PESTLE Analysis of Cybersecurity Education

Sara Ricci*
ricci@vutbr.cz
Brno University of Technology
Brno, Czech Republic

Vladimir Janout
xjanou19@vutbr.cz
Brno University of Technology
Brno, Czech Republic

Simon Parker
simon.parker@dkfz-heidelberg.de
Deutsches Krebsforschungszentrum
Heidelberg, Germany

Jan Jerabek
jerabekj@vutbr.cz
Brno University of Technology
Brno, Czech Republic

Jan Hajny
hajny@vutbr.cz
Brno University of Technology
Brno, Czech Republic

Argyro Chatzopoulou
ac@apiroplus.solutions
APIROPLUS Solutions Ltd.
Limassol, Cyprus

Remi Badonnel
remi.badonnel@loria.fr
University of Lorraine
Villers-lès-Nancy, France

ABSTRACT

Cybersecurity is a vital part of digital economies and digital governing but the discipline is suffering from a pronounced skills shortage. Nevertheless, the reasons for the inability of academia to produce enough graduates with the skills that reflect the needs of the cybersecurity industry are not well understood.

In this article, we have analysed the skills shortages, gaps, and mismatches affecting cybersecurity education. We performed a Political, Economic, Social, Technological, Legal, and Environmental (PESTLE) analysis, that allowed us to have an overview of the cybersecurity education environment from multiple perspectives. The results of this analysis highlight 31 different factors affecting cybersecurity education on a European level. These factors were further analysed from the specific perspectives of 11 European countries. In this further analysis, particular attention was given to the linkages between the identified factors. This helped to reveal which factors are connected and to describe how they are mutually dependent. A statistical approach was used to depict the results in a more general and comprehensive way and facilitated the development of our conclusions. Our analysis identifies a lack of European coordination and cooperation towards a common cybersecurity framework as one of the main factors affecting cybersecurity education.

CCS CONCEPTS

• **Applied computing** → **Education**; • **Security and privacy** → *Human and societal aspects of security and privacy*.

KEYWORDS

Cybersecurity Education, PESTLE analysis, cybersecurity skills gap.

ARES 2021, August 17–20, 2021, Vienna, Austria

ACM ISBN 978-1-4503-9051-4/21/08…$15.00
https://doi.org/10.1145/3465481.3469184

ACM Reference Format:
Sara Ricci, Vladimir Janout, Simon Parker, Jan Jerabek, Jan Hajny, Argyro Chatzopoulou, and Remi Badonnel. 2021. PESTLE Analysis of Cybersecurity Education. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3465481.3469184

1 INTRODUCTION

It is widely understood that there is a shortfall in the number of trained cybersecurity professionals available in relation to the current demand (for those professionals) from organisations, institutions, and governments [5, 10, 40, 45, 49]. Cybersecurity is a vital part of digital economies and digital governing but the discipline is suffering from a pronounced skills shortage [10]. The annual ISACA State of Cybersecurity Report [40] identified a number of reasons for this gap, including the complexity and breadth of the skill set that these professionals should possess. Despite this report, the situation remains complex and many of the reasons for this failure are not well understood. The challenges faced vary by country and sector making it difficult to identify the underlying factors and the interconnections between them.

To better understand this problem we have implemented a PESTLE analysis, facilitating a categorisation of the underlying causes as either Political, Economic, Social, Technological, Legal, or Environmental [28]. A PESTLE analysis is used as a tool of situational analysis for business evaluation purposes and is one of the most used models in the evaluation of the external business environment that is highly dynamic [38]. It is also a common part of development frameworks and provides a method to reveal and understand gaps and challenges from multiple points of view. The information gathered from a PESTLE analysis can also be used to support the development of future research; for example by generating topics for questionnaires or interviews and by guiding the prioritisation of factors to investigate. As such, PESTLE is a useful approach to conceptualise the multifaceted challenges facing cybersecurity education.

The rest of this article is organised as follows. Section 1.2 briefly reviews PESTLE analysis and its usage in the cybersecurity domain. Section 2 introduces the PESTLE analysis implemented for analysing the challenges for cybersecurity education. Section 3 provides the statistical results of the further analysis conducted across 11 European countries. The final section contains our conclusions.

