education frameworks.

The rest of this paper is organized as follows. Section 2 discusses the scope and approach taken in the literature review process while highlighting the key steps and outcomes. Section 3 discusses some of the literature and inspiring works, highlighting the current educational landscape, similar works in the existing literature, a brief on the pedagogy in this field, a note presenting context with regard to the different industry standards and needs and the aims of this research. Section 4 discusses the prevalent cybersecurity educational frameworks which allow us to derive relevant learning objectives. Section 5 identifies and explores the literature on different teaching models applied to cybersecurity education. Section 6 discusses the validity of the identified learning objectives in designing cybersecurity curricula. Section 7 tabulates a comparative analysis of the strengths and weaknesses of the selected teaching models with relation to the identified learning objectives. It also discusses and recommends a contextual element of curriculum design guidance through the classification of learning contexts, evaluation of teaching models and decision support. Section 8 discusses the assumptions in this research, the limitations and shortcomings of this research and potential areas for future works to address. Finally, Section 9 concludes this research with a short overview of this review, some key findings and potential for the future.

2. Methodology

The steps outlined below and in Figure 1 provide a structured approach in conducting a literature review and Table 1 for identifying, evaluating and synthesizing the existing literature and evaluating and comparing effective teaching models that can be applied to cybersecurity.

Table 1. Phases and steps of the literature review process.

Phase	Step	Description	Results
Planning	Step 1	Identification of scope of literature review, exploration and identification of search terms for each aspect of literature review (exploratory research)	-
	Search Terms	Topic domain: ("review" + "cybersecurity education")	-
Exploration	Step 2	Preliminary synthesis of resultant research: identification of search categories	5832
	Search Terms	Frameworks: ("cybersecurity education" + "framework") Models of teaching: ("education model" + "cybersecurity education") Learning outcomes: ("cybersecurity skills gap")	5300 + 112 + 420
	Step 3	Review of filters, review of relevant related research, exploration per filter category, evaluation and tertiary search	675
Analysis	Step 4	Further drill down research	118
	Step 4.1	Sniff test selection and manual search	50
Review	Step 5	Synthesis of finding objectives, success factors, models of teaching, frameworks and alignment	-

Note: This table outlines the structured approach taken in the literature review process, highlighting the key steps and outcomes.



Figure 1. Phase-wise methodical approach.

This review is aimed at identifying the literature showcasing the various types of teaching models with the potential to include educational information systems, their effectiveness in cybersecurity education, their research parameters, and any gaps relating to the implemented model and its apparent research environment or context and to consolidate the researched literature based on relevance.

Through this, we conduct a focused search of academic databases, including Google Scholar, Scopus and IEEE Xplore. While narrowing our search using relevant search terms and keeping in mind inclusion and exclusion criteria, we identify the most relevant articles while maintaining a corpus of related research. As per our approach, this corpus was tabulated and filtered for relevance.

The steps in our systematic literature review and synthesis of our findings methodology are as follows.

2.1. Definition of Scope and Review Criteria

The process begins by defining the scope of the review and establishing the criteria for evaluating the relevance and quality of the studies. This step sets the boundaries of the review, including the specific aspects of cybersecurity education that will be examined. This includes removal of most articles touting cybersecurity awareness and not education.

2.2. Parsing Available Repositories

We then delve into various repositories such as Scopus, Scholar, IEEE Xplore, Elsevier and Springer to gather a broad spectrum of research articles. This step ensures that we do not overlook any significant research that could potentially contribute to our understanding of the topic. Here, we focus primarily on the topic domain while parsing Repos.

The primary source of information was Elsevier and Scopus at first, but that changed as we explored Google Scholar more and found a larger variety of studies related to the topic's domain.

2.3. Preliminary Synthesis of Resultant Research

Once we have a collection of relevant studies, we conduct a preliminary synthesis. This involves categorizing the studies based on their models and objectives, providing an initial overview of the patterns and trends in the research. We use key terms like "Frameworks", "Teaching Models" and "Learning Objectives".

This allows us to then filter our research as well, allowing us to find more related works and improve manual exploration with each filter. Furthermore, we can drill down or perform tertiary searches.

2.4. Further Drill Down Research

The fifth step involves further drill down research on identified patterns, commonalities or linkages. This could involve a deeper examination of the models and frameworks used in the studies, providing a more nuanced understanding of the research.

2.5. Selection Filters

The third step involves applying selection filters to the gathered studies. We focus on studies that fall within the scope of the selected education topic and have relevance based on the scope of applicability of the research. This includes considering the education level, in this case higher education, the available resources, applied models and the infrastructure and environment (scaffolding). We also consider the relevance based on the age of the research and keystone research, ensuring that we include both recent studies and those that have had a significant impact on the field.

2.6. Synthesis of Findings

The sixth step is the synthesis of findings. Here, we categorize the models based on scaffolding and environmental barriers, providing a clear and organized overview of the research findings.

2.7. Report Findings and Recommendations

In the seventh step, we report our findings and recommendations. This involves clearly communicating the results of our review, including the key patterns and trends identified, and providing recommendations based on these findings.

2.8. Identification of Gaps and Suggested Future Work

Finally, we identify gaps in the current research and suggest areas for future work. This step ensures that our review not only provides a comprehensive overview of the current state of research but also contributes to the future development of the field. We identify prevalent gaps, including areas where we feel there is a lack of research despite targeted searching.

This systematic approach ensures a comprehensive review of the literature and provides a solid foundation for understanding the current state of research in the field of cybersecurity education.

This enabled this research to identify a set of common findings, allowing us to tailor a roadmap for education providers based on this extensive review. This allows a general understanding of how to holistically approach curriculum design and what the major objectives and modes of delivery are that suit their context based on research.

3. Related Work

In this section, we delve into the related literature, providing context on the current landscape of cybersecurity education, similar works an analysis of pedagogical models, industry alignment and certification bodies and a note on the aims of this research.

3.1. Landscape of Cybersecurity Education

From works like that by Dini et al., 2023 [11], we learn that there is a well-known and ever increasing cybersecurity threat, and in turn, there is a dearth of cybersecurity professionals. The interdisciplinary nature of cybersecurity education has been a focal point in both academia and industry. With a rich tapestry of research available [12,13], there is an evident need for a more holistic approach, one that not only bridges the chasm between academia and industry but also ensures that educational curricula align with the benchmarks set by esteemed bodies like the ACM and NIST/NICE. This research aspires to be that bridge, offering educators and institutions a roadmap that is both aligned with renowned cybersecurity education frameworks and attuned to the unique challenges of diverse learning contexts and available technologies.

3.2. The Existing Literature

A multitude of articles have reviewed various cybersecurity education efforts [14,15]. However, a closer examination reveals discernible gaps. The research of Cabaj et al. in 2018 [16] on 21 master's programs provides insights into how universities structure their courses in terms of duration and content. While it touches upon the ACM's guidelines and alignment with identified knowledge and skill areas, it does not elaborate on how pedagogical models are selected or applied in different contexts. Stavrou's 2023 work [17] aligns with many findings in cybersecurity education and delves into the pedagogy, highlighting practical use cases of collaborative and mentoring models. Yet, it stops short of discussing the importance of model selection criteria, even though it outlines learning objectives with some degree of contextual application of framework guidelines.

A similar study conducted in the EU by Dragoni et al. in 2021 [18] focused entirely on whether current cybersecurity education across master's programs focused on teaching a more relevant form of cybersecurity, taking key information from cybersecurity frameworks and comparing them across 100 universities in 28 countries of the European Union. It assesses the effectiveness of the education models' application in universities and their alignment with the framework's identified standardized knowledge areas (KAs) and knowledge units (KUs). This criteria for comparison is also kept in mind but adapted, as it ascribes relevance based on whether an institute has made a significant portion of their cybersecurity knowledge units part of mandatory learning. Moreover, their research was aimed at the relevance and importance of a proposed conceptual mindset of having security built in. Yet, we can learn how widespread the adoption of said KAs and KUs are, as well as the primary focus areas of students and institutions. This can further be used to help assess how universities globally stand against a plethora of industry-aligned universities in Europe.

An interesting adaptation of the popularly chosen cybersecurity education model called gamification was adapted for a cybercompetition. In 2023, Balon, T. and Baggili, I. [19] talked holistically about the application of new tools and virtual learning systems as well as adaptability to the skill levels of their users. They suggested a systematized knowledge of attributes, like focus areas, learning outcomes, experience levels and competition types. These attributes could prove useful in various non-cybercompetition scenarios for cybersecurity education.

