Understanding Cybersecurity Education Gaps in Europe

Sara Ricci, Simon Parker, Jan Jerabek, Yianna Danidou, Argyro Chatzopoulou, Remi Badonnel, Imre Lendak, and Vladimir Janout

***Abstract*—Demand for cybersecurity professionals from industry and institutions is high, driven by an increasing digitization of society and the growing range of potential targets for cyber attacks. However, despite this pressing need a significant shortfall in the number of cybersecurity experts remains and a discrepancy has emerged between the skills introduced through education and those required in professional settings. In this article, a political, economic, social, technological, legal, and environmental (PESTLE) analysis was utilized to explore the factors impacting cybersecurity education in Europe. The PESTLE analysis enabled the categorization of factors affecting cybersecurty education and skills and allowed for cybersecurity professionals to assess the relevance of the factors at a national-level and European-level. Utilizing the concept of modularity from social network analysis, the interconnectivity of factors was also considered. Finally, a European-level stakeholder survey was conducted to verify the findings. As a result of the above process, a lack of societal awareness of cybersecurity was identified as a major challenge to education, along with a lack of EU-level certification. It should be noted that significant differences between factors perceived as impacting cybersecurity education were found between countries suggesting a need for local solutions to the problem.**

***Index Terms*—Cybersecurity education, cybersecurity skills gap, political, economic, social, technological, legal, and environmental (PESTLE) analysis, social network analysis.**

Manuscript received 15 July 2022; revised 19 May 2023; accepted 2 December 2023. Date of publication 4 January 2024; date of current version 9 April 2024. This work was supported in part by the ERASMUS+ Programme of the European Union under Grant 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B "REWIRE"; in part by the Ministry of the Interior of the Czech Republic under Grant VJ03030003 through Program IMPAKT 1; in part by the German Research Foundation (DFG)—NFDI 1/1 "GHGA—German Human Genome Phenome Archive"; and in part by the Project Strengthening the EIT Digital Knowledge Innovation Community in Hungary under Grant 2021-1.2.1-EITKIC-2021-00006, and implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed through the 2021-1.2.1-EIT-KIC Funding Scheme. *(Corresponding author: Sara Ricci.)*

Sara Ricci, Jan Jerabek, and Vladimir Janout are with the Department of Telecommunication, Brno University of Technology, 616 00 Brno, Czechia (e-mail: ricci@vut.cz; jerabekj@vut.cz; xjanou19@vut.cz).

Simon Parker is with the German Cancer Research Center, Deutsches Krebsforschungszentrum, 69120 Heidelberg, Germany (e-mail: simon.parker@dkfz-heidelberg.de).

Yianna Danidou is with the Centre of Excellence in Risk and Decision Science, European University Cyprus, 2404 Nicosia, Cyprus (e-mail: y.danidou@euc.ac.cy).

Argyro Chatzopoulou is with the IT Services and IT Consulting, APIROPLUS Solutions Ltd., 3085 Limassol, Cyprus (e-mail: ac@apiroplus.solutions).

Remi Badonnel is with the University of Lorraine, Loria/Inria, 54506 Vandoeuvre-lés-Nancy, France (e-mail: badonnel@loria.fr).

Imre Lendak is with the Faculty of Technical Sciences, University of Novi Sad, 21000 Novi Sad, Serbia, and also with the Data Science and Engineering Department, Eötvös Loránd University, 1117 Budapest, Hungary (e-mail: lendak@uns.ac.rs).

Digital Object Identifier 10.1109/TE.2023.3340868

I. Introduction

IMPROVING the availability, accessibility, and quality of cybersecurity education will play a pivotal role in tackling the current global cybersecurity skills shortage [1]. In 2021, the $(ISC)^2$ [2] estimated that there was a global shortfall of approximately 2.7 million cybersecurity experts. Although globally, the gap had decreased from 3.1 million to 2.7 million in 2021, in Europe this small improvement was not consistently felt, with some nations and sectors able to address the issue more quickly than others.

Recent reports from global associations [2], [3], European organizations [4], [5], and European projects [6], [7], [8], [9] have also highlighted the importance of this matter as well as possible causes of, and solutions to, current challenges within cybersecurity education. ENISA [4] has argued that many of the current cybersecurity educative issues could be overcome by redesigning educational and training pathways. Work by ECSO [5] suggests that cybersecurity education is often viewed as a specialization or "add-on" to a computer science degree, thereby failing to realize its interdisciplinary nature. Despite these reports, the reasoning for the failure to produce a sufficient number of cybersecurity professionals is not fully understood. The challenges faced vary by country and sector [2] making the identification of underlying factors, and the interconnections between, them difficult.

A political, economic, social, technological, legal, and environmental (PESTLE) analysis was implemented to facilitate a better understanding of this problem by categorizing the underlying causes as either PESTLE factors [10]. Such analyses are a common part of development frameworks as they provide an easy-to-use method to reveal and understand gaps and challenges from multiple perspectives. As such, PESTLE is a useful way to conceptualize the multifaceted challenges of cybersecurity education. The PESTLE analysis that was performed also permits the creation of a common taxonomy of challenges for the development of future research and activities.

The remainder of this article is organized as follows. Section II briefly reviews PESTLE analysis as a tool and its usage within the cybersecurity domain. Section III introduces

the PESTLE analysis implemented for analyzing the gaps in cybersecurity education. Section IV provides the statistical results of the further analysis conducted at European and country levels. Section V presents the results of the survey sent out to cybersecurity stakeholders to facilitate the identification of cybersecurity skill gaps and needed competencies. The final section contains the conclusions.

II. PESTLE and Cybersecurity Education

In order to ensure the presented analysis is as exhaustive as possible, several reports and articles related to this topic were considered. The proposed PESTLE analysis can be understood as a summary of the current state of cybersecurity education-related research. In this section, the focus will be on reviewing research that utilized a PESTLE analysis approach to explore cybersecurity education. For a more comprehensive review of cybersecurity education-related publications see Sections III and IV.

A PESTLE approach is often used for market analysis [10], or as part of a risk management process. Baghdasarin [11] employed PESTLE in conjunction with strengths, weaknesses, opportunities, and threats (SWOT) analysis. SWOT explores the environment from a slightly different perspective, splitting it into internal and external portions. In [12], PESTLE is presented as a way to identify social limitations and to coordinate the requirements of stakeholders. Blum mentions PESTLE in [13] as a critical component to consider when setting up the context of a risk program, such as Open FAIR [14] or ISO31000:2018 [15]. In [16], the analysis helped them to highlight major aspects affecting Sri Lanka's national security. In [17], PESTLE was used as part of the design process for an identity access management tool (IAM). PESTLE was presented in the form of a mind map for the development of new ideas. Simpson et al. [18] implemented PESTLE in the field of e-learning in healthcare professional education. In their article, PESTLE uncovered characteristics affecting the Scottish higher-education system.

It is important to note that there are several analytical strategies that are used in business analyses. In this study, a form of external environment analysis was utilized since these allow analysts to identify and then address changes that may arise [10]. There are two commonly used techniques for conducting such external environment analyses: 1) PESTLE analysis or 2) Porter's 5 forces analysis. In particular, Porter's 5 Forces is used to examine where power lies in a specific domain whereas PESTLE identifies the macro-external factors affecting an organization. Due to the multidisciplinary nature of cybersecurity, it was felt that a PESTLE approach would give us the best overview of the different environments involved.

In conclusion, PESTLE is a well-established tool that is currently in use, albeit separately, both in education and also the cybersecurity industry. To the best of research team knowledge, the results, which were presented in [19] and also partly in [20], are the first to target cybersecurity education with a particular focus on the European-level using this approach.

A. Contributions

The PESTLE analysis methodology was introduced and evaluated in [20] and developed during the REWIRE project [19]. 31 factors affecting cybersecurity education were identified, defined, and briefly described. Moreover, the factors were analyzed from the perspective of 11 European countries.

