Addressing the Necessity of CyberSecurity Literacy: The case of ETTCS CyberTeach Project

Journal:	*Information and Computer Security*
Manuscript ID	ICS-04-2024-0095.R1
Manuscript Type:	Original Article
Keywords:	Cybersecurity, Cybersecurity Literacy, ETTCS Project, LMS

SCHOLARONE™
Manuscripts

Addressing the Necessity of CyberSecurity Literacy: The case of ETTCS CyberTeach Project

***Abstract*—The concept of Cybersecurity literacy has become increasingly crucial in recent years, as the digitization of most human activities is being completed within the framework of the 4th Industrial Revolution. Almost all devices, vehicles, and services in the near future will be interconnected to the Internet and operate on advanced computing platforms. The benefits of these technological advancements are evident, as are the potential risks. To this end, organized cybercriminals, black hat hackers, and state-sponsored actors may attempt, through various cyber-attacks, to steal personal data, cause road accidents in connected autonomous vehicles and in general disrupt critical infrastructures. Cybersecurity is a growing concern when it comes to digitalization and cloudification. This way, digital assets must be conveniently protected in order to avoid any concern about their confidentiality, integrity and authentication. Therefore, the ability of every citizen to use the Internet and smart devices wisely and securely is one of the most fundamental skills they should possess. In this work, we present actions and initiatives, developed within the scope of the ETTCS CyberTeach Erasmus Project, to enhance cybersecurity literacy through innovative digital content and contemporary LMS platform. A new approach to teach cybersecurity, based on innovative teaching methods, is presented in order to prepare future citizens and their teachers to keep up with CyberSecurity issues in an efficient manner. To this end, we propose ways to reach CyberSecurity literacy, giving use case examples and proposing the necessary digital skills.**

I. Introduction

Ctybersecurity is becoming one of the most important factors in digital transformation. The 4th Industrial Revolution impacts all aspects of modern life, both personally and professionally. Smart buildings and smart cities offer a variety of new environmentally friendly services to residents. Self-driving vehicles provide safe and relaxing commutes for travelers. Modern 5G networks ensure high-speed connectivity for everyone, everywhere. New medical equipment with sufficient computational power and networking capabilities provides better and more effective healthcare treatment. The revolution in Artificial Intelligence (AI) is largely responsible for these achievements. The benefits of digitalization for humanity are self-evident. Unfortunately, most people fail to understand the potential hazards and threats posed by these permanently connected devices with significant processing power, which serve as the backbone of our daily activities.

The common denominator of all these significant achievements is their dependence on a new generation of smart devices with sophisticated specifications and powerful characteristics. In other words, powerful processors and complex software applications are responsible for acquiring data from various sensors, analyzing it, and executing a set of predefined directives. The unseen outcome of the wide adoption of smart devices and their interconnection through the continuously expanding Internet of Things (IoT) is the substantial increase of the attack surface from hackers and other malicious actors [1]. Despite their critical life-supporting function, medical devices are prone to numerous well-known vulnerabilities [2]. Similarly, smart homes are facing comparable cyberthreats [3], [4], and autonomous vehicles cannot be considered secure against cyberattacks [5], [6].

The increase in cyberthreats is evident across all aspects of Information and Communication Technologies (ICT). The latest generation of processors comprises billions of transistors, leading to an unprecedented level of complexity. These aggressively optimized architectures generate a growing number of vulnerabilities that can be exploited to extract sensitive data [7], [8]. Similarly, modern operating systems and platforms consist of tens of millions of lines of code, while most applications range from tens of thousands to hundreds of thousands of lines of code. Consequently, numerous bugs are present in the most popular software programs [9], [10], making them susceptible to exploitation by cybercriminals.

Over the past years, most cybercriminals have become especially adept at performing lucrative cyberattacks. The surge in ransomware incidents, in particular, demonstrates that cybercrime has become more *organized* and *professional*, targeting high-value entities. The trend to attack better-protected entities (often businesses) rather than simple individuals (a.k.a. soft targets), underscores the capabilities of modern cybercriminals. They are willing to invest more effort and accept higher risks if it is associated with greater rewards. It is well-documented that on the Deep Web and various Black Markets, a wide range of cybercriminal services are available for hire. The *Cybercrime-as-a-Service* model, ensures that various cybercriminal groups have compartmentalized their operations according to their skills, aiming to maximize their efficacy and stay ahead of the cyberdefense community.

The paper is organized as follows. Section 1 introduces the need for Cybersecurity Literacy due to the shortage of experts in the cybersecurity sector. Section 2 presents the related works, in various efforts to teach and raise awareness in cybersecurity in the educational sector. Section 3 discusses the methodology of our work, focusing on the use case and the good practices aquired by the ETTCS Cybersecurity Project, while Section 4 provides concluding remarks and outlines future work.

Information and Computer Security

II. Related Works

The lack of cybersecurity professionals is so severe that various alternative approaches are currently being explored, both inside and outside of academia. The US National Security Agency (NSA) has established Centers of Academic Excellence in collaboration with prominent Universities. While this initiative was crucial when it was launched, today, most Computer Science curricula, include at least one cybersecurity class, though it is questioned where that is sufficient to lay the foundation for future cybersecurity professionals [11]. The significance of cybersecurity has become so evident that many Universities now exclusively offer master's degrees in this field. The benefits of cybersecurity integration within Information Technology (IT) education have been extensively substantiated in scholarly literature. Nevertheless, an ongoing discourse persists regarding the imperative to disseminate cybersecurity knowledge across the vertical spectrum of the curriculum, rather than confining it solely to designated cybersecurity courses [12].

The role of professional bodies and technical organizations, such as ISACA (Information Systems Audit and Control Association), (ISC)², SANS Institute, and OWASP, is of crucial importance. They provide hands-on knowledge and create comprehensive platforms and specialized tools for both professionals and educational purposes [13]. The contribution of the aforementioned professional organizations to the education of their members through certifications and provided educational programs is highly significant. There are more than 100 certifications, directly or indirectly related to cybersecurity, and their number is constantly increasing. These certifications are designed to be completed within a relatively short period of time and to focus on a specific specialized subject within cybersecurity. They are primarily aimed at recent graduates from Computer Science and Software Engineering departments who wish to enhance their resumes, as well as experienced professionals in the IT field who seek to update their knowledge and specialize in a more contemporary area within cybersecurity. The value of these certifications is evident; however, their large number needs thorough evaluation for the selection of the most suitable ones, both in terms of subject matter and quality.

In addition, an alternative way of promoting cybersecurity is through various exercises that are open to the public. These exercises target either young individuals to introduce them to cybersecurity or IT security professionals who can update their knowledge, learn state-of-the-art methodologies, and network with their colleagues. Some well-known cybersecurity exercises include the US Cyber Challenge, CyberPatriot, NetWars, and the Cyber Security Treasure in the US [14]. In Europe, most countries organize their own cybersecurity exercises, such as the Panoptis National Cyberdefense program [15], which brings together academics, computer security professionals, and military personnel working with information systems. At the pan-European level, ENISA is responsible for raising awareness and organizing cybersecurity exercises on a larger scale [16].

Scientific and research organizations bring together academics and researchers working in the field of Information System Security, shaping the goals for future research. Additionally, numerous academic publications and scientific conferences demonstrate the significance of cybersecurity both within academia and society. Some of the most significant scientific organizations, specifically the Association for Computing Machinery (ACM), the IEEE Computer Society (IEEE-CS), the Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8), collaborated on the Joint Task Force on Cybersecurity Education to prepare the Cybersecurity Curricula 2017 [17]. This serves as an indicative recommended curriculum guide for academic institutions. It constitutes a specialization of the updated ACM Computing Curricula 2005 Report (CC2005) that is utilized by university departments in computer science, computer engineering, information systems, information technology, and software engineering.

One of the most systematic interagency initiatives to initiate a comprehensive security program was the NICE (National Initiative for Cybersecurity Education) program, which was led by the NIST (National Institute of Standards and Technology) [18]. The program was executed in conjunction with academia, the private sector and other branches of the government. The aim of this initiative was to develop workforce with sufficient cybersecurity skills for the US government and the private sector. On the other hand, in the United Kingdom the situation is fluid. More than 85 universities offer undergraduate and graduate degrees in cybersecurity, but only 61% of UK include mandatory cybersecurity material. More alarming, the more diversified computer programs do not require any cybersecurity course at all [19]. The situation is becoming more challenging as there is also a shortage in cybersecurity professors.