Esteemed bodies like the European Cybersecurity Organisation (ECISO), the Association for Computing Machinery (ACM) and the National Institute of Standards and Technology's National Initiative for Cybersecurity Education (NIST/NICE) have provided foundational guidelines. Still, the alignment of pedagogical models with these frameworks is not always seamless. Our exploratory search found limited evidence of research focus-

ing on the use of cybersecurity educational frameworks in curricular design, especially concerning the analysis of applied pedagogical models.

3.3. Analysis of Pedagogical Models

Research has spotlighted potential opportunities and pitfalls in various educational models, especially when it comes to attracting, retaining and preparing students for a career in cybersecurity [14,20,21]. Stavrou [17] emphasized that cultivating lifelong learning should be a priority in formal education for cybersecurity subjects. However, the alignment of this principle with established frameworks remains debated.

Approaches like those of Beuran et al. in 2018 [22] have showcased the merits of hands-on and experiential learning models, with platforms like CyRIS leading the charge, emphasising how these tools aid in practical, hands-on learning in cybersecurity and with technology, remote laboratories or virtual classrooms playing a role in the effectiveness of the educational models [23,24]. Yet, the efficacy of these models in diverse educational landscapes remains an open question. The pioneering work of Luo et al. in 2019 [25] on the gamified flipped classroom model demonstrates the potential of engagement-driven learning and the applicability of virtualized education systems. Still, its adaptability, especially within global frameworks like NIST/NICE, requires further exploration.

3.4. Industry Alignment and Certification Bodies

Notable industry leaders in the cybersecurity certification industry like the SANS Institute, (ISC)² and ISACA aligned their learning pathways with prevalent cybersecurity frameworks. These institutions provide tools to guide potential learners through established learning pathways, underscoring the importance of such alignment. In 2019, Suryotrisongko [26] further supported the global applicability of these frameworks, suggesting that they offer a blueprint for ensuring that educational curricula remain agile and responsive to the ever-evolving cybersecurity landscape. However, not every education provider can adapt to and adopt these roadmaps, as also seen in the 2021 work of Dragoni et al. [18]. This research aims to aid education providers in developing their curricula, offering background on the frameworks to align with and suggesting educational models that are both environment- and context-aware.

3.5. The Aim of This Research

While there's a plethora of research on the application of various teaching models in cybersecurity education, most works do not fully address their alignment with cybersecurity frameworks or consider the learning context or the available technologies. This research endeavors to fill this void, offering a generalized guideline to assist a myriad of education providers in crafting suitable educational pathways tailored to their unique contexts.

4. Cybersecurity Education Frameworks

Due to the cybersecurity skill gap, various national bodies and institutions have proposed or developed various frameworks and guidelines to uplift the current state of the industry [27].

Due to the marginally differing opinions in each, this research has identified three popular and globally recognized frameworks. It aims to establish their contributions as well as where we find similarities and differences between the three. This is to help identify the relevant skills or objectives for learning outcomes that are meant to guide education providers in their curriculum design.

4.1. NICE Framework

The National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity [9] introduces a lexicon of Knowledge, Skills, and Abilities (KSAs). By utilizing this standardized approach, educational institutions can more effectively align curricula with job pathways, ensuring students are well prepared for enterprise demands.

This alignment not only fosters a pipeline of students into cybersecurity careers but also enhances the attractiveness of academic programs in the field.

The framework, outlined in Figure 2, sets forth a proficiency measure, spotlighting crucial areas of focus and identifying workforce engagement gaps [28]. Its central goal is to transparently communicate industry requirements, enabling institutions to adapt to academic curricula accordingly. This adaptability, combined with the framework's ability to help educators identify pertinent topics and skills, enhances its overall effectiveness.

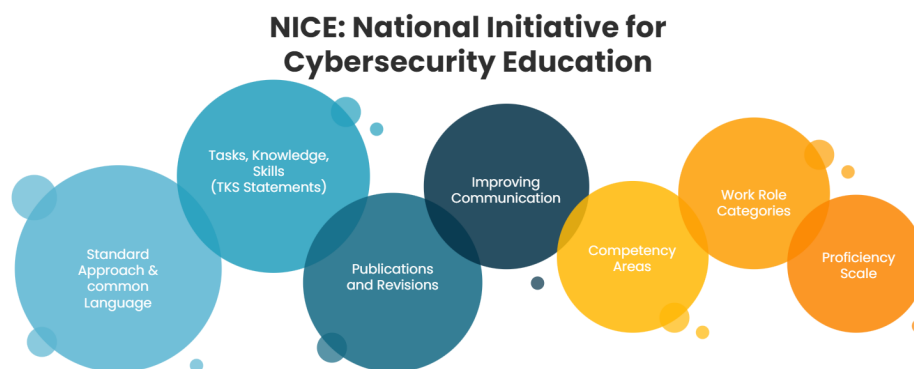


Figure 2. Core components of the NICE framework.

A key emphasis of the framework is student retention. It addresses the challenge faced by education providers in aligning with industry standards and effectively evaluating learners. With this framework in place, tailored curricula can be crafted to resonate with specific career trajectories, bolstering the retention of potential learners. Its standardized proficiency measures allow for meticulous monitoring of student progress, ensuring timely support when needed. This ensures that students are on track in acquiring vital skills for the cybersecurity realm. Additionally, the framework's lexicon simplifies the process for students, making the vast cybersecurity domain more navigable [29].

The NICE also hosts many workshops and conferences. Events like the workshop on “Using NICE Framework Competencies to Build a Better Cybersecurity Workforce” held in June 2022 and the NICE Conference & Expo [30] provide opportunities for educators, students and experts to meet. These gatherings allow for sharing ideas, effective methods and updates in cybersecurity education. The NICE framework, with its comprehensive tasks, knowledge and skills (TSKs), defined work roles and competency measure, allows education providers to standardize their approaches and bring transparency to potential learners. Furthermore, it promotes the enhancement of student retention, knowledge applicability and topic diversity. It facilitates institutions in their alignment with industry needs, equipping students for coveted roles. Through its proficiency measures and lexicon, the framework ensures a streamlined student progression and easier transition into the industry, laying the foundation for a resilient cybersecurity workforce.

4.2. ECSF Framework

The European Union Agency for Cybersecurity (ENISA) is an organization dedicated to achieving a high common level of cybersecurity across Europe, stating that to face the current cybersecurity threat landscape, we need a continuous process of collating, maintaining and communicating cybersecurity knowledge and having a specific aim of aligning that knowledge through the use of cybersecurity policy and operational cooperation [31].

In response to this, sponsored by the ENISA, professionals crafted the European Cybersecurity Skills Framework (ECSF), as seen in Figure 3, a tool meticulously crafted to facilitate the recognition and delineation of tasks, competences, skills and knowledge pertinent to their roles. In this research, we aim to provide a comprehensive understanding and present a condensed overview of this framework with specific objectives:

1. Assess the potential impact of the ECSF on standardizing cybersecurity education and training across Europe.
2. Explore methods through which the ECSF aims to connect professional workplaces with learning environments.
3. Explore the European Cybersecurity Skills Academy and how it plans to utilize the ECSF to tackle the cybersecurity talent shortage in the EU.

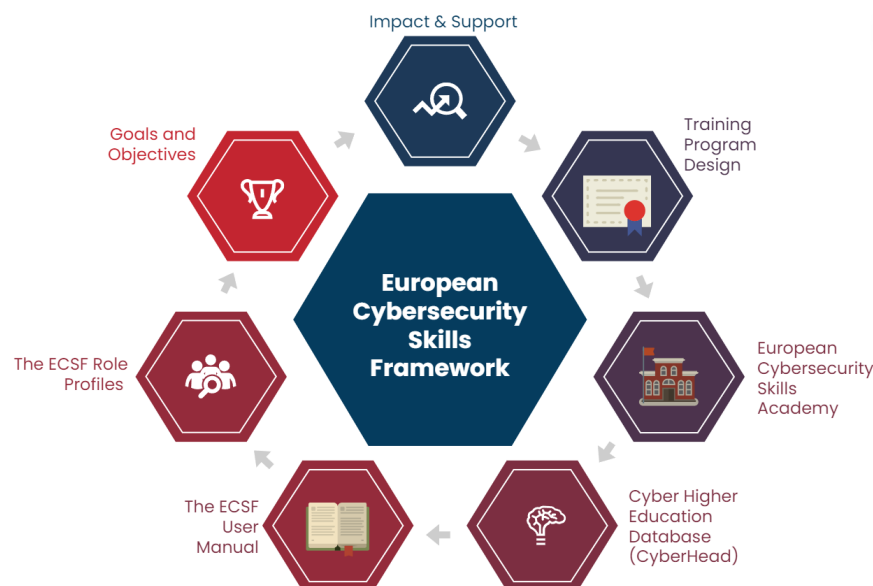


Figure 3. Core features of ECSF.