This article seeks to build on the conclusions of previous work by:

1) improving the descriptions of the factors by providing new up-to-date and primarily European-related references;
2) extending the country-level analysis with more statistics and with the addition of two factors. This enables us to present a more comprehensive view of the situation across Europe from a variety of national (i.e., local) perspectives;
3) developing a social network analysis approach allowing the visualization of connections among factors through the generation of a network map. Four broader areas were identified within wider networks of connected factors. This helped to reveal which factors are connected across categories and to describe how they are mutually dependent in a particular country. It should be noted that the linkages are validated by national references;
4) applying the PESTLE schema and the social network analysis at the European-level by evaluating the findings of the four winning pilot projects (i.e., CONCORDIA, CyberSec4Europe, ECHO, and SPARTA). This strengthens and consolidates the analysis by supporting the previous results;
5) soliciting responses from cybersecurity stakeholders regarding the prioritization of factors by conducting a questionnaire survey.

Notably, statistical approaches were used to view the results in a more general and comprehensive way and to reveal areas of interest. Furthermore, the linkage between identified factors helps to reveal the interconnections and the dependencies among factors in a new and novel manner.

III. PESTLE Analysis

The Cybersecurity Skills Alliance—a new vision for Europe (REWIRE) Project [9] highlighted the need for the development of a European sectorial skills strategy for cybersecurity. This need, and the shortfall in the number of trained cybersecurity professionals available, motivated us to develop a methodology for implementing a cybersecurity-education-oriented PESTLE analysis. This methodology incorporates a series of steps implemented with the contribution of all REWIRE partners. In this section, the results of the first stage of this work and the 31 identified factors are described. These aspects were identified collaboratively by experts in each PESTLE field with an extensive analysis of the state-of-the-art literature. Although a PESTLE analysis categorizes factors into one of six categories, it should not be assumed that these factors are completely unconnected. In Section IV, the authors present the approach taken to analyze the factors across

categories, exploring whether indirectly captured, broader causes exist.

A. Political Factors

The analysis of political factors assesses existing legal and other regulatory frameworks (status and trends) that can affect cybersecurity education. Political factors analyzed may include elements, such as regulations at the national, European, and global levels.

1) Lack of Relevant European Regulatory Frameworks: Several frameworks have been developed at the European-level [21]. Nevertheless, these frameworks however fail to address cybersecurity education and training in sufficient detail, leading to a lack of relevant regulatory frameworks in this area [22].

2) Lack of Coordination: There is a clear need for (national and European-level) coordination amongst stakeholders and leading institutions [23], [24]. This lack of coordination causes roadblocks in its effective implementation [4], and results in the development of training curricula that do not align well with the needs of industry.

3) Vulnerabilities of the Training Systems and Skills Shortage: Cybersecurity education needs to attract more students and to better identify the skills required in the labor market [4].

4) Political Ambition to Create Cooperation Frameworks: There is also a need for greater political efforts regarding the creation and development of cooperation frameworks amongst academia, employers, and governments [25].

5) Greater Attention to Policies Dedicated to Raise Awareness of Cybersecurity Career Paths: Currently, there is an insufficient number of policies aimed at raising awareness of career paths within the field of cybersecurity [26].

B. Economic Factors

The economic factors identified in relation to cybersecurity education can be analyzed across two distinct axes. The first axis contains challenges that are related to the design, development and maintenance of a national or European cybersecurity education framework. The second axis contains challenges that are related to individuals and organizations obtaining the relevant cybersecurity skills.

1) Economic Impact of the European Cybersecurity Educational Ecosystem: According to ISACA report [27], 55% percent of survey respondents claimed to have unfilled cybersecurity positions. This shortfall of the cybersecurity workforce capable of handling cybersecurity tasks represents an issue for both economic growth and national security [4].

2) Economic Incentives for Cybersecurity Education Programmes: EUROSTAT data [28], [29] showed that across the EU-27, 22% of all students in tertiary education were studying business, administration, or law, whereas only 5% were studying information and communication technologies. This has impacted cybersecurity education since a majority of the current curricula are delivered by engineering and computer science faculties. It is therefore important to incentivize the enrollment of practitioners in cybersecurity programmes and systematically implement awareness activities to promote them.

3) Economic Impact of Inadequate (National) Cybersecurity Capabilities: There is a very high chance that (inter)national companies and organizations do not even realize that they are falling victim to cybercrime [30]. As such, they are unable to report incidents of cybercrime to the relevant authorities. This may result in downplaying the value of cybersecurity and cybersecurity education because the perceived level of cybercrime is not representative of the actual situation.

4) Economic Impact of National Economic Resources: As the digital domain evolves, changes to the abilities and needs of the organization incur changes to the cybersecurity controls required and implemented by the organizations. This may be economically challenging for some organizations and nations [31], [32].

5) Licensing Costs of Cybersecurity Education Software: For organizations and individuals to effectively achieve cybersecurity education and training, a combination of platforms and tools are needed [5], [6]. All of these systems and services incur payable licensing costs, making it harder for organizations and individuals to invest in them. This aggravates the lack of skilled workforce by providing a financial barrier to entry [33], [34].

6) Economic Costs of Incompatible Training Platforms and Cyber Ranges: Online training platforms and cyber ranges are not designed to easily exchange exercises and scenarios [35] where the scenario development requires is difficult and costly to implement [36]. This duplicated effort and cost could be easily eliminated if the scenarios were standardized and interoperable.

7) Effects of Digital Economy on Skills Demand: The UNICTAD report [37] described how data has become a key strategic asset for the creation of both private and social value. Data are multidimensional and their use has implications not just for trade and economic development but also for human rights, peace, and security. Cybersecurity is foundational to the digital economy and the shortage of skilled professionals will limit economic growth.

C. Social Factors

Social factors consider demographics, population growth rate, age distribution, income distribution, family size, prioritization of safety, health consciousness, current lifestyle attitudes, and cultural barriers. General consumer perspectives and attitudes, the dominant view of the media, legislative changes affecting social factors, changes in lifestyle, attitude toward work, and history could also be considered here.

1) Gender Balance: A recent EU study [38] found that only 19% of people in management positions in the ICT sector are female. A limited number of women enter cybersecurity studies and a significant percentage of them drop out. This can be attributed partly to lack of support from role models, persistent stereotyped views that the sector is better suited to men, a lack of understanding about what cybersecurity jobs entail, and in some cases, how easy or difficult they find the

topics studied [22], [39]. Gender balance affects the diversity in thinking and problem-solving in cybersecurity.

2) Diversified Workforce: A 2018 American study [40] revealed that minority representation within the cybersecurity profession is slightly higher than in the overall workforce. This also impacts upon leadership where different problem-solving approaches can more effectively mitigate the risks [41].

3) Lack of Dedicated Curricula and Training and No Clear Identification of Skills: The absence of an established quality accreditation authority on cybersecurity, of leading technical thinkers, industry, and government in the process of curriculum development, makes it a mix-and-match process, from which multidisciplinary aspects are often missing and new trends and directions are unlikely to be incorporated in the curriculum [42]. This leads to a lack of applicants for cybersecurity degrees, and as a result, to a shortage of qualified cybersecurity professionals (a quantitative issue) [43]. There is also a mismatch between the industry's expectations and the skills of graduates (a qualitative issue) [44], [45].

4) Stereotypes and Misconceptions of Cybersecurity: This factor refers to the existence of several cybersecurity stigmas and misconceptions which have a negative impact on the cybersecurity industry and its broader role in society [22]. The main identified stereotypes are that: 1) new curricula are often viewed as an add-on to more mainstream computer science and fail to realize the critical importance of the interdisciplinary nature of this area [22]; 2) young people consider cybersecurity as a field more aimed at the public and less at the private sector; 3) a lack of a clear cybersecurity career paths; and 4) cybersecurity is an emergent career with a relatively young workforce. The latter is related to the limited potential for the older generation to encourage and support the development of new workers in this area. Cybersecurity is often considered to be a highly technical discipline, however the current key gaps in industry reveal that there is also a need for nontechnical cybersecurity personnel [24].

5) Social Impact: Alongside the rise of online platforms where individuals could gather, spend, and share information, came the rise of online cybercrime that takes advantage of individuals and whole communities [46]. This has necessitated a greater interaction between society and cybersecurity and requires an increase in cybersecurity awareness by the wider public.