Recently, it has become more evident that a key element in achieving satisfactory cybersecurity education for younger generations, is to train teachers and their educators. Researchers highlight the case of Ukraine, which has suffered numerous cyberattacks in the past months. As a result, it was necessary to update teachers and educators to further raise awareness of cybersecurity issues. The proposed approach builds upon the existing cybersecurity initiative in the EU and suggests a blended method to educate teachers. This method utilizes self-education, group training, and practical applications [20]. The benefits of having cybersecurity aware teachers has been document in other studies [21]. The preparation of teachers to deliver cybersecurity courses or to integrate cybersecurity into other existing courses poses significant difficulties and requires a solid methodological plan [22].

Additionally, an outline on the worldwide shortage of cybersecurity experts, a brief study on current e-learning platforms has been carried out, as well as another one about women's role in cybersecurity, whose main points are presented in the following subsections.

For Peer Review Only

A. Worldwide Shortage of Cybersecurity Experts

The increasing number of cyberattacks highlights the critical situation, faced not only by IT systems, but also by technologically advanced Nations. Moreover, recent military conflicts like the Russia-Ukraine one and geopolitical tensions between China and the USA, have exposed a wide array of highly sophisticated state-sponsored cyberattacks. High-ranking government officials in the US have expressed concerns about the lack of an adequate number of cybersecurity experts, which poses a clear threat to National security. Similarly, the EU is grappling with a shortage of skilled cybersecurity professionals, leading to significant consequences. Many medium and large businesses in the European Union (EU) struggle to find qualified personnel to fill cybersecurity positions. To address this shortage and safeguard financial competitiveness and National security, it is imperative to undertake organized and coordinated efforts to attract talented individuals to the cybersecurity sector [23].

That report provides comparative data between the EU and the US, which verify that the lack of cybersecurity professionals is a global phenomenon. Therefore, it is expected to be a competition among Nations to attract cybersecurity professionals, even among the EU states. The European Union Agency for Cybersecurity (ENISA), has already highlighted the need to address the Cybersecurity Skills Shortage (CSS) [24]. The document examines the efforts of EU Member States to train IT professionals with the required cybersecurity skills, as well as the different approaches adopted by EU Member States to mitigate the shortage and gap in the cybersecurity workforce. To support students and professionals, seeking to enhance their knowledge and skills in cybersecurity, the EU has created the Cybersecurity Higher Education Database (CyberHEAD). This database includes Bachelor's and Master's degree programs and educational programs in general offered in EU Member States.

The ISC2 Cybersecurity Workforce Study conducted a comprehensive global analysis [25], revealing a staggering worldwide shortage of 3.4 million cybersecurity professionals. Specifically in Europe, the shortage of cybersecurity experts is notable, with Germany alone requiring an additional 104,197 experts, France needing 60,859, and Spain seeking 60,436. Even smaller countries like Ireland face a significant deficit, necessitating over 8,481 cybersecurity workers. The global competition for attracting cybersecurity talent is intense. In the United States, the demand for IT security personnel stands at 410,695, while Mexico requires another 203,027, contributing to an estimated global cybersecurity workforce gap of 312,852. The deficiencies in China and India are of immense proportions, with shortages of 1,482,085 and 563,364 cybersecurity professionals respectively. As highlighted in the same report, the lack of adequate cybersecurity expertise presents a substantial risk to organizations.

The Global Cybersecurity Outlook 2022 Insight Report, by the World Economic Forum [26], highlights another crucial aspect of the shortage in the cybersecurity field—specifically, the scarcity of cybersecurity executives. This dearth of qualified executives poses difficulties in understanding the imperative of investing in human capital for cybersecurity, ultimately resulting in potential negative impacts for organizations. ESG's report confirms these findings and highlights the difficulties for various companies to hire mid-career and senior cybersecurity professionals.

B. e-Learning open platforms for Cyber security

To start with, an Integrated Learning Environment (ILE) may be defined as *a portal providing a comprehensive solution of online learning services*, where a Learning Management System (LMS) is the key component, which is not only devoted to content and resource management, but it may also be equipped with other complementary tools such as conferencing, collaboration or learning analytics [27]. There are a bunch of LMS dedicated to teach cybersecurity, although many of them does not provide free access. Some of the most interesting platforms offering courses for free in the cybersecurity field are listed as follows [28]:

1) *EdApp* is a platform for educational purposes, with a course library related only to cybersecurity courses, which could be taken as originally designed, or otherwise, they could be customized according to different needs. Moreover, microlearning programs are also available, and also bite-size lessons in just some minutes. It provides interesting features as a creator tool, reporting, analytics and achievements.
2) *Coursera* is a platform with a wide range of courses, including many of them related to cybersecurity, which are developed by reputable companies and educational institutions. Some of the courses are free, although many of them are offered on a paid basis.
3) *FutureLearn* is another educational platform offering cybersecurity courses, where all its cybersecurity courses are offered for free. Some of the cybersecurity courses are designed by higher education institutions, such as Open University or Coventry University.
4) *ESET* is an antimalware solution, which also has an e-learning platform with courses aimed at cybersecurity awareness for free, where they present their own expertise in the field, even though some of the courses go under paid plans.

All of the LMS cited above could be considered as general purpose e-learning platforms, even though they offer a collection of cybersecurity courses. However, there are a few LMS in the market which are just focused on digital literacy, not only on cybersecurity. Digital Literacy Portal [29] presents a range of courses related to cybersecurity. There are nine courses available, where each of those cover a specific objective related to computer science, which is split in a group of specific topics. Those courses are available in different European languages, such as English, Spanish or Turkish. Cybersecurity LMS (CyLMS) is an open-source set of tools, which integrates the training on cybersecurity with existing LMS platforms, such as Moodle, which may well be the most

For Peer Review Only

widely used LMS. Hence, the features furnished by CyLMS allow trainers to turn a general-purpose LMS into a specific platform to teach cybersecurity topics [30].

Besides, KYPO Cyber Range Platform (KYPO CRP) is an open-source software, run as a cloud-based solution composed of virtual machines (VM) to emulate infrastructures, networks and applications. This tool proposes a collection of scenarios devoted to attack and defense different machines, simulating exercises for red team and blue team, where users must have certain knowledge and skills to get this training done [31]. Additionally, there are some commercial platforms offering cybersecurity learning services in a similar way, where some contents could be accessed for free and some other could be done through a subscription fee. Those could be categorized as cloud-based hosted platforms and self-hosted platforms. Some instances of the former are *HackTheBox, TryHackMe, Root-Me, PentesterLab, and Virtual Hacking Lab (VHL)*, whereas some examples of the latter are *OWASP Juice Shop (OJS), CTFd, PicoCTF, and TinyCTF* [32].

In summary, there is a variety of platforms offering training courses related to cybersecurity, although some of those are not exclusively focused on the topic of cyber security learning, whereas some others are aimed at skilled users and not so much to beginners, while others are not open source. Therefore, the proposal of this project could be considered as innovative in the market, because it combines a set of elements not being present in the rest of platforms reviewed, at least to the best of our knowledge. Those elements are the creation of a specific open source platform only for cybersecurity training with the focus in offering cybersecurity courses on an incremental basis, thus moving from beginner to intermediate and advanced level. Hence, the novelty of our proposal is the combination of those three elements: *open source platform, only cybersecurity training, range of cybersecurity courses for different types of users*.

Focusing on comparing the solution proposed with the other cybersecurity education programs quoted, it is to be noted that EdApp platform provides a wide range of options to customize content into courses. However, it does not have neither the design nor the multimedia power of the brand-new ETTCS platform, which allows for a user experience which makes a difference. Alternatively, the Coursera platform offers a wide range of predefined courses offered by international institutions, such that the courses have a fixed content, so it could not be updated unless the course editor provides a new version of it. However, those updates take time to have it done, as Coursera depends on each particular editor to update a given course. Furthermore, the courses furnished in this platform either do not cover much of the content provided by the ETTCS courses, or otherwise, they do not only focus on cybersecurity but they get out of the scope in many issues. Likewise, FutureLearn represents a similar case, as there are a wide range of courses offered by world-class education institutions, even though such courses do not offer a cybersecurity path covering the grounds of networking and IoT, along with the comments made for Coursera apply.

On the contrary, ESET cybertraining courses are remote courses powered by the antimalware company, which covers basic issues such as email protection, web protection, social engineering, or password policies, although they do not offer the wide range of knowledge offered by the previous provides or by the ETTCS courses. Digital Literacy Portal presents a compilation of general purposes courses related to basic cybersecurity practices, such as digital footprints, cyberbullying, digital citizenship, or ethical use of digital resources, even though its portfolio does not cover as many cybersecurity issues as the ETTCS courses. Regarding cloud-based and self-based platforms related to cybersecurity, such as KYPO Cyber Range Platform, HackTheBox, or CTFd, they provide hands-on environments in order to put into practice the cybersecurity knowledge, skills, and attitudes. This way, such platforms could be seen as a complement to the courses in order to put the knowledge acquired into practice.