The ENISA states that, at present, within the European Union, there is a discernible lack of unified comprehension regarding the makeup of the cybersecurity workforce and the skills associated with it. Additionally, it hinders the development of education and training curricula and the creation of career paths that meet policy and market requirements for those looking to join the profession. They further stated that upskilling and reskilling the workforce often depends on cybersecurity training and certificates, which are typically provided by private companies [4]. They also noted how similar cybersecurity job profiles ought to encompass an identical skillset.

The framework is detailed in two documents: (1) *the ECSF Role Profiles document, which lists the 12 typical cybersecurity professional role profiles, and* (2) *the ECSF User Manual document, offering guidance on how to utilize the framework effectively.* Targeting education providers, the ECSF offers guidance to enhancing cybersecurity education in Europe. Section 3.2 of its manual underscores the framework's role for learning providers. It stresses student engagement and topic diversification in line with industry demands. Mirroring the NICE framework, the ECSF supports standardized proficiency measures for diligent student progress monitoring and support [4,32].

Furthermore, in 2023, its Communication on the Cybersecurity Skills Academy attempted to address the enforcement of policies aimed at improved coordination and the alignment of individual entities like the European Cybersecurity Competence Centre (ECCC), private organizations, the cybersecurity certifications industry and member states with similar initiatives.

These measures empower education providers to guide students toward mastering pivotal cybersecurity skills. The ECSF also accentuates student retention, aiming to boost student interest. By aiding universities in highlighting their cybersecurity programs' core areas, the framework ensures clarity and insight into potential career paths. The ECSF's implementation aids graduates' transition into cybersecurity roles, fostering confidence in potential students and benefiting the entire sector.

In conclusion, the ECSF significantly impacts cybersecurity education. It aligns curricula with industry, diversifies content and offers clear learning paths. With its proficiency measures, it monitors student advancement, ensuring skill adaptability across cybersecurity contexts. The ECSF cultivates a holistic learning space, championing student achievement and industry alignment.

4.3. ACM/IEEE: The Joint Task Force Cybersecurity Curricula 2017

This initiative, a collaboration between the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE), aimed to develop an updated cybersecurity curriculum addressing the evolving challenges of the field. Leveraging the expertise from both the ACM and IEEE, CSEC2017 offers guidelines for institutions to craft cybersecurity curricula in line with industry demands, ensuring future professionals are aptly prepared [8].

This primarily differs from earlier frameworks as it directly focuses on the education providers and the need for appropriate cybersecurity education as a supply for curbing the current skill gaps. It provides curricular recommendations based on their internally developed thought models. Furthermore, it uniquely identifies the characteristics of cybersecurity education programs and the content criteria for said education programs.

The characteristics of these cybersecurity education programs align with our findings, which focus on knowledge areas, cross-cutting concepts which are broadly applicable across a range of cybersecurity specializations and disciplinary lenses showing a direct relationship to the range of specializations meeting the workforce domains of the highest demand.

The CSEC2017 proposes a guideline to education providers in selecting the content of their curricula, as in Figure 4. The joint task force formed working groups per identified knowledge area in order to develop the knowledge units and categorized a few “essentials of cybersecurity” in each knowledge area. It proposes said topics as necessary foundations to be covered in each cybersecurity program while clearly stating the desired learning outcomes for each knowledge area.

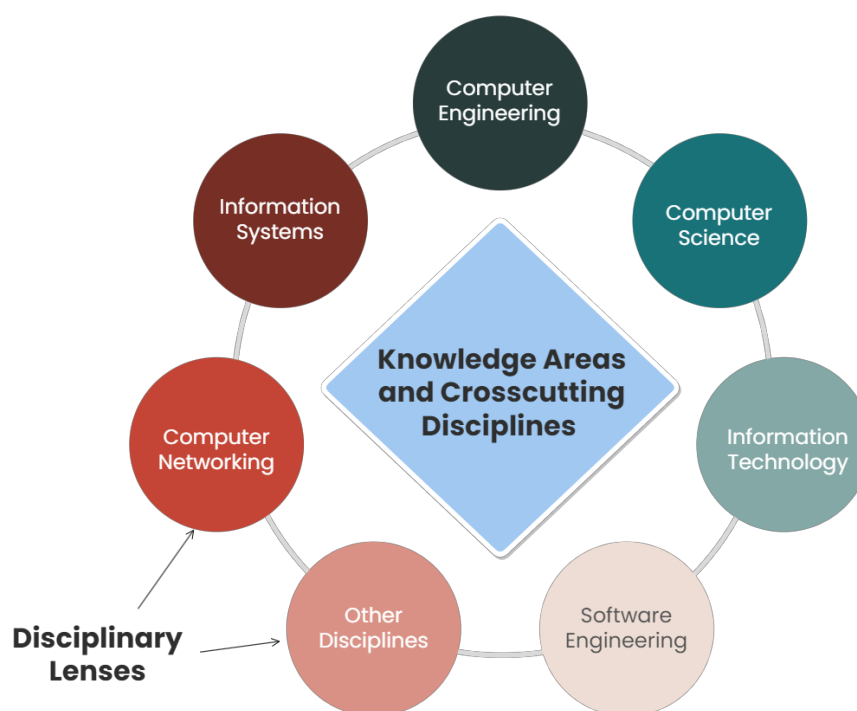


Figure 4. CSEC2017 thought model.

It further identifies areas where context comes into play while designing course curricula, where it is limited to the disciplinary lens and type of institution. The CSEC2017 primarily emphasizes the need to include essential theoretical and conceptual knowledge, as seen in Figure 5, as well as provide opportunities to develop practical skills as part of that knowledge, noting that adaptability is an important personality trait for cybersecurity professionals.

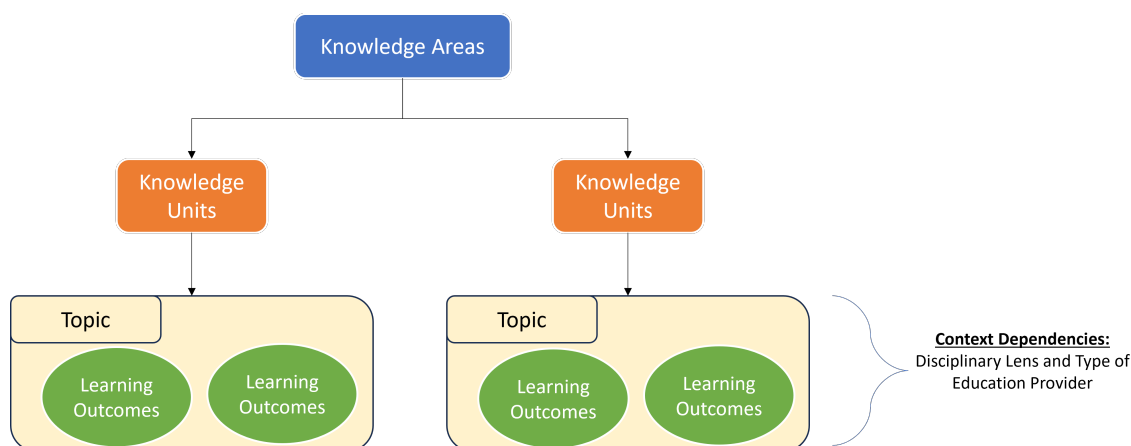


Figure 5. CSEC2017 curricula design hierarchy.

4.4. Comparative Analysis

Notably, there will undoubtedly be many similarities between cybersecurity-focused frameworks. Each of the selected frameworks either promote or imply a competency-based approach to their design and focus toward uplifting the cybersecurity skill gap.

Using insights from the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [33] and the Office of Personnel Management's (OPM) Hiring Cybersecurity Workforce report [34], this study pinpoints the essential skills and competencies. The European Cybersecurity Skills Framework (ECSF) further aids in identifying vital skill sets, promoting uniformity in cybersecurity education.