6) Social Awareness: Although cybersecurity is one of the most important challenges faced by governments today, its visibility and public awareness of it remains limited. Communicating the need for, and importance of, cybersecurity is beset with paradoxes, which have resulted in society not taking appropriate measures to deal with the threats [47].

D. Technological Factors

Technological factors are variables which concern the existence, availability, and development of technology that influence the need for, and the possibilities of, cybersecurity education.

1) Cyber Ranges: A cyber range [48] is a virtual environment which emulates real-world scenarios and is an important technological method for training groups of security professionals [49]. A majority of the commercial cyber ranges can only be obtained under expensive licensing agreements. Furthermore, the usability of cyber ranges is significantly hindered by a lack of interoperability [50].

2) Availability of Tools: Hardware and software tools are essential for providing hands-on experience about the configuration, and therefore the potential vulnerabilities, of software systems [51], [52], [53]. Common virtualized training platforms would enable the sharing of resources and best practice among education providers [49].

3) Digitization of Society: Digitization of society refers to the proliferation of connectivity and computing within basic societal functions, such as critical infrastructures, home automation, finances, home entertainment, personal communication, and business transactions [54]. The ability to collect, use, process, and analyze vast amounts of digital data also increases the likelihood of attacks, and enables new attack vectors to be developed [55], [56].

4) Emerging Technologies: There are a number of emerging technologies which have the potential to change the way computers, networks, systems are operated, and will require a redesign of current security curricula. Examples include quantum computing [57], machine learning [58] and cyber–physical systems [59]. The requirement for the content of curricula to respond to the evolution of the field is an ongoing challenge for cybersecurity education [45].

5) Generalization of Cyber Attacks: Given the increased digitization of society, there is a significant broadening of the scope and diversity of cyber attacks. There is also a lack of differentiation between low-tech attacks (i.e., spam, phishing, and ransomware) and high-tech attacks (i.e., APT,[1] and zero-day exploits) [60]. Education has to be continuously updated with respect to the new threat landscape so as to prepare the future cybersecurity workforce for new types of more complex types of cyber attacks.

E. Legal Factors

Legal factors may be both external and internal to organizations, institutions, and governments. Certain laws will affect cybersecurity or the business environment in a particular country whilst simultaneously, they are also likely to affect the implementation of internal security policies and controls. The legal analysis takes into account both, and charts out the strategies taken in light of such mandates (e.g., cybersecurity laws, personal data protection laws, and consumer laws). During the analysis, five legal aspects were identified. The following sections briefly describe these aspects and how they impact upon cybersecurity education.

1) Lack of European Certification: Certification [61], [62] is a well-established and traditionally used means to define and formalize desired properties and the best practices to achieve them. Cybersecurity certification of products, services, and processes is currently only used to a limited extent [44], and is focused at the member state-level, or on systems that have been introduced by the needs of given industries.

[1] Advanced Persistent Threats.

2) Lack of Legal Framework Unification: Europe lags behind other regions in the development of a comprehensive approach for defining a set of roles and skills relevant to the cybersecurity field [4], [63]. Many security attacks are orchestrated across multiple jurisdictions and originate from non-EU countries.

3) Knowledge Gap of Legal Requirements in Personal Data Protection: Europe's general data protection regulation (GDPR) [64] is perhaps the most wide-ranging and comprehensive piece of data privacy legislation currently in effect. The GDPR requires data controllers and processors to use proportionate security measures when working with personal data.

4) Standardization of Cybersecurity Roles Definition and Cybersecurity Skills Across Europe: The skills required to effectively perform the multitude of possible cybersecurity roles [4] are not formally defined and mapped. Universities and associations have created a variety of possible qualifications that may or may not be suitable for certain cybersecurity roles. The existence of specific qualification bundles [65] linked with specific cybersecurity roles and equivalents is considered a pending issue which requires mitigation through standardization initiatives.

5) Missing Comprehensive Cybersecurity Officer Role Description: Whilst data protection officers have a clear definition in the GDPR [66], there is not a similar comprehensive role description for cybersecurity officers.

F. Environmental Factors

Environmental factors include all those issues and conditions that influence or are determined by the surrounding environment. Factors of a business environmental analysis include, but are not limited to, climate, weather, geographic location, global changes to climate, environmental offsets, etc. As with all other factors, the definitions below describes how the environmental conditions and available projections, at the time of this research, influence cybersecurity and cybersecurity education.

1) Climate Change and Related Effects: Climate change leads to extreme weather events that affect ICT infrastructure and threaten the viability and operations of ICT infrastructures. Cybersecurity teams need to acquire knowledge and skills to respond to such events and strengthen organizational resilience. Furthermore, the International Organization for Migration estimates that 200 million people could be forced to leave their homes due to environmental changes by 2050 [67]. This migration could have multiple effects on society in general.

2) COVID-19 Pandemic Crisis: The restrictions imposed in response to the coronavirus pandemic have encouraged (or mandated) employees to work from home. As a consequence, technology has become even more important in both professional and personal lives. Cybersecurity education and training is a crucial resilience parameter, though its implementation is hindered by the necessity that it has to be conducted remotely [68].

3) Connected Devices Controlling Environmentally Sensitive Productions: Legacy industrial control system (ICS) devices bring forth new threats and risks since as unlike previously, they are networked, introducing a new and interesting attack point for adversaries. The effects of a successful attack to these systems could be numerous and may include environmental disasters [69].

IV. Analysis of Identified Factors and Their Correlations

As shown in Section III, the PESTLE analysis recognized 31 factors that appear to affect cybersecurity education. To further strengthen this outcome, the identified factor at a national-level were evaluated and the 4 European pilots outcomes were analyzed, i.e., Concordia, Cybersec4Europe, Echo, and Sparta. Section IV-A depicts the factors identified by the considered European countries and Section IV-B presents the results of the pilots' overview. In both cases, statistical analyses were performed on the collected data.

A. Country-Level Analysis

Representatives from 11 European countries were requested to 1) review the 31 identified factors; 2) identify if and how they affect cybersecurity education within their country; and 3) identify possible existing dependencies or connections amongst the factors. The countries represented in the survey were: Austria, Cyprus, the Czech Republic, France, Lithuania, Greece, Hungary, Portugal, Serbia, Spain, and Sweden. By utilizing the factors described in Section III as a common taxonomy, it was possible to explore the differences between the countries through the variation of the factors identified as impacting cybersecurity education. It was also possible to investigate the interconnectivity of the factors in order to ascertain the validity of the division of factors within the PESTLE framework.

For the analysis of the collected information, three metrics were considered: 1) the number of connections to other factors; 2) the importance of each factor according to the respondents; and 3) the number of countries that identify at least one of these connections. Due to the volume of the information, the representation of the information is split into Tables I and II.

Factors with more connections can be interpreted as those shortages, gaps, and mismatches that have a greater impact on cybersecurity education because they affect the greatest number of the other recognized factors.

Two factors were identified as having the most connections to other factors, "26. Knowledge gap of legal requirements in personal data protection," and "31. Connected devices controlling environmentally sensitive productions."

Fig. 1 depicts the PESTLE analysis performed for Czechia, Serbia, and Greece. Each numbered rectangle represents one factor. The correspondence between numbers and factors can be found in Section III.

In Fig. 1, colored rectangles depict factors recognized as being of primary relevance, gray rectangles with colored borders represent factors that were considered to be dependent on the primary factors, and plain gray rectangles are factors not identified by respondents in the country. The lines show the links between factors.