C. Encouraging women's participation in cybersecurity careers

The women under-representation in the cybersecurity industry is a well-known fact. Three reasons are commonly considered for this, such as perceiving cybersecurity as a technical profession, devaluing women's capability for such professions, and limited encouragement obtained by women to become such professions [33]. Furthermore, a series of barriers to career advancement has been spotted which deter women to reach managerial positions in the cybersecurity field, even though those issues may well be extrapolated to other fields as well [34]. Those challenges could be classified into social/institutional and personal, where the former could be defined with the *hacking culture* of working long hours and late nights, which seems incompatible with family obligations, whereas the latter accounts for a set of factors such as educational background, personality traits and other characteristics acquired out of the family environment [35].

Additionally, those barriers vary according to career stages and gender. In this sense, girls are not usually aware of opportunity and requisite training, whilst young women are pretty often concerned about being undervalued in a field typically dominated by men, while mid-career women are fairly concerned about getting harassed in an environment dominated by men [36]. The long-term implication of closing the shortage of women in the cybersecurity industry will not only lower the gender gap, but it will also furnish the sector with more professionals to fill in the empty positions, which in turn may help provide more innovative solutions [37]. Moreover, by increasing the engagement of women in cybersecurity, the rise in the interest regarding STEM education in general, and IT formation in particular, could be a further benefit for society [38].

This way, the existing stereotypes which associate men, but not women, with the technology field could be finally overcome. Such stereotypes are geared by different factors, such as unconscious bias, lack of role models, challenges in work-life balance or workplace culture [39]. Furthermore,

For Peer Review

gender seems to influence in how some activities related to cybersecurity are carried out. For instance, many actions assigned to design, defense and response could be considered as gendered because technical competence, protection and working capabilities are usually associated to masculinity, whereas their opposite are often tied to feminity [40].

Hence, closing the gap gender must be a goal in cybersecurity environments, such that more women need to be attracted into it. This could be done in different ways, such as fostering a culture of respect, sparking the interest in cybersecurity from early ages, building up more pathways to get into a cybersecurity career, creating mentoring programs run by women, ensuring an equitable pay, improving career development or broaden the hiring criteria [41]. Finally, in order to cope with this situation and achieve more women in the cybersecurity field, many initiatives have been put in place by the end of 2023, such as WiCyS (women in cybersecurity), WSC (Women's Society of Cyberjutsu), WoSEC (Women of Cybersecurity), the Diana Initiative, WIA (Women in AppSec), SANS Women's Immersion Academy, Code like a Girl, and many others all around the world [42].

III. Methodology

A. Pedagogical Framework related to Cybersecurity training

There are different approaches when it comes to cybersecurity training, which reinforces the idea of taking a multidisciplinary view. This could include both general information about cybersecurity along with specific information about key concepts. Nag et al. proposed that the later should include risk assessment, prevention, and digital forensics for both civil and military use [43]. Mukjerjee et al. present some of the most common frameworks related to cybersecurity education, such as NICE, ECSF, and OPM, where they all have similar fundamental elements, such as the adoption of a competency-based approach, the definition of workforce roles and learning paths, the formulation of workforce development criteria, the emphasis on standardization, the promotion of lifelong learning, and the incorporation of a muldisciplinary approach [44]. Chowdhury et al. present a cybersecurity training framework based on the ADDIE model, which stands for analysis, design, development, implementation and evaluation, by applying a rapid prototyping approach in order to furnish additional dynamicity and interactiveness [45].

Hwang proposes an framework based on educational games in order to teach cybersecurity concepts, where the learning outcomes basically depend on four independent variables, such as game characteristics, game context, learning theory, and user characteristics [46]. Arabo et al. claim that there is strong correlation between academic performance and motivation, which is enhanced by contextualizing the learning materials with realistic real-world scenarios [47]. Langner et al. present an innovative approach devoted to include not only technical skills in the cybersecurity teaching, but also soft skills, such as critical thinking, problem solving, communication, and empathy, which are key skills when getting into the labour market [48]. Chowdhury et al. describe a teaching framework whose foundation is a game-based scenario by using a specific training video game and a table-top team exercise, where students displayed a high level of engagement, which made a positive impact in their results [49].

Bodea et al. propose the use of a specific framework called Activity Theory, which states that the outcome, which are the improved skills, depend on six factors. Those are tools, represented by knowledge, skills, and software tools, subject, represented by teachers, object, represented by student's skills, rules, represented by norms and requirements, division of labor, represented by specializations, and community, represented by students, teachers, and institution. Those income factors could be related to each other in different ways, which eventually determines the outcome [50]. Prümmer et al. carried out a systematic review of training methods, where game-based ones were the most employed and successful method, followed at a significant distance by presentation-based ones, simulation-based ones, information-based ones, video-based ones, text-based ones, and discussion-based ones [51]. Eventually, as a proof of the importance of cybersecurity, it is to be noted that US military doctrine established cybersecurity as a warfighting domain two decades ago, joining the classical four warfighting domains, such as land, sea, air, and space [52].

B. ETTCS CyberTeach Project and Scopes

Empowering Teachers to Trigger Cybersecurity at Schools (ETTCS), is a two years project, co-funded by the Erasmus+ programme and coordinated by Naples-based Consorzio CLARA, to tackle the issue of cybersecurity and in particular the spreading of information and training on cybersecurity, starting from key figures in our society, i.e. teachers. Teachers can be the driver of this change, their preparation on cybersecurity can support the creation of safer educational environments and transfer of their knowledge to their students. The key functional characteristics of ETTCS are:

1) *Innovative Platform*, as it is possible to access cybersecurity training content, as well as collaborating in real time and monitoring your progress. Besides, this platform supports tailor-made training, as it is continuously adapting to the user needs.
2) *Authoritative Content*, as the courses offered have been designed and created by experts in the field of cybersecurity. Actually, the project was undertaken out of the collaboration of heterogeneous entities, including universities, schools and companies in order to guarantee a complete training on cybersecurity topics.
3) *Easy Access*, as getting to the training materials are intuitive and fast, which may be done from desktop and mobile devices. Moreover, learning is accessible and convenient for anyone thanks to its user-friendly user interface and its powerful search tool

Focusing on the innovative platform, a brand new learning platform has been designed in order to incorporate all key functionalities related to multimedia, easy interaction, and communication in both synchronous and asynchronous way. Hence, a clean slate design allowed to improve some of the key

For Peer Review

aspects already present in existing platforms such as Moodle. This way, the learning platform has been considered as user-friendly by most of the teachers and students taking part in the courses.

Regarding the authoritative content, the courses have been designed by a panel of experts in the cybersecurity field from different European countries. Therefore, each course was carried out by the most appropriate group of researchers according to their academic background and their level of knowledge in a particular matter. For instance, the course dedicated to networking essentials has been designed by experts with many years of experience in the networking field, whereas the course devoted to Introduction to IoT has been designed by researchers with a wide experience in that field. Likewise, the content within the three courses of cybersecurity has been designed by the researchers with a proven experience with each particular matter.

With respect to the easy access, both the platform and the content have been designed to be run in a multiplatform environment, thus it could be executed either in a desktop PC, a laptop PC, a smartphone, or a tablet, as the content get adapted to the features of any specific device. Furthermore, the content has been carefully designed to be as user-friendly as possible, such that any type of user may easily interact with the different types of content, such as multimedia, infographics, or the quizzes available after every subsection within the course.

The following paragraphs describe the main points of the project from a methodological point of view:

1) Project Scopes:

According to the CyberTeach Project summary, included within the application of the CyberTeach Project [53], the objectives expected are the following:

- The development of an open e-learning platform focused on cybersecurity topics.
- The development of digital skills and cybersecurity competences for both teachers and students.
- The development of the ability of teachers so as to achieve a safe online environment.
- The preparation of teachers in order to get ready to train their students on cybersecurity.
- The development of cybersecurity contents and skills so as to lower the skill shortage on this area
- The reduction of the gap between the education world and the labor market so as to lower the unemployment rates.
- The development of students' skills related to cybersecurity, such as problem-solving, technical aptitude, attention to detail, communication or critical thinking.
- The encouragement of women participation in cybersecurity careers.

In order to achieve those goals, the project aims to act in two different ways:

I. The development of an e-learning platform will allow both synchronous and asynchronous training, as well as collaboration activities due to the integration of professional videoconferencing systems.
II. The development of a curriculum on cybersecurity in order to acquire the necessary cybersecurity competences, which will be available on the e-learning platform and will be accessible to the community of teachers and students involved. In this sense, innovative teaching methodologies will be put in place, where gender equality actions will be undertaken in order to ensure at least a fifty percent of women participation during the training activities during the project.