This research emphasizes the multidisciplinary nature of cybersecurity education as endorsed by the ECSF, NICE, and OPM. This holistic approach ensures adaptability, resilience and job readiness. The OPM's rotational strategy aids in cultivating versatile skills responsive to the dynamic cybersecurity landscape.

Yet, the skills gap in cybersecurity persists, being attributed to limited student engagement and knowledge retention [35]. This study outlines the factors behind this gap, suggesting objectives that address these while redefining cybersecurity education standards. These objectives, rooted in the NICE and ECSF frameworks, aim to nurture and retain adept cybersecurity professionals.

Upon evaluating various educational models, this study notes overlaps and gaps. By analyzing the distinct features of each model, it identifies the elements beneficial for desired learning outcomes, refining the educational approach by amalgamating the most effective aspects.

In summary, this research spotlights effective teaching models in cybersecurity education, drawing on Ghosh et al. (2021) [36] to provide an enriched view of contemporary cybersecurity education.

All frameworks agree that defined learning pathways and workforce roles can be achieved by way of standardization. This in turn brings clarity to the potential learners for a career pathway. It is therefore essential to also tailor education pathways based on the workforce roles.

The NICE framework, ECSF and CSEC 2017 share several foundational elements: they all (1) adopt a competency-based approach, (2) define workforce roles and learning paths, (3) formulate workforce development criteria, (4) emphasize standardization, (5) promote lifelong

learning and (6) incorporate a multidisciplinary approach. However, a notable distinction lies in the area of curriculum guidelines: *The CSEC 2017 framework includes specific curriculum guidelines, while the NICE framework and the ECSF do not.*

5. Education Models

Research on pedagogical models for cybersecurity education in higher institutions reveals diverse approaches [37,38]. While some works do not explicitly name a specific teaching model in use, many employ techniques intrinsic to certain pedagogical models, and each have some room to employ technologically enhanced teaching tools with a more realistic and “appropriate-to-model” approach. We summarize these identified models, detailing their criteria and key features. Further validity research helped with structuring and selecting the models described below.

5.1. Problem-Based Learning

Problem-based learning is a student-centric method where students tackle complex, open-ended problems [39]. They identify core issues and collaboratively devise solutions. As Yang et al. (2022) [40] noted, the educator transitions from a directive role to that of a facilitator, steering students through the problem-solving process while providing feedback and further assisting with help of technology which is adaptive and provides a collaborative learning environment.

Advocates for problem-based learning [41,42] emphasize its efficacy in honing critical thinking, problem-solving and communication skills. They also highlight its role in boosting students’ motivation and information retention, referencing Duch, Groh, and Allen’s findings from 2001 [43]. In problem-based learning, the focus remains on addressing specific problems, whereas in project-based learning, the emphasis is on project execution meeting set criteria.

However, problem-based learning is not without critiques. Shivapurkar et al. (2020) [42] pointed out its potential shortcoming in fully acquainting students with intricate, real-world cybersecurity challenges. This gap might hinder their comprehensive problem-solving abilities in real-world scenarios, which appropriate information tools would help address. Thus, integrating problem-based learning with other instructional strategies can offer students a more rounded learning experience.

5.2. Project-Based Learning

Project-based learning is an educational method where students work on a detailed project, applying their skills to address real-world challenges over an extended period. This method often involves designing and implementing problem solutions, with students ensuring their outcomes adhere to specific criteria. Typically, there’s an element of collaborative learning or hands-on experience which can be facilitated well by current online educational tools in a controlled environment.

Younis et al. (2021) [44] emphasized that project-based learning enhances soft skills and provides practical experience in team projects. Using provided resources, students collaborate, refining skills like decision making, planning and communication. This approach supports self-directed learning, reducing the emphasis on lecture-based instruction.

Vijayalakshmi et al. (2021) [45] viewed project-based learning as key in acquiring 21st century skills, particularly deepening conceptual understanding. This model promotes thorough exploration of topics via sustained inquiry, transitioning from a traditional teacher-focused approach to a more student-centered one, encouraging independent and active learning [46].

5.3. Hands-on Learning

Students participate in practical activities, applying their skills to tangible cybersecurity challenges such as penetration testing or cyber-attack simulations. While hands-on learning often overlaps with experiential or work-integrated learning, its core is typically

delivered within a classroom. This can however be enabled with technologies offering a controlled learning environment.

As highlighted by Wahsheh and Mekonnen in 2019 [47], hands-on learning often involves lab exercises where students translate lecture knowledge into simulated scenarios. Using controlled virtual settings, students grasp the practical aspects of cybersecurity concepts. Collaborations with companies can lead to virtual labs based on real scenarios, benefiting both learners and businesses.

The primary aim, according to Wahsheh and Mekonnen (2019) [47], is to utilize tools and knowledge to address intricate problems necessitating analytical skills. However, a significant limitation is the method's restricted exposure to real-world work practices, which can impact immediate employability in the cybersecurity domain. This is why it is frequently paired with experiential and work-integrated learning. Information tools like gameified or adaptive virtual learning environments can reduce the limitations of this model.

5.4. Experiential Learning

Experiential learning immerses students directly in the subject, using methods like simulations, internships or field trips. This enables students to apply theoretical knowledge in real-world contexts, enhancing skills through firsthand experiences.

A study by the University of South Wales, in partnership with the South Wales Cyber Cluster, Welsh government and industry collaborators, showcased the advantages of industry-driven projects in advancing students' cybersecurity understanding. This method lets students collaborate with industry experts, offering a more hands-on learning experience than conventional routes. As Johnson (2019) [48] noted, these projects inherently incorporated employability skills, making the learning more genuine and impactful and underscoring the significance of industry-centric learning for cybersecurity careers.

This learning style often encompasses work-integrated and embedded learning and is frequently combined with project-based and hands-on methodologies.

5.5. Flipped Classroom Model

This style of teaching is often simply mistaken with flexible learning. Here, the students receive course materials ahead of time or outside class hours, enabling self-paced learning and revisiting content when necessary. This model works best when technology-assisted.

Classroom sessions prioritize interactive discussions and activities to enhance knowledge retention. This model often integrates with other student-focused methods, moving away from teacher-led styles. It has been effective in blended and hybrid delivery modes, as noted by Rasheed et al. (2020) [49].

Bordel et al. (2021) [50] observed that this method addresses challenges like varied student backgrounds, potential student attrition due to personal frustrations and the high costs of learning resources. By not relying solely on weekly lectures, it offers broader tool access. The approach has proven to deepen understanding, boost retention and improve student satisfaction and academic outcomes.

5.6. Case-Based Learning

This involves presenting students with a real-world problem or scenario and having them analyze and solve the problem using the knowledge and skills they learned in class, typically during a small time window. Here, students may be asked to evaluate different options and choose the best course of action based on the information provided. This differs from project-based learning as that involves completing a more extended project that requires collaboration, research and multiple stages of problem solving. However, due to similar elements, the methods are often used concurrently. Adaptive technological learning tools have been reportedly used to enable virtual collaboration in applications of this model [51].

According to Ahmad et al. (2021) [52], case-based learning prompts critical discussion, elicits pertinent experiences from students, fosters an inquiry into accepted practices and establishes a connection between theory and practice through constructive dialogues.

Through the course of this study, various modern teaching methodologies, ranging from collaborative to flipped classroom models, can be adapted to delivery in any blended learning environment. We identify various teaching models and how they relate to our learning objectives. Namely, we aim to address areas that undermine the persistence of education and student resilience, leading to eventual professional longevity.

6. Identification of Objectives

This research acknowledges the growing demand from institutions and corporations for certified professionals as an alternative or supplement to traditional university education [21,53]. It challenges the previous assumption that the prevailing skill gap was attributed to a lack of learning opportunities in higher education institutes [54], which caused many to turn to professional training providers [3]. Consequently, it sheds light on the industry's diminishing trust in the adequacy of university education and hence their preparedness to face a need for additional training and development.

Our approach first identifies broad-spectrum solutions to mitigate the factors that led to a decline in student education across various fields. We then narrow down our focus to those aspects which address the challenges that undermine student resilience, persistence and eventual professional longevity in the field of cybersecurity. This approach allows us to safely identify a set of educational objectives that can significantly improve learner outcomes.