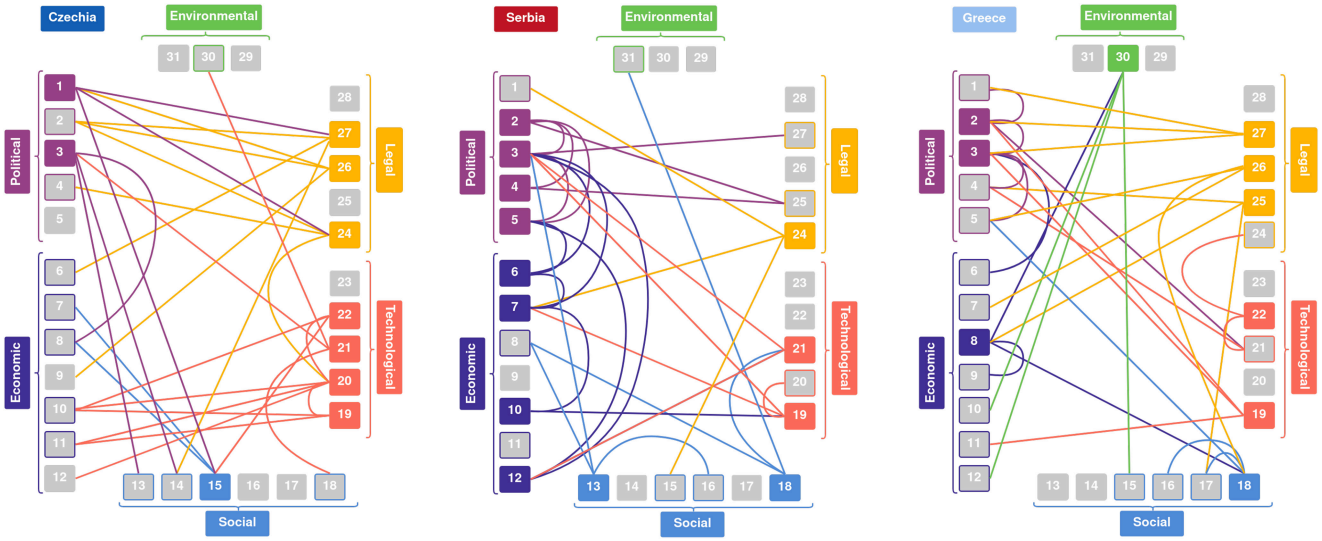

Fig. 1. Comparison of Czechia, Serbia, and Greece PESTLE interconnections.

TABLE I
POLITICAL, ECONOMIC, AND SOCIAL FACTORS WITH NUMBER OF CONNECTIONS (CONN.), THEIR IMPORTANCE (IMPORT.), AND NUMBER OF COUNTRIES IDENTIFYING THEM (STATE)

Factors	Conn.	Import.	State
Political			
1. Lack of relevant European regulatory frameworks	12	Medium	5
2. Lack of coordination	13	Medium	4
3. Vulnerabilities of the training systems/Skills shortage	11	Medium	7
4. Political ambition to create cooperation frameworks	13	High	2
5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	5	Medium	2
Political connections in total	54		
Economic			
6. The economic impact of the European cybersecurity educational ecosystem	3	Medium	2
7. Economic incentives for cybersecurity education programs	7	Medium	2
8. Economic impact of inadequate (national) cybersecurity capabilities	6	High	2
9. The economic impact of National economic resources	1	High	1
10. Licensing costs and different licensing models of software	3	Medium	2
11. Economic costs of incompatible training platforms and cyber ranges	1	Medium	1
12. Effects of digital economy on skills demand	4	Medium	2
Economic connections in total	25		
Social			
13. Gender balance	6	Medium	5
15. Lack of dedicated curricula and training and no clear identification of skills	10	Medium	5
16. Stereotypes and misconceptions of Cybersecurity	6	Medium	2
17. Social impact	6	Medium	3
18. Social Awareness	12	High	6
Social connections in total	40		

TABLE II
TECHNOLOGICAL, LEGAL, AND ENVIRONMENTAL FACTORS WITH NUMBER OF CONNECTIONS (CONN.), THEIR IMPORTANCE (IMPORT.), AND NUMBER OF COUNTRIES IDENTIFYING THEM (STATE)

Factors	Conn.	Import.	State
Technological			
19. Cyber Ranges	7	Medium	6
20. Availability of Tools	6	Medium	4
21. Digitalization of Society	6	Medium	4
22. Emerging Technologies	9	High	4
23. Generalization of cyber attack	12	High	2
Technological connections in total	40		
Legal			
24. Lack of European Certification	10	Medium	6
25. Lack of legal framework unification	5	Medium	3
26. Knowledge gap of legal requirements in personal data protection	14	Medium	7
27. Standardisation of cybersecurity roles definition and cybersecurity skills across European Union	10	High	3
Legal connections in total	39		
Environmental			
30. COVID-19 pandemic crisis	7	High	4
31. Connected devices controlling environmentally sensitive productions	14	High	2
Environmental connections in total	21		

In Serbia and Greece, political factors were the most significant, indeed all political factors were identified as primary factors, or linked to, and they account for the greatest number of connections in the diagrams. The large number of connections between political factors and others that focus on cooperation and coordination suggests that there may be a broader overarching factor relating to a lack of cybersecurity governance at national and European level. In contrast, Czechia differed from Serbia and Greece in that technological factors were perhaps the most prominent based on their level of primary identification and their number of connections.

As shown in Fig. 1, similarities and discrepancies can be found in the analyses depending on the countries. For instance, Greece is the only country among the three selected that identified an environmental factor as a primary factor. Nevertheless, this factor was also identified in Cyprus,

Hungary, and Spain. Please see Tables I and II for more details. Undoubtedly "3. Vulnerabilities of the training systems and skills shortage" is a factor requiring further research in the future as it was regularly identified as a primary factor, and was frequently linked to other factors. This finding highlights how a PESTLE analytical approach can help focus future research by identifying broad issues that may be obscured if researchers focus narrowly on individual factors or do not analyze data from multiple contexts.

Tables I and II list the identified national-level PESTLE factors. Remarkably, each country identified a majority of the highlighted factors. Only 3 factors were not identified directly within the national data: "14. Diversified workforce;" "28. Missing comprehensive cybersecurity officer role description;" and "29. Climate change and related effects" belonging to the social, legal, and environmental areas, respectively.

It should not be interpreted that these three factors were seen as irrelevant by the respondents; factors that were not directly identified may have been noted as connecting to other factors. For instance, "14. Diversified workforce," is not included in Table I, but was reported to be connected to "27. Standardization of cybersecurity roles definition and cybersecurity skills across the European Union." This can instead be interpreted as Factor 27 is perceived to be of major importance, whereas Factor 14 is a related issue of secondary-importance within the revised national document.

During this further analysis, the respondents from Cyprus defined two new Social factors that were not listed on the proposed PESTLE factors. It is important to mention them here since they will be part of the evaluation presented below.

1) Fragmentation of Cybersecurity Training and Certification for Professionals: Currently, different professional qualifications are offered in the EU. This creates a fragmentation of cybersecurity training and certifications and is likely to stem from the lack of an EU regulatory framework [70]. This factor is presented as a connection of "1. Lack of relevant European regulatory frameworks."

2) Cybersecurity Training for Lower Ages: Cybersecurity and related definitions should be introduced into secondary education allowing students to be aware of cybersecurity earlier, and as they are better acquainted with this field, they may be more likely to engage professionally with cybersecurity in their later career [70]. Notably, the sooner people are engaged with cybersecurity, the greater the benefit returned to society. This factor is presented as a connection of "16. Stereotypes and misconceptions of Cybersecurity" and "17. Social impact."

The importance of each factor has been computed on average according to the respondents' answers. This value is shown in Tables I and II. This metric represents the current consciousness on the issue. As it would be expected, "Number of Connections" and "Importance of Aspect" are often proportionally related; a larger number of connections is associated with greater perceived importance.

Finally, the metric of the number of countries identifying the factor is considered. For instance, the Political factor "3. Vulnerabilities of the training systems and skills shortage" was nominated by the largest number of countries. This metric gives relevance to those factors that are more commonly perceived across Europe and potentially worldwide. Note that the Environmental factor "30. COVID-19 pandemic crisis" has only seven connections but it is considered of high importance. This is due to the fact that the COVID-19 pandemic is currently affecting daily life in Europe and worldwide, and therefore, it is currently keenly felt by the respondents. Aside from the present disruption however, the lack of connections to other factors perhaps suggests that its impact is not expected to be long-lived with respect to cybersecurity education.