Considering that cybersecurity skills are essential to achieve a secure online user experience, this is even more important when it comes to schools. In this context, young students should all be educated in the safe use of the Internet, where cybersecurity-trained teachers could make a difference in raising cybersecurity awareness in their pupils whilst integrating cybersecurity subjects into their lessons. On the other hand, cybersecurity skills were not so necessary for teachers before the breakout of Covid-19 pandemic, as the vast majority of teaching activities were carried out on-site. However, after this turning point, the spread of distance learning was compulsory and teachers needed to quickly get ready to face those challenges. As a consequence, knowledge about cybersecurity and how to stay safe online must become a key point in the curricula, especially with respect to younger students.

2) Digital Skills and Cybersecurity Competencies:

Digital skills and cybersecurity should go *hand in hand*, as a successful online experience must account for having abilities when navigating the digital space, while protecting against potential threats online. In this sense, some useful cybersecurity techniques are to carry out password hardening, device hardening, safe internet practices, phishing vigilance, malware defense and social engineering safeguard [54]. Digital competence may be seen as a set of capacities regarding not only knowledge, skills and attitudes, but also strategies and values in order to permit users to take advantage of digital technologies for task performance, problem solving and effective communication [55]. Hence, a variety of frameworks may be designed to achieve digital competence, where each of them is expected to cover specific needs, whilst being used on a flexible manner, according to the goals expected in its own particular scenario [56].

In fact, world-leading countries have their own National Cybersecurity Strategic Plans, which gear the associated cybersecurity education in each country, or union of countries, along with training improvement initiatives. Specific plans are in place in the United States, United Kingdom, European Union, Canada, Russia, China, Australia, Association of South Eastern Asian Nations, United Arab Emirates and Switzerland. Anyway, all of them have some common elements, such as the goal of getting cybersecurity resilient, the search for new talent in cybersecurity, the need to invest in research & development (R&D) against emerging attacks and society's maturity and awareness related to cybersecurity [57].

For Peer Review Only

In the context of the European Union, DigComp 2.2 is the current digital Competence Framework for citizens, which furnishes a common language in order to spot key domains of digital competence [58]. DigComp conceptual reference model is composed of 5 competence areas, which are further divided into 21 competences overall. Those are presented in the following list:

1. Information and data literacy:
   - 1.1 Browsing, searching and filtering data, information and digital content.
   - 1.2 Evaluating data, information and digital content.
   - 1.3 Managing data, information and digital content.
2. Communication and collaboration:
   - 2.1 Interacting through digital technologies.
   - 2.2 Sharing information and content through digital technologies.
   - 2.3 Engaging in citizenship through digital technologies.
   - 2.4 Collaborating through digital technologies.
   - 2.5 Netiquette.
   - 2.6 Managing digital identity.
3. Digital content creation:
   - 3.1 Developing digital content.
   - 3.2 Integrating and re-elaborating digital content.
   - 3.3 Copyright and licenses.
   - 3.4 Programming.
4. Safety:
   - 4.1 Protecting devices.
   - 4.2 Protecting personal data and privacy.
   - 4.3 Protecting health and well-being.
   - 4.4 Protecting the environment.
5. Problem Solving:
   - 5.1 Solving technical problems.
   - 5.2 Identifying needs and technological responses.
   - 5.3 Creatively using digital technologies.
   - 5.4 Identifying digital competence gaps.

The digital skills related to cybersecurity are allocated in competence area 4, which is called *Safety*, and it is composed of four competences. The first one is focused on protecting not only devices but also digital content, as well as understanding risks and threats in digital environments. The second one is centered on protecting personal data and privacy in digital environments, as well as understanding the way to use and share personally identifiable information. The third one is focused on avoiding health-risks and threats to both physical and psychological well-being in the use of digital technologies. The fourth one is centered on being aware of the impact of using digital technology on the environment [59].

Those four competences must be taken into consideration when referring to cybersecurity in the education field. In fact, cybersecurity needs to be seen as everyone's responsibility, including educational institutions, staff and students, because it represents an ongoing challenge in the ever-growing and necessary digitalization of education and society [60]. Actually, cybersecurity may be seen as an interdisciplinary discipline, because it does not only involves technology, but also different aspects of law, policy, human factors, ethics, and risk management [61].

Sticking to those competences, which are the ones related to cybersecurity within the DigComp 2.2, the 6 courses included in the CyberTeach Project permit to acquire all those competences in different ways. As a matter of fact, the protection of devices and data content is a constant priority along all courses, no matter which learning level a particular course is aiming at. Likewise, the protection of personal data and privacy is treated one way or another within all courses as a key point. Moreover, the protection of health and well-being online is also a fundamental fact all around the curricula offered. And besides, the protection of the environment is incentivized throughout the whole range of courses in order to restrain from wasting unnecessary energy consumption and to undertake green practices so as to reduce carbon emissions. Therefore, it may be concluded that the courses, offered within the ETTCS CyberTeach Project, meet the requirements established in competence area 4 of DigComp 2.2 regarding the digital competence of safety, as all of its four competences are addressed throughout the whole range of courses provided. This results in the awareness of protection concerns when it comes to not only going online with any device, but also to dealing with digital content, personal data and privacy, health and well-being, as well as the environment.

3) Cybersecurity Curricula:

It is to be reminded that the target of this e-learning platform is to host a series of cybersecurity courses which cover the digital skills and cybersecurity competences quoted above, as per the DigComp 2.2 framework. An overall amount of 6 courses have been design, which compose the curricula on cybersecurity offered in the e-learning platform. Following, we provide information about them:

1) The first course is called *Innovative Methods & Tools*, which is composed of 10 modules, each of those being made of 5 sections. This course is not aimed at students but it was thought for teachers, as it goes through the new tendencies in active learning. This way, teachers may get an alternative view on how to face the cybersecurity teaching, where students take the active role and teachers act more like facilitators [62].
2) The second course is called *Introduction to Cybersecurity*, which is composed of 11 modules, each of them being made of 5 sections. This could be considered as the first course to get into the field of cybersecurity, as this is a beginner's course where the basic features of cybersecurity are explained. Hence, this should be the starting course for students and teachers with little or no knowledge about cybersecurity.
3) The third course is called *Introduction to IoT*, which is composed of 11 modules, each of them being made of 5 sections. This course undertakes a review on Internet of Things (IoT) devices on the most prominent areas of application. This is also a beginner's course and its target

Information and Computer Security

is to provide some basic knowledge about the capabilities of this type of devices whose use is rising year by year.

4) The fourth course is called *Networking Essentials*, which is composed of 11 modules, each of them being made of 5 sections. This course carries out a review on networking fundamentals, which is a critical part when getting into the cybersecurity field. This is a beginner's course as well and its goal is to furnish some basic understanding about how network interconnections work, as well as the main features of the network devices.
5) The fifth course is called *Cyber Ops*, which is composed of 10 modules, each of them being made of 5 sections. This course gets deeper into the cybersecurity field, so it could be seen as an intermediate course, where topics on cybersecurity are exposed on the grounds of the three beginner's courses, which could be considered as a prerequisite of this one.
6) The sixth course is called *Cybersecurity Advanced*, which is composed of 9 modules, each of them being made of 8 sections. This course gets even deeper into the cybersecurity field, so it may be seen as an advanced course, where cybersecurity topics are shown on the grounds of the intermediate course, which could be seen as a prerequisite of this one.

In summary, those courses cover the digital skills and the cybersecurity competences, expected for a beginner user, an intermediate user or an advance user, as they are displayed on an incremental basis, from rookie to expert.

In this context, the cybersecurity path proposed with those six courses is structured into three levels. The first one is devoted to basic level, where the target is set to users with little or no knowledge about cybersecurity. However, it would be highly recommended for users with an intermediate level in cybersecurity to review those basic contents, and even for high level users in order to brush up their knowledge. Among the basic level courses, "Introduction to Cybersecurity" is the key point, as it is devoted to explain the foundation of cybersecurity.

On the other hand, "Introduction to IoT" and "Networking Essentials" are additional basic courses which provides necessary contents to face the higher level courses with a sound background. The second level is dedicated to intermediate level, where users need previous knowledge to understand the concepts exposed. There is only one course called "Cyber Ops" and it is considered as the linking point between the basic level courses and the advanced one. The third level is committed to advanced level, where a higher level of knowledge is needed in order to face the contents. There is only one course named "Cybersecurity Advanced" and it allows users to acquire advanced skills in current and incipient cybersecurity techniques.