6.1. Validation of the Identified Objectives

Struyf et al. (2019) [55] underscored the pivotal role of student engagement in fostering positive academic outcomes. Yet, Arora and Mendhekar (2020) [54], alongside a survey from the National Cybersecurity Alliance and Raytheon Corporation Communications (2017) [56], indicated that millennials, despite heightened awareness, remain largely disengaged from cybersecurity pursuits. This disengagement, as the survey elucidates, is attributed to factors such as diminished interest and a limited grasp of cybersecurity nuances. Further research focused on these factors [57,58], as highlighted by Masten et al. (2022) [59], emphasizes that fostering robust student engagement is paramount in cultivating resilience, thereby equipping students with resources to navigate adversities.

Branoff et al. (2022) [60] articulated the imperative of academic support and efficacious instructional strategies in bolstering student retention in undergraduate programs. They advocated for augmenting traditional methods with resources like targeted tutoring and mentorship. Concurrently, Masten et al. (2022) [59] delved into the indispensable role of resilience factors in the educational landscape.

The salience of knowledge retention in the realm of cybersecurity education is undeniable, especially given the field's ever-changing nature. Effective retention and the subsequent application of knowledge not only bolster student engagement but also enhance employability and sustained interest in the domain. Prioritizing knowledge retention is pivotal to ensuring a competent and adept cybersecurity workforce.

The transposability of cybersecurity pedagogical methodologies across diverse educational contexts is of paramount importance. As delineated in ECSO (2017) [3], an adaptable educational paradigm can cater to the multifaceted needs of a diverse student populace, thereby fortifying knowledge retention and preparing students to adeptly navigate the multifarious challenges of cybersecurity.

Lastly, championing a diversified approach to cybersecurity education was advocated by the ECSO (2017) [3] and Blažič (2021) [35] to ensure alignment with the industry's needs. Such an approach equips students to confront the myriad challenges inherent in cybersecurity. However, a perspective highlighted by the ECSO (2017) [3] suggests a tilt toward specialized higher education, relegating broader educational pursuits to

professional training entities. We generated a set of goals that were derived from the learners' objectives and the motivations behind previous works while also taking into consideration the present-day requirements of the industry.

6.2. Identified General Model Learning Objectives

- **Student engagement:** We aim to address the overall attention, intrinsic motivation and interactivity of the student base in relation to the taught subject.
- **Student retention:** This aims to address the pervasive problem of dropouts and professional aversion to the industry.
- **Knowledge retention:** This refers to the transferability of knowledge to the learner and their ability to grasp the concepts and analyze and apply them [61] in the later stages of their careers with or without continuity of exposure.
- **Diversification and multi-disciplinary:** Here, we mean the diversity of concepts that can be taught with a particular model effectively, where a multi-disciplinary field like cybersecurity can have certain aspects taught fairly well with one methodology while other methods can be hindered within those parameters. For example, intrusion prevention and detection taught using hands-on learning will have a much better result in student outcomes than if taught using a theory-based flipped classroom approach.
- **Transferability and transposeability of a model:** This is the extent to which the effect of a particular model can be replicated in another setting. This can include considerations of financial resources, infrastructure resources, time the and mode of instruction.

7. Findings and Recommendations

7.1. Model Analysis

The evaluation of cybersecurity education models, as shown in Table 2, involves assessing their efficacy in key objectives like student engagement, retention, persistence, knowledge retention, diversification and transferability. By examining the impact of various models on these objectives, we can pinpoint areas for enhancement and strategize how to optimize student learning experiences tailored to specific learning contexts. Such insights are invaluable for educators and policymakers aiming to bolster cybersecurity education in an ever-evolving domain. Moreover, the effectiveness of these models can be further scrutinized based on their adaptability to different educational environments.

Table 2. Summary of learning objectives aligned with various frameworks.

Learning Objectives	NICE Framework	ECSF	CSEC2017
Student engagement	Highlights real-world applicability and competency-based methods.	Emphasizes workforce perspectives and skills.	Requires active student engagement.
Student retention	Stresses evolving competencies in dynamic cybersecurity.	Highlights sustained curriculum engagement for career goals.	Emphasizes student retention.
Knowledge retention	Focuses on continuous learning in cybersecurity.	Emphasizes retaining essential cybersecurity skills.	Stresses knowledge retention.
Diversification and multidisciplinary	Recognizes multidisciplinary cybersecurity needs.	Suggests a diversified curriculum.	Advocates a multidisciplinary approach.
Transferability and transposeability of the model	Suggests a flexible, adaptable curriculum.	Indicates a flexible curriculum for diverse needs.	Emphasizes curriculum adaptability.

Note: This table provides a comparative overview of different educational frameworks and their alignment with key learning objectives.

It is evident that no single model addresses all learning objectives comprehensively. For instance, while experiential and hands-on learning significantly bolster student engagement and preparedness, they do not impact knowledge and student retention as effectively as the flipped classroom model. Our goal is to offer a framework to assess these

models, identifying adaptable components that, when combined, can holistically address all learning outcomes.

7.2. Common Findings

Through our comprehensive review, partially seen in Table 3, we discovered that the degree of effectiveness in achieving the desired learning outcomes varied across the selected teaching models. Another major factor we find necessary to be cognizant of is the learning context, which includes the method, the medium and the resources available to the students and the institute [23]. However, in reviewing each model, each showed some degree of success in satisfying one or more of the identified objectives.

Table 3. Comparison of teaching models.

Teaching Model	Advantages	Disadvantages
Problem-based learning	Student engagement: Active participation in real-world problems. Knowledge retention: Enhances understanding through problem-solving. Diversification: Applicable to various topics in cybersecurity.	Resource needs: May require more resources and specialized facilitators. Student retention: Can be overwhelming without foundational knowledge.
Project-based learning	Student engagement: Involvement in projects boosts motivation and collaboration. Knowledge retention: Practical application improves long-term retention. Diversification: Tailorable to various cybersecurity topics.	Resource intensity: Can be resource-intensive and not feasible in all settings.
Hands-on learning	Student engagement: Direct interaction enhances interest and motivation. Knowledge retention: Practical experience enhances understanding. Diversification: Effective for technical aspects of cybersecurity.	Resource requirements: Needs specific tools and set-ups and is not available everywhere.
Experiential learning	Student engagement: Learning through experiences is highly engaging. Knowledge retention: Real-world experiences enhance memory retention. Diversification: Applicable to various aspects of cybersecurity.	Replicability: Challenging to replicate in different settings due to unique experiences.
Flipped classroom model	Student engagement: Engage with materials at their own pace before class. Ease of implementation: Easily implemented in various settings with minimal resources.	Content limitations: Some complex topics might not be effectively conveyed.
Case-based learning	Student engagement: Real-world cases boost interest and relevance. Knowledge retention: Analyzing cases improves understanding and application. Diversification: Tailorable to various cybersecurity scenarios.	Case study availability: Requires access to relevant and updated case studies.

Note: This table provides a comparative analysis of various teaching models in cybersecurity education, highlighting their respective advantages and disadvantages.

Through our review, we learned that there are overarching must-haves in order to successfully address all the nuances and differentiating gaps of the learning objectives:

- Exposure to a variety of topics:
 - o A multi-disciplinary approach is deemed imperative for a truly work-ready graduates in cybersecurity, a multidisciplinary field.
 - o This has the added benefit of ensuring learners are cognizant of the various roles in cybersecurity and their tasks and requirements.
 - o This exposes students to various avenues of pursuit should they seek advancement in a particular field of interest or specialization. This can be a further education pathway or pursuit of a specific role in the industry.

This aligns with the impetus behind the definition of learning pathways and skills within each of the reference frameworks.

- Application-based learning opportunities:
 - o To be considered work-ready for a field like cybersecurity requires comprehension of the relevant areas, and this is best demonstrated through the following:
 - Application of previously learned topics;
 - Hands-on tasks;
 - Work-integrated learning opportunities.

This is meant to simplify aligning with the competency requirements defined in each reference framework.

- Compatibility and suitability: In different learning contexts, one may find specific aspects of each model and mode of delivery enticing to their own needs, but the primary criteria should be the following:
 - o Compatibility of a model to the mode of delivery;
 - o Suitability of the model to the subject matter, classroom size and overall learning context.

This is where most frameworks fall short, as they are too generalized to address the varying barriers and opportunities across learning contexts. Through this review, our work will aggregate these learning contexts based on the level of educational support and based on the material and environmental limitations of the learner and education provider.