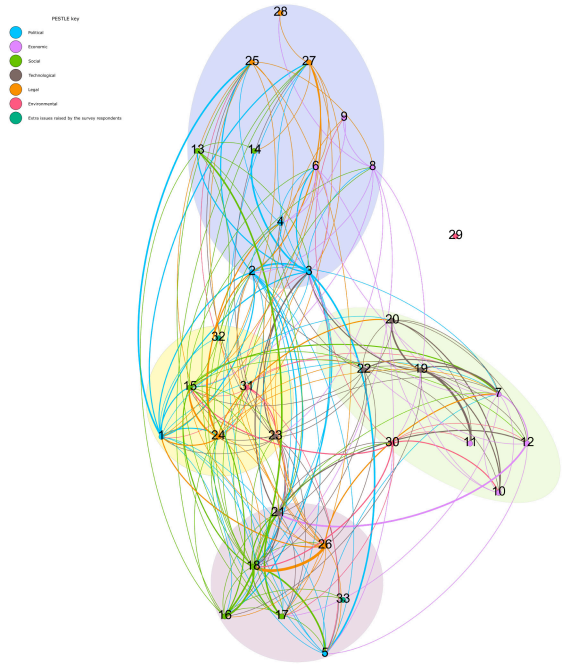

Fig. 2. Modularity analysis of REWIRE data.

As previously stated, it should not be assumed that the categories of a PESTLE analysis are completely independent from one another. For example, it may be expected that political factors both reflect and influence social factors, and so a separation of factors in a PESTLE analysis may obscure their interconnected nature. It was hypothesized that there might be broader factors affecting cybersecurity education indirectly captured in the results. These broader factors would be implied by the overlap between factors that had been assigned to different PESTLE categories. To test for this, the concept of modularity drawn from social network analysis was utilized. Modularity is a technique used to identify subgroups within wider networks of connected nodes. Using the information relating to the connections between factors, it was possible to generate a network map of the factors and identify the groups of factors which may be subfactors of those broader factors using the modularity algorithm included in the Gephi software package [71]. The network map generated can be seen in Fig. 2. A higher-resolution image can be made available upon request.

As depicted by the colored regions, four broader factor groups were identified, each containing multiple factors from multiple PESTLE categories. Factor 29 is an outlier and was not found to be part of any broader groups. The factors

TABLE III
FOUR BROADER FACTOR GROUPS IDENTIFIED BY THE MODULARITY ALGORITHM

Blue Group - Failure of stakeholders to cooperate
2. Lack of coordination 3. Vulnerabilities of the training systems and skills shortage 4. Political ambition to create cooperation frameworks 6. The economic impact of the European cybersecurity educational ecosystem 8. Economic impact of inadequate (national) cybersecurity capabilities 9. Economic impact of national economic resources 13. Gender balance 14. Diversified workforce 25. Lack of legal framework unification 27. Standardisation of cybersecurity role definition and cybersecurity skills across Europe 28. Missing comprehensive cybersecurity officer role description
Yellow Group - Lack of a skills framework
1. Lack of relevant European regulatory frameworks 15. Lack of dedicated curricula and training and no clear identification of skills 23. Generalisation of cyber attacks 24. Lack of European certification 31. Connected devices controlling environmentally sensitive productions 32. Fragmentation of cybersecurity training and certification for professionals
Green Group - Lack of training resources
7. Economic incentives for cybersecurity programs 10. Licensing costs of cybersecurity education software 11. Economic costs of incompatible training platforms and cyber ranges 12. Effects of digital economy on skills demand 19. Cyber ranges 20. Availability of tools 22. Emerging technologies 30. COVID-19 pandemic crisis
Mauve Group - Low level of societal interest in cybersecurity
5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths 16. Stereotypes and misconceptions of cybersecurity 17. Social impact 18. Social awareness 21. Digitisation of society 26. Knowledge gap of legal requirements in personal data protection 33. Cybersecurity training for lower ages - secondary education curriculum

were grouped as shown in Table III. From the groupings of factors identified through the modularity analysis, it can be hypothesized that there are perhaps four broader factors which are contributing to the current challenges regarding cybersecurity education. Presently, these have been termed as: 1) failure of stakeholders to cooperate; 2) lack of a skills framework; 3) lack of training resources; and 4) lack of societal interest in cybersecurity. Further research is required in the future to ascertain if these broader factors can be identified in other data and what their impact might be.

B. European-Level Analysis

CONCORDIA, CyberSec4Europe, ECHO, and SPARTA[2] are four winning pilot projects among the 12 eligible proposals that the European Commission received for the Horizon 2020 call SU-ICT-03-2018.[3] This call had the aim of "establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research and Innovation Roadmap." The pilot projects are composed of more than 160 partners from 26 EU Member States and include big companies, Small and Medium Enterprises (SMEs), universities, and cybersecurity research institutes. The pilots' outcomes can be considered a proto-analysis of the current European cybersecurity development and the main issues encountered by European experts in the sector.

[2]please check, respectively, https://www.concordia-h2020.eu/, https://cybersec4europe.eu/, https://echonetwork.eu/, and https://www.sparta.eu/.

[3]https://ec.europa.eu/programmes/horizon2020/en

TABLE IV
POLITICAL, ECONOMIC, AND SOCIAL FACTORS WITH NUMBER OF CONNECTIONS, THEIR IMPORTANCE, AND NUMBER OF PILOTS IDENTIFYING THEM

Factors	Conn.	Import.	Pilots
Political			
2. Lack of coordination	4	High	2
3. Vulnerabilities of the training systems/Skills shortage	3	Medium	1
4. Political ambition to create cooperation frameworks	7	Medium	2
Political connections in total	14		
Economic			
6. The economic impact of the European cybersecurity educational ecosystem	2	Medium	1
10. Licensing costs and different licensing models of software	2	High	1
Economic connections in total	4		
Social			
13. Gender balance	4	Medium	3
14. Diversified workforce	2	Medium	1
15. Lack of dedicated curricula and training and no clear identification of skills	9	High	3
16. Stereotypes and misconceptions of Cybersecurity	3	Medium	1
17. Social impact	2	High	1
18. Social Awareness	7	Medium	3
Social connections in total	27		

The REWIRE project builds on the pilots' outcomes and in the current consortium at least one partner belongs to both the REWIRE project and one of the pilots. This has enabled the REWIRE project to access all of the pilots' data, including that not previously published. Here, representatives of the pilots analyzed the outcomes of the PESTLE analysis described within this document. In particular, they 1) reviewed the factors; 2) identified if and how they affect cybersecurity education from their perspective; and 3) identified possible existing dependencies (connections) amongst factors.

Tables IV and V depict the identified PESTLE factors by the pilots' analyses. A total of 20 factors of the 31 recognized in Section III were identified by the pilots as existing in the European environment. Remarkably, all 6 Social factors were identified by the respondents in combination. The pilot studies identified approximately two-thirds of the factors utilized in the REWIRE project. The results are summarized in Tables IV and V.

As in Section IV-A, it should be noted that if a factor is not mentioned in Tables IV and V, it is not equivalent to no connection being identified with it. The factor "24. European Certification lack" has the highest number of interconnected factors (total of 10). Interestingly, it is linked to factors from all

TABLE V
TECHNOLOGICAL, LEGAL, AND ENVIRONMENTAL FACTORS WITH NUMBER OF CONNECTIONS, THEIR IMPORTANCE, AND NUMBER OF COUNTRIES IDENTIFYING THEM

Factors	Conn.	Import.	Pilots
Technological			
19. Cyber Ranges	7	Medium	4
20. Availability of Tools	5	Medium	3
21. Digitalization of Society	2	High	1
22. Emerging Technologies	2	Medium	1
Technological connections in total	16		
Legal			
24. European Certification lack	10	Medium	4
25. Legal framework unification lack	3	Medium	1
26. Knowledge gap of legal requirements in personal data protection	5	Low	2
27. Standardisation of cybersecurity roles definition and cybersecurity skills across European Union	2	Medium	1
Legal connections in total	20		
Environmental			
30. COVID-19 pandemic crisis	5	Medium	3

TABLE VI
SUMMARY STATISTICS FROM MODULARITY ANALYSES

Study	Factors Identified	Overlap with REWIRE
Concordia	25	52%
CyberSec4Europe	17	71%
ECHO	19	63%
SPARTA	22	59%