Furthermore, the first course offered is called "Innovative Methods & Tools", which is focused on how teachers can implement active learning techniques when teaching cybersecurity to their students. Active learning paradigm is characterized by given the active role in education to students, whilst teachers act as facilitators of the teaching-learning process [63]. Different features of active learning are reviewed during this course, such as interactive learning environments, digital learning environments, gamification and its impact on education, peer education and its implications, project work as a teaching methodology, the use of workshops in the education field, how to carry out storytelling in education, or Challenge-Based Learning (CBL).

Fig. 1. Homepage of the on-line platform hosting the cybersecurity courses.

4) Cybersecurity e-Learning Platform:

As state before, the main point of the cybersecurity e-learning platform being built up in this project is the construction of a brand-new open source platform solely aimed at cybersecurity training, whose focus is set on offering cybersecurity courses to cover the training needs of beginner, intermediate and advanced level users. The implementation of the e-learning platform was carried out in four steps:

I. Analysis, where other e-learning platforms available in the market were studied in order to identify their strengths and weaknesses, as well as to identify the current trends in the market regarding design and features.
II. Design, where technical details in the specification of the platform were decided in relation to the desired functionalities of the platform from the macro and micro point of view.
III. Implementation, where the design of the platform was implemented with all the expected features according to the product design, which was followed by the appropriate testing and the commissioning.
IV. Training, where the necessary instruction and coaching were given to the partners involved about the use of the platform.

This platform is available at https://ettcs.com and the top of its homepage is shown in Figure 1, where we can see the project's logo, along with a button to log in if a user has already been registered into the platform, or otherwise, a user can do it through the button to sign up.

Furthermore, other important features have been added to the platform, such as the following:

✓ Multimedia content, as the course is composed of a variety of sources, such as video lessons, slide presentations, simulations, infographics, animations and interactive quizzes.

For Information and Computer Security

- ✓ Personalized feedback, as the learning process is constantly monitored by means of periodic tests, which will point out the areas to improve.
- ✓ Certificate of competence, which may be acquired directly from the platform.
- ✓ Contact with teachers, which may be done in both synchronous and asynchronous way.
- ✓ Community, as users may get in contact with cybersecurity enthusiasts and experts.

In this sense, multimedia content makes the content more user-friendly, as it allows users to interact with content, as opposed to only text curriculum. Relevant images have been added in all sections, which facilitates the understanding of the main points. Moreover, a wide range of video lessons is available in order to get deeper in some issues, which is also promoted with the use of simulations, infographics, and animations. Additionally, there are interactive quizzes after finishing each subsection in order for users to assess the knowledge they acquired. Those quizzes let users know whether they are fit to pass through to the next subsection, or otherwise, they should repeat the current subsection again in order to review the materials and retake the quiz.

5) Bridging the Gap between Education World and the Labor Market to Reduce Unemployment Rates:

There is a gap between education and production in all IT sector, although the shortage of skilled professionals related to the cybersecurity field is the strongest, where about 4 million jobs were uncovered worldwide in 2023, whereas the workforce itself is around 5.5 million [64]. Furthermore, skills gaps are ever an issue, as workers often lack proficiency and expertise in particular critical cybersecurity skills for certain areas [65]. Some of the areas with skills gaps are software and hardware security, security management, requirements engineering, compliance and certification [66].

Regarding the skills gaps, three points are recommended, such as mastering the fundamentals of computer science, where a proficient knowledge of operating systems, networking protocols, programming languages, cloud management, as well as exploitation and mitigation methods should be achieved. Besides, hand-on experience is also important, as theory alone does not get graduates ready to go. Moreover, the development of soft skills is also important, as it may convert technical knowledge into value for the company [67]

With respect to the shortage of cybersecurity workforce in areas like penetration testing and threat analysis, some convenient actions could be undertaken, such as the increase enrolment in cybersecurity programs, the support of a unified approach among government, industry and higher education institutions, the understanding of job market needs and trends, the promotion of analysis about the necessities in the market, or the accessibility and openness of initiatives [68].

An outstanding trend when hiring new employees in cybersecurity in the last years is the importance on certificates as a way to validate individual skills, which assure technical competence, as well as a deep understanding of them [69]. Another interesting concept is sec [70]. Anyway, some recommendations to be prepared is to gain visibility into potential security gaps, prioritize identity protection, prioritize cloud protection, get to know your adversary and keep practicing as that is the way to perfection [71]. In this sense, some of the most common complaints in the cybersecurity sector are those related to cloud management, the need of hands-on experience and training courses to keep up with the last tendencies, the increase of staff workload due to skills shortage, the need to improve soft skills as much as the technical ones, and the delay in filling in critical cybersecurity positions [72].

Therefore, the shortage of personnel on the cybersecurity sector could be tackled with the adequate education on the necessary skills, hence the role of educational institutions becomes crucial to sort this issue out. In this sense, education institutions could help bridge the gap by creating educational programs to furnish the necessary knowledge, skills and abilities for the current and future cybersecurity workforce, no matter if the come from STEM (science, technology, engineering and mathematics) or non-STEM disciplines [73]. In this context, the NICE Cybersecurity Workforce Framework, led by National Industry of Standards and Technology (NIST), is a partnership which involves US government, academia and private sector focused on educating and training the cybersecurity posture of organizations. It basically furnishes a set of building blocks in order to describe tasks, knowledge and skills necessary to carry out cybersecurity work. Some of its goals are to promote the discovery of careers in cybersecurity, adapt learning to build and sustain a skilled workforce, modernize talent management to address skills gaps in cybersecurity, and drive research on effective practices related to cybersecurity. NICE strategic plans have also been put in place in different countries, such as in the United States [74] or in the United Kingdom [75], as each one has its own characteristics when it comes to cybersecurity [76].

On the other hand, although holding a college degree or gaining industry certifications is always important, the main focus has to be set on getting a technically sound skillset in order to perform well in cybersecurity job roles. Traditional education usually provides hands-on access to equipment, as well as direct interaction with instructor and team mates, although prices are higher and content is not usually updated fast enough. On the contrary, platform-based education, where the learning process is based on online connections, allows for an on-demand, browser-based, cheaper and more up-to-date experience, even though direct interaction with equipment is lost and there are fewer manners to build up critical soft skills. Hence, a balanced combination of both approaches is meant to be the optimal solution, as the weaknesses of one method are cancelled by the strengths of the other [77].

Anyway, the current trends in the education field after the COVID-19 pandemic go towards empowering online education and there it is where the CyberTeach Project fits in [78]. In other words, the CyberTeach Project provides all the advantages of cloud-based education, as the learning experience is on an on-demand basis, it could be accessed with

Information and Computer Security

any device, and the content has been designed by experts in the field. Additionally, different communication tools have been implemented on the platform in order to build up a community of users interested in cybersecurity topics, where they can communicate with teachers and also with other members of the community.

C. Cybersecurity related Case Studies

We present herein two case studies: one at a Regional level and another one at a National level. The former is called Learn-A-Thon 2023 and its scope is set on Europe, whereas the latter is called Panoptis competition and its scope is set on Greece.

1) Learn-A-Thon 2023:

In order to spread the word of the CyberTeach Project, a series of dissemination events were organized by the different partners involved. The main goal of those events were to present the conclusions of the project to relevant stake holders, such as secondary teachers and educational institutions, which effectively were to unveil the platform and the cybersecurity courses available to the potential end users. Furthermore, some hackatons related to cybersecurity learning at a basic level were held in order to promote it. In this context, some partners in the CyberTeach project were in charge of co-organizing the European Cyber Cup 2023, which was managed by the European division of Cisco Systems. The main point on this event was Learn-A-Thon 2023, which was a hackaton in the form of a Capture The Flag (CTF) session, where all questions were related to cybersecurity learning at an entry level. There were 16 teams taking part in it, each of them composed of 4 members, and coming from different European countries [79], which were selected among the best participants in a previous round, where a great deal of participants got enrolled.

The CTF had seven blocks, each of them related to a specific cybersecurity topic, such as end point security, cyber threat management, network defense, network support, network basics, network troubleshooting, and network secure configuration. The overall amount of questions, represented by flags, was 90. Flags were somewhat evenly distributed among courses, where a number of points was awarded when properly asking each question. However, a series of clues were available in every question, even though some points were taken out of the value of such a question according to how many clues were uncovered before getting the right answer. This CTF was held during 3 hours in the afternoon and the winning team got to finish a few minutes before the deadline, while the rest of the teams were not able to get it done completely. Nonetheless, the competitive environment and the good mood among the participant teams made a remarkable experience for them, where they not only applied their knowledge and skills on the cybersecurity field, but they also enjoyed and had fun with it. Hence, this event could be considered as an absolute success as the expected goals were fully achieved.