In order to support education providers, we developed a simple roadmap, Figure 6, that utilizes these findings and produces supporting material to facilitate the decision-making process.

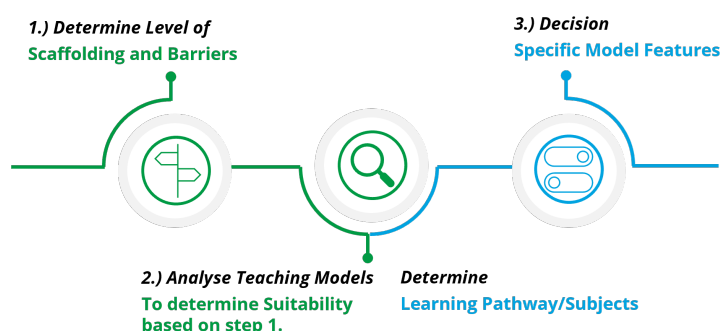


Figure 6. Course design roadmap.

7.3. Determine the Level of Scaffolding and Barriers

From our firm understanding that not all models are suitable across various learning contexts, we could synthesize a series of sets of teaching models over an aggregation of the summarized learning contexts, as in Table 4. This was based on two primary factors: one being the level of support available to each learner, such as the infrastructure, resources, learning support and engagement, which we refer to as scaffolding [62,63], and the other

being material and environmental factors like location, class size and lack of governmental support, which we refer to as barriers. Catota et al. (2019) [64] listed a series of potential barriers in emerging countries, which can be likened to the potential barriers faced by most learners globally, with differing levels of impact.

Furthermore, we suggest a simple scale from low to high in order to classify context in a binary fashion, allowing education providers the ability to make quick determinations and navigate the nuances themselves.

Table 4. Categorization of learning environments based on scaffolding and barriers.

Scaffolding and Barrier Levels	Environment Description	Example
Low scaffolding, low barriers	Minimal teacher guidance or educational support is given or needed, and there are few challenges.	A self-directed online course on basic cybersecurity skills available for a low cost on a platform like Coursera or Khan Academy.
Low scaffolding, high barriers	Minimal teacher guidance or educational support is given or needed, but there are significant challenges.	A workshop on cybersecurity skill development offered in a remote town with limited infrastructure and resources.
High scaffolding, low barriers	High level of teacher guidance or educational support is provided, and there are few challenges.	An education provider in an urban area offering guided bootcamps for beginners with ample support and resources.
High scaffolding, high barriers	High level of teacher guidance or educational support is provided, but there are significant challenges.	A cybersecurity training program by a top tech company focusing on advanced topics with a rigorous selection process and high tuition fees.

Note: This table categorizes different learning environments based on the combination of scaffolding and barriers, providing a clear understanding of how teaching models can be adapted to various contexts.

7.3.1. Low Scaffolding, Low Barriers

Here, the environments have minimal teacher guidance or educational support given or needed, and there are few challenges to overcome in effectively implementing the teaching model. An example of a low scaffolding and barriers learning context is a self-directed online course on basic cybersecurity skills available for a low cost on a platform like Coursera or Khan Academy. Here, students can learn at their own pace without much guidance, and there are minimal barriers to access the content.

7.3.2. Low Scaffolding, High Barriers

This includes environments where minimal teacher guidance or educational support is given or needed, but there are significant challenges that might hinder the effective implementation of the teaching model, such as a workshop on cybersecurity skill development offered in a remote town. While the workshop encourages independent exploration and does not provide much guidance, the barriers are high due to the lack of infrastructure, limited access to computing resources and potential language barriers.

7.3.3. High Scaffolding, Low Barriers

This environment has a high level of teacher guidance or educational support provided, and there are few challenges to overcome in effectively implementing the teaching model. This can be ascribed to a situation where an education provider in an urban area offers guided bootcamps for beginners, with mentors available for assistance. This environment provides a lot of support and guidance, and there are minimal barriers to participation since it is easily accessible and offers resources like computers and internet access. The potential cost barrier may be levied.

7.3.4. High Scaffolding, High Barriers

This environment has a high level of teacher guidance or educational support provided, but there are significant challenges that might hinder the effective implementation of the teaching model. Although seemingly rare, a situation such as this would be similar to a cybersecurity training program offered by a top tech company focusing on advanced topics. While the program provides in-depth guidance, hands-on training and access to industry experts, it has a rigorous selection process, high tuition fees and might require participants to relocate or have specific prior certifications.

7.4. Evaluating the Teaching Models

We analyzed the various teaching models to determine their suitability based on the previously identified levels of scaffolding and barriers.

This method is aimed at simplifying the process of determining the mode of teaching adaptive learning, the use of remote or virtual classrooms for blended learning, collaborative learning environments, assessment and feedback mechanisms and professional certifications with industry alignment. As such, educators and institutions are encouraged to consider these findings in their curriculum design and teaching strategies, easily adapting to leverage the benefits of technological advancements in education.

7.5. Decision

The provided supporting tables and roadmap allow one to make a quick selection based on the context and determine the likeliest models to suit that context.

One can further analyze the type of education pathway they want to provide and align the model best suited for the development of those skills and attract learners:

- If the environment has low scaffolding and low barriers, then prioritize problem-based learning, project-based learning and case-based teaching.
- If the environment has low scaffolding and high barriers, then consider avoiding hands-on learning, experiential learning and the flipped classroom model.
- If the environment has high scaffolding and low barriers, then most models are suitable, with a special emphasis on models that require the necessary resources.
- If the environment has high scaffolding and high barriers, then be cautious with all models and consider the specific barriers before implementation. Models like the flipped classroom model work well when the education material is provided, and there are geographical barriers or physical barriers.

8. Limitations

This paper remains ignorant to subjective external deterrents or proponents like mental health, domestic stability and familial support. Furthermore, while addressing the integration of advanced technology in education, such as remote laboratories and virtual classrooms, it does not delve deeply into the specific challenges and opportunities these technologies present in the cybersecurity education context. This is a review primarily intended for post-secondary education providers and the like to analyze the applicability and impact certain educational models, including technology-enhanced methods, can have on cybersecurity education over a normalized population within specific learning contexts.

Furthermore, the literature review process followed various facets, not allowing full exploration of all combinations of model frameworks and learning outcomes. This can benefit from further meta analysis. We propose alignment with specific countries' standardized knowledge areas and knowledge units in cybersecurity education, providing empirical evidence of relevant case studies and choosing more informative success metrics.

This research could be expanded to conduct a comprehensive study on the impact of various learning contexts on this model, especially those involving advanced information applications in education. However, a more beneficial approach would be to further this research by assessing and incorporating the features of each teaching model, which are well documented in terms of learning outcomes and characteristics, into a unified course curriculum that optimally leverages technology. This curriculum could be tailored to best fit the learning context of each higher education institution and learner, with a special emphasis on the effective integration of remote laboratories, virtual classrooms and other digital tools.

Moreover, an in-depth evaluation of the integration of work-integrated learning and professional certification into the course curriculum should be considered, particularly in terms of their feasibility and effectiveness in technology-enhanced learning contexts. This would also include assessing the integrability of such tools with the chosen teaching model, as well as exploring the unique challenges and benefits that come with the adoption of these advanced educational technologies.

There is also the scope to explore the potential impact of generative AI on the application of educational and informational technologies used in a cybersecurity higher-education classrooms.

9. Conclusions

This research meticulously examined the frameworks that underpin educational institutions and professional certification programs, ensuring alignment with the evolving demands of the cybersecurity industry. Through our analysis, distinct learning objectives can be extrapolated from these guiding frameworks, each of which has been substantiated through relevant research within the domain, presuming the integrability of advanced technological tools in educational settings.

Moreover, a variety of pedagogical models, each demonstrating notable success in the realm of cybersecurity education, were identified, partly based on their effectiveness and applicability in technology-enhanced environments. These models, characterized by their unique attributes, were chosen based on the ubiquity of their application in online, in-person and remote learning contexts and their empirically validated efficacy. Furthermore, they advocate for a curriculum that embraces the potential of digital platforms to provide comprehensive, accessible and engaging learning experiences.

Ultimately, an in-depth evaluation of each model's capacity to achieve the previously delineated learning objectives was presented, offering a concise overview of their respective merits. Ultimately, this research elucidates the evolving integration of these frameworks into academic curricula, serving as a valuable resource for curriculum designers. It is hoped that this study will inspire further exploration into the effective use of technology in cybersecurity education, given the holistic context, and encourage educators to adopt innovative approaches that align with the dynamic nature of this field.