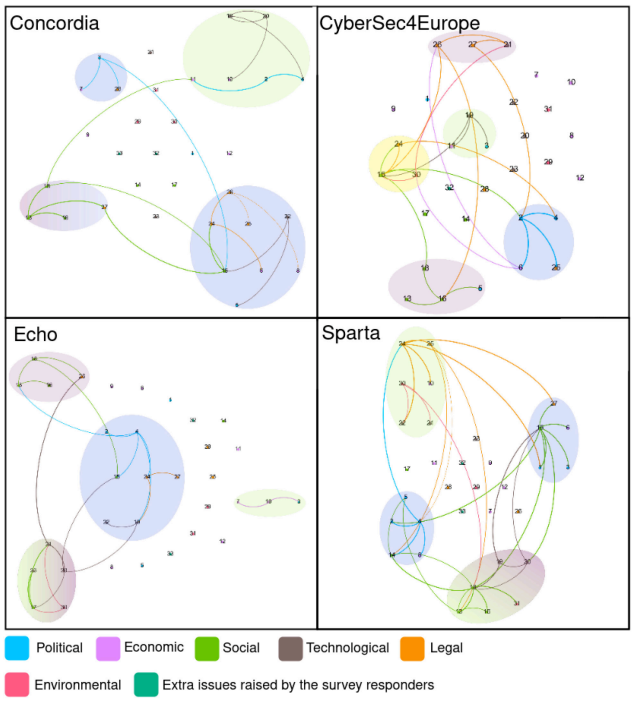

Fig. 3. Modularity analysis of Concordia, CyberSec4Europe, ECHO, and SPARTA data.

other categories, except the Environmental group. Therefore, based on pilots' findings, it seems that this issue is critical and should be addressed. From this perspective, factors with more connections are recognized by pilots' experts as core issues to be addressed by the cybersecurity field.

There are two factors identified by all 4 pilots, these are "19. Cyber Ranges" and "24. European Certification lack." There is a broad consensus on the importance of these issues. In the case of Factor 24, it can be interpreted as confirmation of the importance of this factor. In the case of Factor 19, it highlights that Technological factors that should not be overlooked.

Fig. 3 displays the modularity networks for the responses of the Concordia, CyberSec4Europe, ECHO, and SPARTA projects, respectively. The colored regions again show the groups proposed by the modularity algorithm. These regions have been coded in such a way so that the color matches the region in Fig. 2 that a majority of the factors belong to; in the event that the factors were as closely linked to two regions, the colors were combined. As there is less underlying data, the networks are noticeably more sparse with many isolated factors. However, there is some overlap with the categories seen for the REWIRE data.

The analysis of the Concordia, CyberSec4Europe, ECHO, and SPARTA groups found considerable overlaps between the groups identified for each study and those generated through the analysis of data from REWIRE. Summary statistics from this can be seen in Table VI. As it can be seen in the table, the overlap between the analysis of data from CyberSec4Europe and REWIRE was strongest (71% of factors were judged to be in the same modularity regions) with slightly smaller correlations found for the Concordia, ECHO and SPARTA data. This may in part be because the grouping "Lack of a skills framework" was completely missing from these three analyses as it was not discovered by the modularity algorithm. The large overlap for all four additional analyses can perhaps lend support for the broad categories of factors defined using Fig. 2. That similar groups were found in the pilot studies does suggest that the broader categories defined previously do represent actual phenomena. This further supports the view that more research into these broad categories is required. It should be noted however that many factors were not identified through the limited data collection for the pilot studies, further data collection may elucidate whether the inclusion of the missing factors would support or contradict the performed analysis of the REWIRE data.

V. STAKEHOLDERS SURVEY

As part of this research, an online survey to collect additional information from a wider group of European stakeholders was conducted. The goal of the survey was to collect information about unfilled cybersecurity job positions, the most sought-after skills, and the ability of education providers to train the needed professionals. The respondents were asked to gauge the vacancies and skills needs in both their organizations and on the national level. A section of the survey was dedicated to the conducted PESTLE analysis. The respondents could, depending on their knowledge, either confirm the selection of the most relevant factors affecting cybersecurity education or suggest new factors. The survey was sent out to the contacts identified in the REWIRE stakeholder database in July 2021 and was run until September, 2021. In particular,

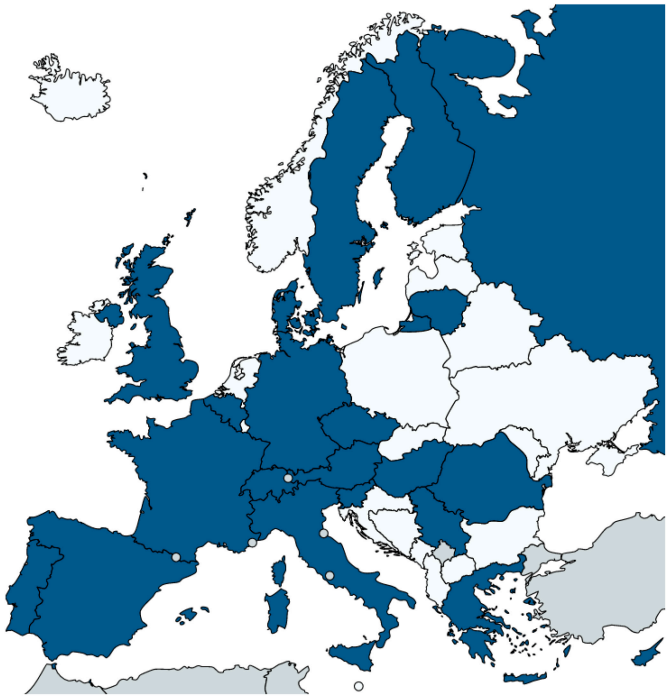

Fig. 4. Overview of countries with active participant(s) in the survey.

the REWIRE team targeted and contacted key recognized cybersecurity experts. For instance, REWIRE network counts stakeholders from ENISA, ECSO, ISC^2, and national security agencies. These stakeholders were selected based on their involvement in relevant national and international projects and initiatives in cybersecurity capacity development. Their responses were considered to be expressions of their national contexts. In this period, a total of 138 responses from 21 European countries were received and saved to a spreadsheet. Participating countries are shown in blue in Fig. 4.

Most responses were received from professionals working in higher education and/or research (44 out of 138) followed by cybersecurity companies (36 out of 138), noncybersecurity large companies (19 out of 138) and noncybersecurity SMEs (15 out of 138). As the survey was conducted as part of an EU-funded sector skills alliance project, it came as no surprise that the survey respondents were primarily trainers/professors and researchers (80 out of 138), followed by managers, consultants, analysts, engineers, and policymakers.

The survey consisted of five sections and contributed toward crafting the tools and approaches necessary to tackle Europe's cybersecurity workforce gap. The survey contained two questions related to the PESTLE analysis. The respondents were asked to rate the level of impact on cybersecurity education of the following, most frequently mentioned country-level factors from the PESTLE analysis.

1) Lack of EU coordination on cybersecurity.
2) Economic impact of low capabilities or awareness.
3) Lack of social awareness.
4) Lack of dedicated curricula and training.
5) Lack of knowledge about cyber attacks.
6) Lack of knowledge about personal data protection.
7) The COVID-19 pandemic.

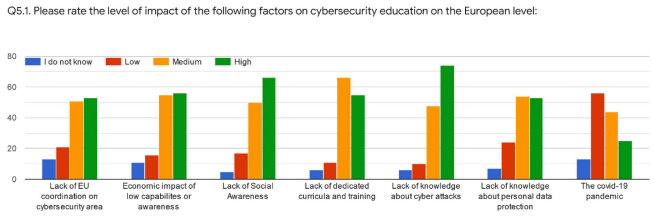

Fig. 5. Result of the evaluation of the respondents on the most mentioned aspects.

The survey results are shown in Fig. 5. The distribution of responses was found to vary significantly between questions. For most factors, respondents considered them to have a "Medium" or "High" level of impact on cybersecurity education. "Lack of knowledge about cyber attacks" and "Lack of Social Awareness" were clearly assessed as high impact factors, whereas for the other factors the difference between high and medium impact was considerably smaller. Note that the "Lack of dedicated curricula and training" factor was assessed as "Low" impact in very few responses, similarly to the highest-ranked two factors. The "Lack of knowledge about personal data protection" is still very important, particularly as the introduction of the wide-ranging GDPR (approved in 2016 and valid from 2018) has seemingly not (yet) prompted a significant change in awareness.