2) Panoptis 2023:

One of the most important national cybersecurity exercises in Greece is Panoptis. Panoptis takes place on an annual basis and is the largest and most challenging cybersecurity event, as the participating entities exceed one hundred. The demographic characteristics of the participants represent all key players and stakeholders in Greece, including military and law enforcement agencies, universities and academic institutions, as well as the private and public sectors.The participants can either observe all stages of the exercise, including preparation, scenario development, execution, and debriefing, or actively engage with their own teams in one or more challenges. Given its multi-day duration, the exercise demands considerable effort due to the complexity and sophistication of the challenges. The evolving scenarios require quick responses from contesting teams. Invariably, participation in Panoptis extends well beyond the scheduled drill days. Organized by the Directorate of Cyberdefense of the Greek army, the exercise's scenario design and preparations commence many months in advance. It's not uncommon for exceptional past participants to collaborate with army officers in developing new challenges. Overall, the Panoptis cybersecurity exercise stands as Greece's most comprehensive, mature, meticulously planned, and realistic cybersecurity challenge [80].

It comprehensively addresses various facets of cybersecurity threats, encompassing malware analysis, network perimeter protection, forensics, social engineering, mobile cyberattacks, Industrial Control Systems (ICS) security, incident handling for the Internet of Things, and more. A key feature of the Panoptis competition is its facilitation of team collaboration, recognized as essential for managing the complexity of exercises within the allocated time frames. Concurrently, the Panoptis challenge framework fosters inter-team competition, thereby motivating teams to deliver optimal performance and devise solutions to diverse cybersecurity challenges. Noteworthy aspects of the competition include the absence of a requirement for participants to procure proprietary tools; instead, the utilization of available open-source cybersecurity tools is deemed adequate for addressing all challenges presented.

The academic sector has consistently engaged in every Panoptis cybersecurity exercise since its inception. Initially, during the early years, certain Greek universities were able to field separate teams; however, the evolving demands and heightened competition in recent years have rendered it challenging for universities to sustain independent participation. In recent times, most academic institutions have opted to participate under the auspices of the Greek Open Technologies Alliance (GFOSS). Within this framework, members of the ETTCS project assumed responsibility for coordinating student teams representing the University of Thessaly across three distinct departments spanning multiple cities. The cumulative experience and insights gleaned from the Panoptis national cybersecurity exercises have proven invaluable for the organization of hackathons and other practical activities within the ambit of the ETTCS initiative [81].

Another valuable experience for the ETTCS project was our involvement in the OWASP Hackademic project. The Hackademic project, which later became an official OWASP project and was also sponsored by the Google Summer of

Information and Computer Security

Code program, was among the pioneering efforts to impart ethical hacking education within university curricula. Students were afforded the opportunity to think innovatively and cultivate an attacker mindset, thereby comprehending cybersecurity beyond traditional disciplinary boundaries, recognizing that hackers operate without strict adherence to rules. Every oversight or misconfiguration during software system design and deployment could be susceptible to exploitation. The Hackademic project focused primarily on the OWASP Top 10 web application security risks, including cross-site scripting (XSS) attacks, web server misconfigurations, Local File Inclusion (LFI) attacks, and path traversal attacks, while also addressing core cybersecurity domains such as cryptography, steganography, and social engineering.

As expected, the challenges presented to the students were not derived from real vulnerable systems that could potentially be exploited, causing broader issues for the university networks. Instead, they were simulated examples within a securely constrained environment. A substantial portion of this course focused on ethical education, covering responsibilities, duties, codes of conduct, and other obligations pertinent to cybersecurity researchers and professionals. The outcomes of these endeavors, particularly the students' engagement and satisfaction, were overwhelmingly positive. Consequently, we are contemplating integrating fundamental aspects of the ETTCS project with ethical hacking components to develop a future cybersecurity educational program, that will offer a holistic understanding of both cyberdefense and cyber-offensive operations.

IV. Concluding Remarks and Future Work

Our work demonstrates a new methodology to infuse cybersecurity awareness into teachers so that they can train and prepare their students accordingly. We identify the teacher as the critical link between a young generation of *digital natives*, who consider the Internet as a utility, and the most experienced IT security experts striving to enforce good cybersecurity practices among users. Understanding the fundamental aspects of cybersecurity is not just a vital professional skill but also an essential survival mechanism for both children and adults in today's world of ubiquitous connectivity. Especially for young students, the fundamentals of cybersecurity should be incorporated into all educational programs. This is imperative, given that a considerable percentage of cybercrimes against minors occur through online channels. The ETTCS project aids educators in assimilating the pivotal aspects of this field and furnishes them with essential materials, encompassing both theoretical and practical components, to instruct students. This enables teachers to concentrate solely on pedagogical methods, enhancing their ability to effectively convey their educational message.

In summary, the strategic goal of the CyberTeach Project was to raise awareness on cybersecurity in teachers in order for them to become the driving force to trigger cybersecurity learning to their students. This goal was implemented through two objectives, such as the construction of an open-source on-line platform devoted to host cybersecurity courses, and the design of a series of cybersecurity courses to be offered within that platform. Regarding the cloud-based platform, a brand-new platform was created from scratch in order to get it customized with the features expected. In this sense, some of its characteristics are the independence of external providers, straightforward design, easy URL to access, inclusion of communication tools with teachers and other peers, and support for a community of enthusiasts and experts in the cybersecurity area.

With respect to the courses, a panel of experts in the cybersecurity field got together in order to design six courses for different types of learners. As a matter of fact, *Innovative Methods & Tools* is solely oriented to teachers and is devoted to expose a collection of active learning tools for their teaching sessions on cybersecurity. On the other hand, there are three courses oriented to cybersecurity learners at a beginner's level, which are "Introduction to Cybersecurity", "Introduction to IoT" and "Networking Essentials", where the fundamentals of different necessary areas are exposed in order to better understand further courses. Furthermore, there is another course aimed at learner's at an intermediate level, which is *Cyber Ops*, where the knowledge of the previous courses are brought to a further level. Additionally, there is a course intended for learner's at an advanced level, which is *Cybersecurity Advanced*, where high-level topics are displayed.

Eventually, it is to be reminded that the official name of the CyberTeach Project is Empowering Teachers to Trigger Cybersecurity at School, whose acronym is ETTCS and whose website is located at https://ettcs.com. Therefore, the primary target of this project was to provide teachers with an independent platform and a set of expert-created courses devoted to support them in order to teach cybersecurity to their pupils. This way, the overall aim of the CyberTeach Project was to raise awareness of cybersecurity threats by promoting safe and secure browsing when going online, and we consider that the resources offered in this project furnish enough elements so as to be more conscious of cybersecurity dangers in order to ensure a safe and secure browsing experience.

Regarding the future work, we plan to extend the range of cybersecurity courses available in order to widen the range of topics involved in the current courses. For instance, some ideas could be a course dedicated only to the security in wireless deployments managed by a controller, or another one devoted only to secure programmable logic controllers (PLC) in industrial environments, or even another one targeting the security perspective in vehicular networks. On the other hand, it is also considered to extend the number of courses at intermediate and advanced level, as there are just only one of each type. This way, new courses getting deeper into securing IoT and networking could also be released. Furthermore, another possible line of courses could be those related to go further into Linux management or Python scripting, as those are both necessary skills in the cybersecurity area. Anyway, these are just some of the ideas to offer a new range of courses in the near future in order to both attract new users and keep

For Peer Review Only

current users involved.

Additionally, the platform´s effectiveness can't be measured at this point, as it has recently been released and no students have already finished any of the courses. However, in future research, we plan on undertaking a longitudinal study in order to examine how the cybersecurity skills of the participants have evolved over a period of time as they keep taking the full itinerary of courses provided in the platform. This way, we could track the efficiency of the educational intervention when it comes to upskill or reskill the participants. Nonetheless, several usability tests have been undertaken in order to assess the functionality of the platform and the courses, where users from different countries and backgrounds have been interacting with it. Most of those users stated that the platform is user-friendly, which allows them to easily move along the courses, considering the content exposed within the different sections and subsections, along with the extra materials offered, and the quizzes at the end of each subsection. These are encouraging results, even though the definitive results will have to wait until the platform and the courses are all up and running and real students undertake the whole cybersecurity path, starting from the beginner level, moving to the intermediate level, and eventually completing the advanced level.