Author Contributions: Conceptualization, M.M., N.T.L., Y.-W.C. and W.S.; methodology, M.M.; validation, M.M., N.T.L., Y.-W.C. and W.S.; formal analysis, M.M.; investigation, M.M.; writing—original draft preparation, M.M.; writing—review and editing, M.M., N.T.L. and Y.-W.C.; visualization, M.M.; supervision, N.T.L., Y.-W.C. and W.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

ISC2	International Information Systems Security Certification Consortium's
MOOCs	Massive open online sources
NIST	National Institute of Standards and Technology's
NICE	National Initiative for Cybersecurity Education's Framework
IEEE	Institute of Electrical and Electronics Engineers
ACM	Association for Computing Machinery
CSEC2017	ACM/IEEE Joint Task Force Cybersecurity Curricula 2017
ECISO	European Cybersecurity Organisation
ECSF	European Cybersecurity Skills Framework
OPM	Office of Personnel Management
CyRIS	Cyber Range Instantiation System
SANS	SysAdmin, Audit, Network, and Security
ISACA	Information Systems Audit and Control Association
KSAs	Knowledge, skills and abilities
TSKs	Tasks, knowledge and skills
ENISA	The European Union Agency for Cybersecurity
ECCC	European Cybersecurity Competence Centre

References

- ISC2. Cybersecurity Workforce Study 2022. 2022. Available online: <https://www.isc2.org/research> (accessed on 16 May 2023).
- European Cybersecurity Organisation. European Cybersecurity Education and Professional Training: Minimum Reference Curriculum. 2022. Available online: https://ecs-org.eu/ecso-uploads/2022/12/2022_SWG5.2_Minimum_Reference_Curriculum_final_v3.0.pdf (accessed on 16 May 2023).
- European Cybersecurity Organisation. Gaps in European Cyber Education and Professional Training. 2017. Available online: <https://ecs-org.eu/ecso-uploads/2022/10/5fdb282a4dcdbd-1.pdf> (accessed on 16 May 2023).
- ENISA. About ENISA. 2019. Available online: <https://www.enisa.europa.eu/about-enisa> (accessed on 16 May 2023).
- Australian Computer Society. Cybersecurity Pathway Chart. Available online: <https://www.acs.org.au/content/dam/acs/acs-documents/ACS-CP-CyberSecurity-Pathway-Chart.pdf> (accessed on 16 May 2023).
- Skills Framework for the Information Age. Information and Cyber Security. Available online: <https://sfia-online.org/en/sfia-8/sfia-views/information-and-cyber-security?path=/glance> (accessed on 16 May 2023).
- Communication on the Cybersecurity Skills Academy. 2023. Available online: <https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy> (accessed on 13 April 2023).
- Cybersecurity Curricula 2017: Curriculum Guidelines for Undergraduate Degree Programs in Cybersecurity. Technical Report Draft Version 0.5, ACM Joint Task Force on Cybersecurity Education. 2017. Available online: <http://www.csec2017.org/csec2017-v-0-5> (accessed on 16 May 2023).
- Newhouse, W.; Keith, S.; Scribner, B.; Witte, G. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*; U.S. Department of Commerce: Gaithersburg, MD, USA, 2017; NIST Special Publication, Volume 800-181 Revision 1.
- European Cybersecurity Skills Framework (ECSF). 2023. Available online: <https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework> (accessed on 16 May 2023).
- Dini, P.; Elhanashi, A.; Begni, A.; Saponara, S.; Zheng, Q.; Gasmi, K. Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity. *Appl. Sci.* **2023**, *13*, 7507. [CrossRef]
- Workman, M.D.; Luévanos, J.A.; Mai, B. A study of cybersecurity education using a present-test-practice-assess model. *IEEE Trans. Educ.* **2021**, *65*, 40–45. [CrossRef]
- Beuran, R.; Chinen, K.I.; Tan, Y.; Shinoda, Y. *Towards Effective Cybersecurity Education and Training*; Japan Advanced Institute of Science and Technology: Ishikawa, Japan, 14 October 2016.
- Kim, E.; Beuran, R. On designing a cybersecurity educational program for higher education. In Proceedings of the 10th International Conference on Education Technology and Computers, Tokyo, Japan, 26–28 October 2018; pp. 195–200.
- Tamur, M.; Mandur, K.; Pereira, J. Do combination learning models change the study effect size? A meta-analysis of contextual teaching and learning. *J. Educ. Expert.* **2021**, *4*, 1–9.
- Cabaj, K.; Domingos, D.; Kotulski, Z.; Respício, A. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Comput. Secur.* **2018**, *75*, 24–35. [CrossRef]
- Stavrou, E. Planning for Professional Development in Cybersecurity: A New Curriculum Design. In Proceedings of the International Symposium on Human Aspects of Information Security and Assurance, Kent, UK, 4–6 July 2023; pp. 91–104.
- Dragoni, N.; Lafuente, A.L.; Massacci, F.; Schlichtkrull, A. Are we preparing students to build security in? A survey of European cybersecurity in higher education programs. *IEEE Secur. Priv.* **2021**, *19*, 81–88. [CrossRef]

19. Balon, T.; Baggili, I. Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education. *Educ. Inf. Technol.* **2023**, *28*, 11759–11791. [CrossRef] [PubMed]
20. Hajny, J.; Ricci, S.; Piesarskas, E.; Levillain, O.; Galletta, L.; De Nicola, R. Framework, tools and good practices for cybersecurity curricula. *IEEE Access* **2021**, *9*, 94723–94747. [CrossRef]
21. Conklin, W.A.; Cline, R.E.; Roosa, T. Re-engineering cybersecurity education in the US: An analysis of the critical factors. In Proceedings of the 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 6–9 January 2014; pp. 2006–2014.
22. Beuran, R.; Pham, C.; Tang, D.; Chinen, K.I.; Tan, Y.; Shinoda, Y. Cybersecurity education and training support system: CyRIS. *IEICE Trans. Inf. Syst.* **2018**, *101*, 740–749. [CrossRef]
23. Nweke, L.O.; Bokolo, A.J.; Mba, G.; Nwigwe, E. Investigating the effectiveness of a HyFlex cyber security training in a developing country: A case study. *Educ. Inf. Technol.* **2022**, *27*, 10107–10133. [CrossRef] [PubMed]
24. Baldassarre, M.T.; Santa Barletta, V.; Caivano, D.; Raguseo, D.; Scalera, M. Teaching Cyber Security: The HACK-SPACE Integrated Model. In Proceedings of the ITASEC, Pisa, Italy, 13–15 February 2019.
25. Luo, Z.Y.; Wang, J.Y.; Sun, G.L.; Chen, Y.D. Research on Gamification Teaching of “Network Security Technology” Under Improved Flipping Classroom. In Proceedings of the International Conference on E-Learning, E-Education, and Online Training, Kunming, China, 18–19 August 2019; pp. 36–47.
26. Suryotrisongko, H.; Musashi, Y. Review of cybersecurity research topics, taxonomy, and challenges: Interdisciplinary perspective. In Proceedings of the 2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA), Kaohsiung, Taiwan, 18–21 November 2019; pp. 162–167.
27. AlDaajeh, N.; Saleous, N.; Alrabae, S.; Barka, E.; Breiting, F.; Choo, K.K.R. The role of national cybersecurity strategies on the improvement of cybersecurity education. *Comput. Secur.* **2022**, *119*, 102754. [CrossRef]
28. Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework Table of Contents. 2023. Available online: <https://www.nist.gov/system/files/documents/2023/10/05/NIST%20Measuring%20Cybersecurity%20Workforce%20Capabilities%20207-25-22.pdf> (accessed on 9 October 2023).
29. NIST. Events | NICE | Conference and Expo. 2023. Available online: <https://niceconference.org/events/> (accessed on 9 October 2023).
30. Mouheb, D.; Abbas, S.; Merabti, M. Cybersecurity curriculum design: A survey. In *Transactions on Edutainment XV*; Springer: Berlin, Germany, 2019; pp. 93–107.
31. The SANS Institute. Cyber Security Skills Roadmap | SANS Institute: Cyber Security Skills Roadmap. 2019. Available online: <https://www.sans.org/cyber-security-skills-roadmap> (accessed on 16 May 2023).
32. Wetzel, K. NICE Framework Competency Areas: National Institute of Standards and Technology. 2023. Available online: <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8355.pdf> (accessed on 16 May 2023).
33. Petersen, R.; Santos, D.; Smith, M.C.; Wetzel, K.A.; Witte, G. Workforce Framework for Cybersecurity (NICE Framework). National Institute of Standards and Technology. 2020. Available online: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf> (accessed on 22 March 2023).
34. Workforce Planning for the Cybersecurity Workforce. U.S. Office of Personnel Management. Available online: <https://www.opm.gov/policy-data-oversight/human-capital-management/cybersecurity/> (accessed on 22 March 2023).
35. Blažič, B.J. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Educ. Inf. Technol.* **2021**, *27*, 3011–3036. [CrossRef]
36. Ghosh, T.; Francia, G., III. Assessing Competencies Using Scenario-Based Learning in Cybersecurity. *J. Cybersec. Priv.* **2021**, *1*, 539–552. [CrossRef]
37. Xia, P. Exploration on Open Practice Teaching Mode of Network Security Based on Cultivation of Innovative Talents. In Proceedings of the International Conference on Applications and Techniques in Cyber Security and Intelligence, Fuyang, China, 20–22 June 2020; pp. 172–179.
38. Sánchez, J.; Mallorquí, A.; Briones, A.; Zaballos, A.; Corral, G. An integral pedagogical strategy for teaching and learning IoT cybersecurity. *Sensors* **2020**, *20*, 3970. [CrossRef]
39. Yew, E.H.; Goh, K. Problem-based learning: An overview of its process and impact on learning. *Health Prof. Educ.* **2016**, *2*, 75–79. [CrossRef]
40. Yang, J.; Rae Kim, Y.; Earwood, B. A Study of Effectiveness and Problem Solving on Security Concepts with Model-Eliciting Activities. In Proceedings of the 2022 IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 8–11 October 2022. [CrossRef]
41. Strobel, J.; Van Barneveld, A. When is PBL more effective? A meta-synthesis of meta-analyses comparing PBL to conventional classrooms. *Interdiscip. J. Probl.-Based Learn.* **2009**, *3*, 44–58. [CrossRef]
42. Shivapurkar, M.; Bhatia, S.; Ahmed, I. Problem-based Learning for Cybersecurity Education. *J. Colloq. Inf. Syst. Secur. Educ.* **2020**, *7*, 6.
43. Duch, B.J.; Groh, S.E.; Allen, D.E. *The Power of Problem-Based Learning: A Practical “How To” for Teaching Undergraduate Courses in Any Discipline*; Stylus Publishing, LLC: Sterling, VA, USA, 2001.
44. Younis, A.A.; Sunderraman, R.; Metzler, M.; Bourgeois, A.G. Developing parallel programming and soft skills: A project based learning approach. *J. Parallel Distrib. Comput.* **2021**, *158*, 151–163. [CrossRef]