We also considered the COVID-19 pandemic impact due to its current and ongoing impact on cybersecurity. Somewhat surprisingly the participants considered this factor as having a low impact. This rating might be attributed to the fact that organizations became more adept at addressing and overcoming the disruption caused by the prolonged pandemic; or it might be just too soon to retrospectively assess the impact of the COVID-19 pandemic upon the training of cybersecurity professionals.

Apart from the COVID-19-related factor, the rest are closely aligned with the other findings presented in this article and validate the proposal for the high-level grouping of the PESTLE factors into 1) failure of stakeholders to collaborate ("Lack of EU coordination on cybersecurity"); 2) lack of a skills framework/training resources ("Lack of dedicated curricula and training") and a low level of societal interest (supported by the remaining non-COVID-19 factors).

VI. Conclusion

Research conducted by relevant organizations (ISC2, ISACA and other) shows that roughly three million cybersecurity experts are missing worldwide. Cybersecurity education is a significant element in most strategies developed for tackling this workforce gap. The state of the art was enhanced in this domain with a PESTLE analysis aimed at cybersecurity education. The proposed analysis identified a total of 31 different factors affecting cybersecurity education and skills development. Up-to-date and primarily European-level references were provided for each described factor. Moreover, this article details the efforts to further collect data, analyze, and formulate conclusions on the factors affecting cybersecurity education. These efforts can be split into: 1) national-level;

2) pilots'; and 3) stakeholders' reviews of the proposed PESTLE.

First, representatives from 11 European countries were asked to review the PESTLE schema and identify possible existing dependencies amongst the factors. Remarkably, each country had identified a majority of the skills shortages, gaps, and mismatches highlighted at a European-level. The PESTLE categories were found to be approximately equally relevant for the identified factors with no category being disproportionately important. However, differences in importance and identification can be found at the national-level, suggesting that any European-level efforts developed and implemented to resolve these challenges need to adapt to local contexts.

Furthermore, a network map of the factor was generated using a modularity algorithm. Four broader areas of closely linked PESTLE factors were identified: 1) failure of stakeholders to cooperate; 2) lack of a skills framework; 3) lack of training resources; and 4) low level of societal interest in cybersecurity.

Second, the same approach were applied at the European-level by evaluating the four winning cybersecurity pilot projects' (i.e., CONCORDIA, CyberSec4Europe, ECHO, and SPARTA) findings based on information collected from experts involved in these projects. Significant overlap with the categories seen for the REWIRE data was found even though the data available from the pilot projects was not as rich as the dataset created as part of the REWIRE project.

Third, a survey was sent out to the contacts identified in the REWIRE stakeholder database. This survey received a total of 138 responses spread across 21 European countries. The survey collected data about workforce gaps and skills needs in the respondents' organizations and their national contexts. The survey respondents recognized the "Lack of knowledge about cyber attacks" and their impact upon businesses as well as the "Lack of Social Awareness" as having the highest impact on cybersecurity education on the European-level, both of which align with the broader area "Lack of societal interest in cybersecurity" identified in the proposed modularity analysis.

Our PESTLE analysis generated a common taxonomy for the development of future research involving interviews and surveys. Going forward it is important to assess the utility of the broader areas identified through the modularity analyses, and it may be necessary to collect further data so that a denser network can be analyzed. This would further validate the conclusions of this study and provide a conceptual framework from which cybersecurity educative challenges could be addressed with solutions which respect the local context and differences between European countries.

REFERENCES

[1] [Online]. Available: https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

[2] "(ISC) cybersecurity workforce study." 2021. [Online]. Available: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[3] "State of cybersecurity 2020: Part 1: Global update on workforce efforts and resources." ISACA. 2020. [Online]. Available: https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf

[4] "Cybersecurity skills development in the EU." ENISA. 2019. [Online]. Available: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[5] "ECSO gaps in European cyber education and professional training." Accessed: Mar. 2, 2022. [Online]. Available: https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf

[6] "Assessing the courses for cybersecurity professionals already developed by CONCORDIA partners." 2020. [Online]. Available: https://www.concordia-h2020.eu/wp-content/uploads/2020/04/CONCORDIA-AssessmentOfCoursesT3.4-ForWebsite.pdf

[7] "SPARTA deliverables." Accessed: Nov. 26, 2021. [Online]. Available: https://www.sparta.eu/deliverables/

[8] "D6.3: Design of education and professional framework," CyberSec4Europe, Brussels, Brussels, Rep. Call H2020-SU-ICT-03-2018, 2021.

[9] "REWIRE: Cybersecurity skills alliance—A new vision for Europe." 2020. [Online]. Available: https://rewireproject.eu/

[10] J. Cadle, D. Paul, and P. Turner, *Business Analysis Techniques: 72 Essential Tools for Success*. London, U.K.: BCS, The Chartered Inst., 2010.

[11] D. Baghdasarin, "MRO cybersecurity SWOT," *Int. J. Aviation, Aeronaut., Aerosp.*, vol. 6, no. 1, p. 9, 2019. [Online]. Available: https://commons.erau.edu/ijaaa/vol6/iss1/9/

[12] A. Couce-Vieira and S. H. Houmb, "The role of the supply chain in cybersecurity incident handling for drilling rigs," in *Proc. Int. Conf. Comput. Saf., Rel., Security*, 2016, pp. 246–255.

[13] D. Blum, "Create your rational cybersecurity success plan," in *Rational Cybersecurity for Business*. Berkeley, CA, USA: Apress, 2020, pp. 297–313.

[14] "Risk analysis (O-RA)." Accessed: Apr. 13, 2021. [Online]. Available: https://publications.opengroup.org/c13g

[15] *Risk Management—Guidelines*, ISO Standard ISO 31000:2018(en), Feb. 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

[16] B. Senaratne, *Dynamics in Cybersecurity: Challenges to Sri Lankas National Security*, General Sir John Kotelawala Defence Univ., Dehiwala-Mount Lavinia, Sri Lanka, 2017.

[17] S. Hiscock. "User guardian." 2013. [Online]. Available: https://sites.google.com/site/userguardian1/investigation-and-market-research/2-6-pestle-analysis?authuser=0

[18] E. Simpson, J. Hart, A. Phillips, and D. Angus, "Higher education: Environmental analysis & industry scenarios: Scottish Universities," Aug. 2015. [Online]. Available: https://doi.org/10.13140/RG.2.1.2814.1281

[19] "WP2 PESTLE analysis of cybersecurity education." 2021. [Online]. Available: https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf

[20] S. Ricci et al., "PESTLE analysis of cybersecurity education," in *Proc. 16th Int. Conf. Availability (ARES)*, 2021, pp. 1–11.

[21] "European cybersecurity skills framework." 2020. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

[22] *Gaps in European Cyber Education and Professional Training*, Eur. Cyber Security Org., Brussels, Belgium, 2018.

[23] "Digital education action plan (2021–2027)." 2020. [Online]. Available: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

[24] "Addressing skills shortage and gap through higher education." ENISA. Nov. 2021. [Online]. Available: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

[25] "Joint communication to the European parliament and the council the EU's cybersecurity strategy for the digital decade." 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018&from=EN

[26] "Cybersecurity Education." 2020. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education

[27] "State of cybersecurity 2021, part 1: Global update on workforce efforts, resources and budgets." ISACA. 2021. [Online]. Available: https://www.isaca.org/go/state-of-cybersecurity-2021

[28] "Tertiary education statistics." 2023. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Tertiary_education_statistics#Finance

[29] "Distribution of tertiary education students by broad field and sex, EU-27, 2018 ET2020." 2020. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Distribution_of_tertiary_education_students_by_broad_field_and_sex,_EU-27,_2018%25)_ET2020.png

[30] D. P. Fidler, "Final acts of the world conference on international telecommunications," *Int. Legal Mater.*, vol. 52, no. 3, pp. 843–860, 2013. [Online]. Available: https://www.cambridge.org/core/product/identifier/S0020782900001418/type/journal_article