ACKNOWLEDGMENT

The CyberTeach Project, also known as Empowering Teachers to Trigger Cybersecurity at School (ETTCS), has been carried out thanks to a partnership composed of Consorzio Clara from Naples (Italy), University of Thessaly from Volos (Greece), BiASC from Belgium, Miguel Hernández University from Elche (Spain), ITIS G. Ferraris from Naples (Italy) and Euphoria.net from Rome (Italy). Additionally, this project was funded by the European Union through the Erasmus+ Programme and has been undertaken during the last two years.

REFERENCES

[1] P. A. Vervier and Y. Shen, "Before toasters rise up: A view into the emerging IoT threat landscape," in Proceedings of Research in Attacks, Intrusions, and Defenses: 21st International Symposium (RAID 2018), pp. 556–576, Heraklion, Crete, Greece, September 10-12, 2018.

[2] A. Razaque, F. Amsaad, M. J. Khan, S. Hariri, S. Chen, C. Siting, and Xingchen Ji. "Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain," IEEE Access, vol. 7, pp. 168774–168797, 2019.

[3] J. I. Iturbe-Araya and Helena Rifa-Pous, "Anomaly-based cyberattacks detection for smart homes: A systematic literature review," Internet of Things, vol. 22, 100792, 2023.

[4] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. R. J. Fontaine, A. Filippoupolitis, and E. Roesch, "A taxonomy of cyber-physical threats and impact in the smart home," Computers & Security, vol. 78, pp.398–428, 2018.

[5] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems," vol. 16(2), pp.546–556, 2015.

[6] S. Malik and W. Sun, "Analysis and simulation of cyber attacks against connected and autonomous vehicles," in Proceedings of 2020 International Conference on Connected and Autonomous Driving (MetroCAD 2020), pp. 62–70, Detroit (MI), United States, February 27-28, 2020.

[7] A. P. Fournaris, L. Pocero-Fraile, and O. Koufopavlou, "Exploiting hardware vulnerabilities to attack embedded system devices: a survey of potent microarchitectural attacks," Electronics, vol. 6(3), 052, 2017.

[8] N. F. Polychronou, P. H. Thevenon, M. Puys, and V. Beroulle, "A comprehensive survey of attacks without physical access targeting hardware vulnerabilities in IoT/IIoT devices, and their detection mechanisms," ACM Transactions on Design Automation of Electronic Systems (TODAES), vol. 27(1), pp. 1–35, 2021.

[9] F. Li and V. Paxson, "A large-scale empirical study of security patches," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS'17), pp. 2201–2215, Dallas (TX), United States, November 3rd, 2017.

[10] Y. Shin and L. Williams, "An initial study on the use of execution complexity metrics as indicators of software vulnerabilities," in Proceedings of the 7th International workshop on software engineering for secure systems, pp. 1–7, Honolulu (HI), United States, May 22nd, 2011.

[11] A. McGettrick, "Toward effective cybersecurity education," IEEE Security & Privacy, vol. 11(6), pp. 66–68, 2013.

[12] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," Journal of Computer Information Systems, vol. 62(1), pp. 82–97, 2022.

[13] S. Furnell, "The cybersecurity workforce and skills," Computers & Security, vol. 100, 102080, 2021.

[14] D. J. Kay, T. J. Pudas, and B. Young, "Preparing the pipeline: The US cyber workforce for the future," Defense Horizons, no. 72, 2012.

[15] D. Gritzalis and S. Papageorgiou, "Panoptes: The greek national cyber defence exercise," CEER-ENISA Workshop, Athens, Greece, 2016.

[16] M. Gafic, S. Tjoa, P. Kieseberg, O. Hellwig, and G. Quirchmayr, "Cyber exercises in computer science education," in Proceedings of 8th International Conference on Information Systems, Security and Privacy (ICISSP 2022), Vienna, Austria, February 9th-11th, 2022. pages 404–411, 2022.

[17] D. L. Burley, M. Bishop, S. Buck, J. J. Ekstrom, L. Futcher, D. Gibson, E. K. Hawthorne, S. Kaza, Y. Levy, H. Mattord, and A. Parrish, "CSEC: cybersecurity curricula 2017 - curriculum guidelines for post-secondary degree programs in cybersecurity," Technical Report Version 1.0, Report 31, Association for Computing Machinery, IEEE Computer Society, Association for Information Systems, International Federation for Information Processing, 2017.

[18] W. Newhouse, S. Keith, B. Scribner, and G. Witte., "National initiative for cybersecurity education (NICE) cybersecurity workforce framework," NIST special publication, 800-181, 2017.

[19] T. Crick, J. H. Davenport, A. Irons, and T. Prickett, "A UK case study on cybersecurity education and accreditation," in Proceedings 2019 IEEE Frontiers in Education Conference (FIE), pp. 1–9, Covington (KY), United States, October 16th-19th, 2019.

[20] I. Kuzminykh, M. Yevdokymenko, O. Yeremenko, and O. Lemeshk, "Increasing teacher competence in cybersecurity using the eu security frameworks," International Journal of Modern Education & Computer Science, vol. 13(6), pp. 60–68, 2021.

[21] H. I. Haseski, "Cyber security skills of pre-service teachers as a factor in computer-assisted education," International Journal of Research in Education and Science, vol. 6(3) pp. 484–500, 2020.

[22] P. Pusey and W. A. Sadera, "Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference," Journal of Digital Learning in Teacher Education, vol. 28(2), pp.82–85, 2011.

[23] M. McLean, "2024 Must-Know Cyber Attack Statistics and Trends," report accessed on January 26th 2024, available online at https://www.embroker.com/blog/cyber-attack-statistics/, 2024.

[24] ENISA flags cybersecurity skills shortage; identifies measures to bolster workforce, accessed on January 26th 2024, available online at https://industrialcyber.co/news/enisa-flags-cybersecurity-skills-shortage-identifies-measures-to-bolster-workforce/, 2021.

[25] The 2022 (ISC)2 cybersecurity workforce study, report accessed on January 26th 2024, available online at https://www.isc2.org/Research/Workforce-Study, 2022.

[26] A. Pipikaite, G. Bueermann, A. Joshi, and J. Jurgens, "Global cybersecurity outlook 2022," report, World Economic Forum (WEF), Davos (Switzerland), 2022.

[27] T. Byers, W. Imms and E. Hartnell-Young, "Evaluating teacher and student spatial transition from a traditional classroom to an innovative learning environment," Studies in Educational Evaluation, vol. 58, pp. 156–166, 2018.

For Peer Review Only

[28] 10 Cyber Security Training Platforms, accessed on January 26th 2024, available online at https://www.edapp.com/blog/cyber-security-training-platforms/, 2023.

[29] Digit@l Literacy Project, accessed on January 26th 2024, available online at https://digitalliteracyportal.com/LMS/, 2021.

[30] R. Beuran, D. Tang, Z. Tan, S. Hasegawa, Y. Tan and Y. Shinoda, "Supporting Cybersecurity Education and Training via LMS Integration: CyLMS," Education and Information Technologies, vol. 24, pp. 3619–3643, 2019.

[31] V. Svábenský, J. Vykopal, P. Celada and J. Dovjak, "Automated feedback for participants of hands-on cybersecurity training," Education and Information Technologies, pp. 1–30, 2023.

[32] A. Rahaimi, Y. Sadqi and Y. Maleh, "A Comparative Study of Online Cybersecurity Training Platforms," Lecture Notes in Computer Science, vol. 14368, pp. 122–134, 2023.

[33] I. Bongiovanni and M. Gale, "Women in Cyber – Exploring the Barriers, Redesigning the Profession," report, University of Queensland Business School, Australia, 2023.

[34] H. G. Corneliussen, "What Brings Women to Cybersecurity?: A Qualitative Study of Women's Pathways to Cybersecurity in Norway," in Proceedings of the 2020 European Interdisciplinary Cybersecurity Conference (EICC'20), art. 09, Rennes, France, November 18th 2020.

[35] S. Bagchi-Sen, R. Rao, S. J. Upadhyaya and S. Chai, "Women in Cybersecurity: A Study of Career Advancement," IT Professional, vol. 12(1), pp. 24–31, 2010.

[36] J. S. Giboney, B. B. Anderson, G. A. Wright, S. Oh, Q. Taylor, M. Warren and K, Johnson, "Barriers to a cybersecurity career: Analysis across career stage and gender," Computer & Security, vol. 132, 103316, 2023.

[37] K. K. Lingelbach, "Perceptions of Female Cybersecurity Professionals Toward Factors that Encourage Females to the Cybersecurity Field," PhD Thesis in Information Systems at Nova Southeastern University, Davi (FL), USA, 2018.

[38] N. Berríos, "Increasing the Participation of Young Women in Cybersecurity," report, Polytechnic University of Puerto Rico, 2019.