45. Vijayalakshmi, M.; Raikar, M.M. Development of Network Applications and Services Through Project-Based Learning to Meet 21st Century Skills. In Proceedings of the 2021 IEEE Global Engineering Education Conference (EDUCON), Vienna, Austria, 21–23 April 2021. [\[CrossRef\]](#)
46. Sherman, A.T.; Peterson, P.A.H.; Golaszewski, E.; LaFemina, E.; Goldschen, E.; Khan, M.; Mundy, L.; Rather, M.; Solis, B.; Tete, W.; et al. Project-Based Learning Inspires Cybersecurity Students: A Scholarship-for-Service Research Study. *IEEE Secur. Priv.* **2019**, *17*, 82–88. [\[CrossRef\]](#)
47. Wahsheh, L.A.; Mekonnen, B. Practical Cyber Security Training Exercises. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019. [\[CrossRef\]](#)
48. Johnson, C. University of South Wales national cyber security academy—Creating cyber graduates who can ‘hit the ground running’: An innovative project based approach. *High. Educ. Pedagog.* **2019**, *4*, 300–303. [\[CrossRef\]](#)
49. Rasheed, R.A.; Kamsin, A.; Abdullah, N.A.; Kakudi, H.A.; Ali, A.S.; Musa, A.S.; Yahaya, A.S. Self-Regulated Learning in Flipped Classrooms: A Systematic Literature Review. *Int. J. Inf. Educ. Technol.* **2020**, *10*, 848–853. [\[CrossRef\]](#)
50. Bordel, B.; Alcarria, R.; Robles, T.; Martin, D. Flipped classroom and educational videos to improve the cybersecurity competencies in future computer engineers. In Proceedings of the EDULEARN, 13th International Conference on Education and New Learning Technologies, IATED, Virtual, 5–6 July 2021. [\[CrossRef\]](#)
51. Fernández-Caramés, T.M.; Fraga-Lamas, P. Use case based blended teaching of IIoT cybersecurity in the industry 4.0 era. *Appl. Sci.* **2020**, *10*, 5607. [\[CrossRef\]](#)
52. Ahmad, A.; Maynard, S.B.; Motahhir, S.; Anderson, A. Case-based learning in the management practice of information security: An innovative pedagogical instrument. *Pers. Ubiquit. Comput.* **2021**, *25*, 853–877. [\[CrossRef\]](#)
53. Fortinet. 2022 Cybersecurity Skills Gap—Fortinet. 2022. Available online: <https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf> (accessed on 16 May 2023).
54. Arora, A.; Mendhekar, A. Innovative Techniques for Student Engagement in Cybersecurity Education. In *Data Management, Analytics and Innovation*; Springer: Singapore, 2020; pp. 395–406. [\[CrossRef\]](#)
55. Struyf, A.; De Loof, H.; Boeve-de Pauw, J.; Van Petegem, P. Students’ engagement in different STEM learning environments: Integrated STEM education as promising practice? *Int. J. Sci. Educ.* **2019**, *41*, 1387–1407. [\[CrossRef\]](#)
56. Communications, R.C. Raytheon: Fifth Annual Survey by Raytheon, Forcepoint and NCSA Finds Young Adults’ Interest in Cybersecurity Careers Stagnant-Oct 24, 2017, Raytheon News Release Archive. Available online: <https://raytheon.mediaroom.com/2017-10-24-Fifth-annual-survey-by-Raytheon-Forcepoint-and-NCSA-finds-young-adults-interest-in-cybersecurity-careers-stagnant> (accessed on 16 May 2023).
57. Bezanilla, M.J.; Fernández-Nogueira, D.; Poblete, M.; Galindo-Domínguez, H. Methodologies for teaching-learning critical thinking in higher education: The teacher’s view. *Think. Ski. Creat.* **2019**, *33*, 100584. [\[CrossRef\]](#)
58. Asim, H.M.; Vaz, A.; Ahmed, A.; Sadiq, S. A Review on Outcome Based Education and Factors That Impact Student Learning Outcomes in Tertiary Education System. *Int. Educ. Stud.* **2021**, *14*, 1–11. [\[CrossRef\]](#)
59. Masten, A.S.; Nelson, K.M.; Gillespie, S. Resilience and Student Engagement: Promotive and Protective Processes in Schools. In *Handbook of Research on Student Engagement*; Springer International Publishing: Cham, Switzerland, 2022; pp. 239–255. [\[CrossRef\]](#)
60. Branoff, T.; Mohammed, J.; Brown, J. The role of spatial visualization ability in course outcomes and student retention within technology programs. *J. Geom. Graph* **2022**, *26*, 159–170.
61. Ramsoonder, N.K.; Kinnoo, S.; Griffin, A.J.; Valli, C.; Johnson, N.F. Optimizing Cyber Security Education: Implementation of Bloom’s Taxonomy for future Cyber Security workforce. In Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020. [\[CrossRef\]](#)
62. Collins, A.; Brown, J.S.; Holum, A. Cognitive apprenticeship: Making thinking visible. *Am. Educ.* **1991**, *15*, 6–11.
63. Matsuo, M.; Tsukube, T. A review on cognitive apprenticeship in educational research: Application for management education. *Int. J. Manag. Educ.* **2020**, *18*, 100417. [\[CrossRef\]](#)
64. Catota, F.E.; Morgan, M.G.; Sicker, D.C. Cybersecurity education in a developing nation: The Ecuadorian environment. *J. Cybersecur.* **2019**, *5*, tyz001. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.