[31] A. Papanikolaou, V. Vlachos, A. Papathanasiou, K. Chaikalis, M. Dimou, and M. Karadimou, "A survey of cyber crime in Greece," *Telfor J.*, vol. 6, no. 2, pp. 86–91, 2014. [Online]. Available: http://scindeks.ceon.rs/Article.aspx?artid=1821-32511402086P

[32] A. Papathanasiou et al., "Legal and social aspects of cyber crime in Greece," in *E-Democracy, Security, Privacy Trust a Digital World*. Athens, Greece: Springer, 2014, pp. 153–164. [Online]. Available: http://link.springer.com/10.1007/978-3-319-11710-2_14

[33] D. Katsianis, I. Neokosmidis, A. Pastor, L. Jacquin, and G. Gardikis, "Factors influencing market adoption and evolution of NFV/SDN cybersecurity solutions. Evidence from the SHIELD project," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, 2018, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/8442845/

[34] E. Ukwandu et al., "A review of cyber-ranges and test-beds," *Sensors*, vol. 20, no. 24, p. 7148, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/24/7148

[35] V. E. Urias, W. M. Stout, B. Van Leeuwen, and H. Lin, "Cyber range infrastructure limitations and needs of tomorrow: A position paper," in *Proc. Int. Carnahan Conf. Security Technol. (ICCST)*, 2018, pp. 1–5.

[36] R. Nakata and A. Otsuka. "CyExec: Automatic generation of randomized cyber range scenarios." 2021. [Online]. Available: https://www.scitepress.org/Papers/2021/103245/103245.pdf

[37] "Digital economy report 2021, cross-border data flows and development: For whom the data flow." 2021. [Online]. Available: https://unctad.org/system/files/official-document/der2021_en.pdf

[38] E. Parliament. "More women in ICT: Empowering women in the digital world—News European parliament." 2018. [Online]. Available: https://www.europarl.europa.eu/news/en/headlines/society/20180301STO98927/more-women-in-ict-empowering-women-in-the-digital-world

[39] M. J. Cobb, "Plugging the skills gap: The vital role that women should play in cyber-security," *Comput. Fraud Security*, vol. 2018, no. 1, pp. 5–8, 2018.

[40] J. Reed and J. Acosta-Rubio. "Innovation through inclusion: The multicultural cybersecurity workforce." 2018. [Online]. Available: https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx

[41] J. Reed and J. Acosta-Rubio (Frost & Sullivan, Santa Clara, CA, USA). *Innovation Through Inclusion: The Multicultural Cybersecurity Workforce; An (ISC) 2 Global Information Security Workforce Study*. (2018). [Online]. Available: https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx

[42] F. B. Schneider, "Cybersecurity education in universities," *IEEE Security Privacy*, vol. 11, no. 4, pp. 3–4, Jul./Aug. 2013.

[43] "Strategies for building and growing strong cybersecurity teams." 2019. [Online]. Available: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019

[44] "European framework for cyber security certification (in Czech)." 2020. [Online]. Available: https://www.nukib.cz/download/publikace/vyzkum/Evropsky_ramec_certifikace_kyberneticke_bezpecnosti.pdf

[45] B. J. Blažič, "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?" *Educ. Inf. Technol.*, vol. 27, pp. 3011–3036, Sep. 2022.

[46] K. M. Carley, "Social cybersecurity," *Comput. Math. Org. Theory*, vol. 26, no. 4, pp. 365–381, 2020. [Online]. Available: http://link.springer.com/10.1007/s10588-020-09322-9

[47] H. de Bruijn and M. Janssen, "Building cybersecurity awareness," *Govt. Inf. Quart.*, vol. 34, no. 1, pp. 1–7, 2017. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0740624X17300540

[48] J. Davis and S. Magrath. "A survey of cyber ranges and testbeds." 2013. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA594524.pdf

[49] "Understanding cyber ranges: From hype to reality," European Cyber Security Organization (ECSO), Brussels, Belgium, Working Group 5 (WG5), 2020. [Online]. Available: https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf

[50] T. D. Zan. "Mind the gap: The cyber security skills shortage and public policy interventions." Global Cyber Security Center. 2019. [Online]. Available: https://ora.ox.ac.uk/objects/uuid:e9699fc6-279c-4595-b707-7fd0acc487b3

[51] "Rootme—Hacking and information security learning platform." 2021. [Online]. Available: https://www.root-me.org/

[52] "QEMU—The FAST! Processor emulator." 2023. [Online]. Available: www.qemu.org

[53] J. Vykopal, V. Švábenský, and A. Farkas, "Virtual lab for open-source tools education and research." 2021. [Online]. Available: https://cybersec4europe.eu/wp-content/uploads/2021/01/D7.2-virtual_lab-v0.2_submitted.pdf

[54] (ANSSI-51, Paris, France). *Essential Measures for a Healthy Network*. (Jan. 2013). [Online]. Available: https://www.ssi.gouv.fr/uploads/2013/01/guide_hygiene_v1-2-1_en.pdf

[55] "Cidadão Ciberseguro (Cybersecure Citizen)." Feb. 2020. [Online]. Available: https://www.nau.edu.pt/curso/cidadao-ciberseguro/

[56] "ENISA threat landscape 2020: Phishing," ENISA. 2020. [Online]. Available: https://www.enisa.europa.eu/publications/phishing

[57] (NIST, Gaithersburg, MA, USA). *Post-Quantum Cryptography PQC*. (2021). [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals

[58] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity," *J. Defense Model. Simulat. Appl., Methodol. Technol.*, vol. 19, no. 1, pp. 57–106, 2022. [Online]. Available: http://journals.sagepub.com/doi/10.1177/1548512920951275

[59] "Adversarial ML threat matrix." 2020. [Online]. Available: https://github.com/mitre/advmlthreatmatrix

[60] "The 15 biggest data breaches of the 21st century." Jan. 2021. [Online]. Available: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[61] V. Lotz, "Cybersecurity certification for agile and dynamic software systems: A process-based approach," in *Proc. IEEE Eur. Symp. Security Privacy Workshops*, 2020, pp. 85–88. [Online]. Available: https://ieeexplore.ieee.org/document/9229655/

[62] E. Commision. "The EU cybersecurity certification framework." Sep. 2017. [Online]. Available: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

[63] W. M. Stahl, "The uncharted waters of cyberspace: Applying the principles of international maritime law to the problem of cybersecurity," *Georgia J. Int. Comparative Law*, vol. 40, no. 1, p. 247, 2011. [Online]. Available: https://digitalcommons.law.uga.edu/gjicl/vol40/iss1/9

[64] "Recitals 75-77 and articles 24.1 and 32 of the GDPR." 2018. [Online]. Available: https://www.privacy-regulation.eu/en/article-24-responsibility-of-the-controller-GDPR.htm

[65] P. J. Fischer, "A cybersecurity skills framework," in *Cybersecurity Education for Awareness and Compliance*. Hershey, PA, USA: IGI Global, 2019, pp. 202–221. [Online]. Available: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-5225-7847-5.ch011

[66] "European data protection supervisor: Data protection officer (DPO)." 2021. [Online]. Available: https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

[67] "Migration data portal: The bigger picture." 2020. [Online]. Available: https://migrationdataportal.org/themes/environmental_migration

[68] J. Styles. "The unseen COVID-19 ripple effect: Security misconfiguration risk." 2020. [Online]. Available: https://www.securityinfowatch.com/covid-19/article/21137323/the-unseen-covid19-ripple-effect-security-misconfiguration-risk

[69] S. Bullard. "A practical approach to using IoT devices to support legacy SCADA field systems in the transition to Internet-based industrial automation systems." 2019. [Online]. Available: https://www.wateronline.com/doc/a-practical-approach-to-using-iot-devices-to-support-legacy-scada-field-systems-0001

[70] "Republic of cyprus: Cybersecurity capacity review." 2017. [Online]. Available: https://ocecpr.ee.cy/sites/default/files/cmm_cyprus_report_2017_final.pdf

[71] M. Bastian, S. Heymann, and M. Jacomy, "Gephi: An open source software for exploring and manipulating networks," in *Proc. Int. AAAI Conf. Web Social Media*, 2009, pp. 361–362. [Online]. Available: http://www.aaai.org/ocs/index.php/ICWSM/09/paper/view/154