[39] Y. Asiry, "Closing the Gap: Boosting Women's Representation in Cybersecurity Leadership," Journal of Information Security, vol. 15(1), pp. 15–23, 2024.

[40] K. Millar, J. Shires and T. Tropina, "Gender approaches to cybersecurity: design, defence and respons," report, United Nations Institute for Disarment Research, 2021.

[41] Closing the gender gap: 7 ways to attract more women into cybersecurity, accessed on January 26th 2024, available online at https://www.welivesecurity.com/en/we-live-progress/closing-gender-gap-7-ways-attract-more-women-cybersecurity/, 2023.

[42] 35+ initiatives to get more women into cybersecurity, accessed on January 26th 2024, available online at https://www.comparitech.com/blog/information-security/women-cybersecurity-initiatives/, 2023.

[43] A. K. Nag, V.S. Bhadauria, C. Gibson, R. C., Naupane, and D. Creider, "A Conceptual Learning Framework of Cybersecurity Education for Military and Law Enforcement: Workforce Development", International Journal of Smart Education and Urban Society, vol. 13(1), 1-14, 2022.

[44] M. Mukherjee, N. T. Le, Y. W. Chow, and W. Susilo, "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes", Information, vol. 15, 117, 2024.

[45] N. Chowdhury, S. Katsikas, and V. Gkioulos, "Modeling effective cybersecurity training frameworks: A delphi method-based study", Computers & Security, vol. 113, 102551, 2022.

[46] M. Hwang, and S. Helser, "Cybersecurity educational games: a theoretical framework", Information and Computer Security, vol. 30(2), 225-242, 2022.

[47] A. Arabo, and M. Serpell, "Pedagogical Approach to Effective Cybersecurity Teaching", Transactions on Edutainment XV, Lecture Notes in Computer Science, vol. 11345, 129-140, 2019.

[48] G. Langner, S. Furnell, G. Quirchmayr, and F. Skopik, "A comprehensive design framework for multi-disciplinary cyber security education", Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674, 105-115, 2023.

[49] N. Chowdhury, and V. Gkioulos, "A Personalized Learning Theory-based Cybersecurity Training Exercise", International Journal of Information Security, vol. 22, 1531-1546, 2023.

[50] C. N. Bodea, M. I. Dascalu, and M. Cazacu, M.,"Increasing the effectiveness of the cybersecurity teaching and learning by applying activity theory and narrative research", Issues in Information Systems, vol. 20(3), 186-193, 2019.

[51] J. Prümmer, T. van Steen, and B. van den Berg, "A systematic review of current cybersecurity training methods", Computers & Security, vol. 136, 103585, 2024.

[52] L. M. Prough, "Education theories applied to a cyber security bootcamp", Master's Thesis, Kansas State University (KS), USA, 2018.

[53] Empowering Teachers to Trigger Cybersecurity at School, accessed on January 26th 2024, available online at https://ettcs.com/, 2024.

[54] Digital Literacy and Cybersecurity Skills for eLearning Success, accessed on January 26th 2024, available online at https://elearningindustry.com/digital-literacy-and-cybersecurity-skills-for-elearning-success/, 2024.

[55] M. Ríoseco-País, J. Silva-Quiro and C. Carrasco-Manríquez, "Development of Digital Competences in Students of a Public State-Owned Chilean University Considering the Safety Area," Education Sciences, vol. 13(7), 710, 2023.

[56] M. Bacigalupo, "Competence frameworks as orienteering tools," Revista Interuniversitaria de Investigación en Tecnología Educativa, vol. 12, 20–33, 2022.

[57] S. Al Daajeh, H. Saleous, S. Alrabaee, E. Barka, F. Britinger and K. K. R. Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education," Computers & Security, vol. 119, 102754, 2022.

[58] R. Vourikari, S. Kluzer and Y. Punie, "DigComp 2.2 – The Digital Competence Framework for Citizens," report, European Commission, 2022.

[59] R. Vourikari, N. Jerzak, Z. Karpinski, A. Pokropek and J. Tudek, "Measuring Technical Skills across the EU: Digital Skills Indicator 2.0," JRC Technical Report, European Commission, 2022.

[60] A. Irons and T. Crick, "Cybersecurity in the digital classroom: implications for emerging policy, pedagogy and practice," in The Emerald handbook of higher education in a post-covid world: new approaches and technologies for teaching and learning, Emerald Publishing Limited, Leeds, United Kingdom, pp. 231-244, 2022.

[61] L. C. Chen, A. Cotoranu, P. Mandhare and Darren. Hayes, "An Integrated System for Connecting Cybersecurity Competency, Student Activities and Career Building," Lecture Notes in Networks and Systems, vol. 310, pp. 3–12, 2021.

[62] P. J. Roig, S. Alcaraz, K. Gilly, C. Bernad and C. Juiz, "Using Escape Rooms as Evaluation Tool in Active Learning Contexts," Education Sciences, vol. 13(6), 535 (2023).

[63] P. J. Roig, S. Alcaraz, K. Gilly, C. Bernad and C. Juiz, "An Active Learning Approach to Evaluate Networking Basics," Education Sciences, vol. 14(7), 721 (2024).

[64] How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, report, ISC2 Cybersecurity Workforce Study, 2023.

[65] Cybersecurity workforce shortage reaches 4 million despite significant recruitment drive, accessed on January 26th 2024, available online at https://www.csoonline.com/article/657598/cybersecurity-workforce-shortage-reaches-4-million-despite-significant-recruitment-drive.html/, 2023.

[66] F. Goupil, P. Laskov, I. Pekaric, M. Felderer, A. Dürr and F. Thiesse, "Towards Understanding the Skill Gap in Cybersecurity," in Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE), Vol. 1, pp. 477–483, Dublin, Ireland, July 8th-13th 2022.

[67] W. Crumpler and J. A. Lewis, "The Cybersecurity Workforce Gap," report, Center for Strategic & International Studies (CSIS), 2019.

[68] J. R. C. Nurse, K. Adamos, A. Grammatopoulos, and F. Di Franco, "Addressing the EU cybersecurity skills shortage and gap through higher education," European Union Agency for Cybersecurity (ENISA), 2021.

[69] 2023 Cybersecurity Skills Gap. Global Research Report, Fortinet, 2023.

[70] Security Outcomes Report (Volume 3), Cisco, 2023.

[71] 2023 Global Threat Report, CrowdStrike, 2023.

[72] Key cybersecurity skills gap statistics you should be aware of, accessed on January 26th 2024, available online at https://www.helpnetsecurity.com/2024/01/02/cybersecurity-skills-gap-statistics/, 2024.

[73] M. H. Maras, S. Jain, H. Johnson and M. Khodjaeva, "How Educational Institutions Can Help Fill the Cybersecurity Workforce Gap," Security Management (ASIS International), 2022.

For Peer Review Only

[74] NICE Strategic Plan (2021-2025) for US, accessed on 26th January 2024, available online at https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan/, 2021.
[75] NICE strategy 2021 to 2026 for UK, accessed on January 26th 2024, report available online at https://www.nice.org.uk/Media/Default/Get-involved/Meetings-In-Public/Public-board-meetings/Mar-24-pbm-NICE-strategy-2021-2026.pdf, 2021.
[76] Which countries have the worst (and best) cybersecurity? Global rankings, accessed on January 26th 2024, available online at https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/, 2024.
[77] Cybersecurity in higher education 2.0: Closing a (gaping) industry skills gap, accessed on January 26th 2024, available online at https://www.hackthebox.com/blog/state-of-cybersecurity-in-higher-education/, 2023.
[78] P. J. Roig, S. Alcaraz, K. Gilly, C. Bernad and C. Juiz, "Design and Assessment of an Active Learning-Based Seminar," Education Sciences, vol. 14(4), 371 (2024).
[79] European CyberCup Learn-A-Thon, accessed on January 26th 2024, available online at https://www.netacadlearnathon.com/projects/europeancybercup-2023/, 2023.
[80] Papanikolaou, A., Karakoidas, V., Vlachos, V., Venieris, A., Ilioudis, C. and Zouganelis, G., 2011, September. A Hacker's Perspective on Educating Future Security Experts. In 2011 15th Panhellenic Conference on Informatics (pp. 68-72). IEEE.
[81] Papanikolaou, A., Vlachos, V., Venieris, A., Ilioudis, C., Papapanagiotou, K. and Stasinopoulos, A., 2013. A framework for teaching network security in academic environments. Information Management & Computer Security, 21(4), pp.315-338.

For Information and Computer Security

Homepage of the on-line platform hosting the cybersecurity courses

967x454mm (47 x 47 DPI)