1.1 PESTLE and Cybersecurity

PESTLE is a widely used tool, which is most frequently used for market analysis [28], or as a part of the risk management process, the later of which is of great interest to cybersecurity research. As part of our study, we sought to review similar analyses but found that, because of the frequent business-oriented nature of PESTLE and the commercial valuable of the asset it represents, few of the analyses results are available to researchers. The analyses often include sensitive information about a business and thus are not shared publicly. However, some existing resources mention PESTLE in regards to cybersecurity and discuss its applicability in different contexts and scenarios.

In [25], the authors used PESTLE alongside Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis, giving a slightly different perspective by dividing the environment into internal and external parts. Moreover, in [31], PESTLE is introduced as a part of additional considerations for coordinated incident handling as a way to identify social limitations and the requirements of stakeholders involved in the oil and gas drilling industry.

In [26], Blum refers to PESTLE as an important pillar when establishing the context of a risk program, e.g. when employing a risk management framework standard such as ISO31000:2018 [41] or Open FAIR [53]. It is highlighted as a useful tool to gather knowledge and to document the risk program's business context for leaders. PESTLE was also introduced as an important part of the qualitative and exploratory methodology in research analysing challenges to Sri Lanka's national security; it was used as a tool to evaluate inputs collected during research. Moreover, PESTLE was utilised to identify threats to the country's legislation and categorise them accordingly [50].

Hiscock [39] applied PESTLE as part of the process of designing an Identity Access Management tool (IAM). It was used in the form of a mind map to generate ideas and to produce a better overview of factors that could impact the usage and lifespan of the IAM tool. Although this usage has a slightly different scope to this research (software development vs cybersecurity education), it is highlighted because the process identified relevant aspects connected to the cybersecurity industry.

PESTLE is also a tool used in the education domain. For example, in [51], the analysis was employed to discover factors that are affecting the Scottish higher education system. In [57], a PESTLE analysis of e-learning in healthcare professional education is presented. They state that although e-learning is about education, it cannot be viewed in isolation from the social, technological, and political context in which it is based.

To conclude, PESTLE is a well-known tool, which is already being used in the cybersecurity industry and in education. However, to the best of our knowledge, there are no analyses that specifically target cybersecurity education at the European level.

1.2 Contributions

Our contribution is threefold:

- Firstly, factors affecting cybersecurity education are identified, defined, and described. Relevant, up-to-date, and primarily European-level references are provided for all factors. A total of 31 factors are identified.
- Secondly, the identified factors are further analyzed from the perspective of 11 European countries. This second stage allowed us to obtain a comprehensive view of the situation across Europe from a variety of national perspectives, as well as possible correlations between the factors.
- Finally, a statistical approach is used to view the results in a more general and comprehensive way and to reveal interesting findings.

The most important outcome of this analysis is the linkage between identified factors. This helps in revealing the interconnections and the dependencies of the factors within a particular country.

2 PESTLE ANALYSIS

The Cybersecurity Skills Alliance - A New Vision for Europe (REWIRE) project [16] highlighted out the need to develop an European sectoral skills strategy for cybersecurity. This need, and the shortfall in the number of trained cybersecurity professionals available, motivated us to develop a methodology for the implementation of a cybersecurity-education-oriented PESTLE analysis. This methodology incorporates a series of steps implemented with the contribution of all partners of the REWIRE project. In this section, the results of the first stage of our work are presented where the 31 identified factors are described. Figure 1 shows the analysis results in a mind-map, which serves as a graphical representation of the collected data. Each factor is then described below.

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

1 *Lack of relevant European regulatory frameworks.* A number of frameworks have been developed at a European-level [12]. Nevertheless, these frameworks fail to address cybersecurity education and training in sufficient detail, leading to a lack of relevant regulatory frameworks in this area [45].
2 *Lack of coordination.* There is a need for (national and European-level) coordination among stakeholders and leading institutions [11]. This lack of coordination causes roadblocks in the implementation of a skills framework [5].
3 *Vulnerabilities of the training systems and skills shortage.* Cybersecurity education needs to attract more students, and to better identify the skills needed in the labour market [5].
4 *Political ambition to create cooperation frameworks.* There is a need for greater political effort regarding the creation of cooperation frameworks among academia, employers, and governments [14].
5 *Greater attention to policies dedicated to raise awareness of cybersecurity career paths.* Not enough policies dedicated

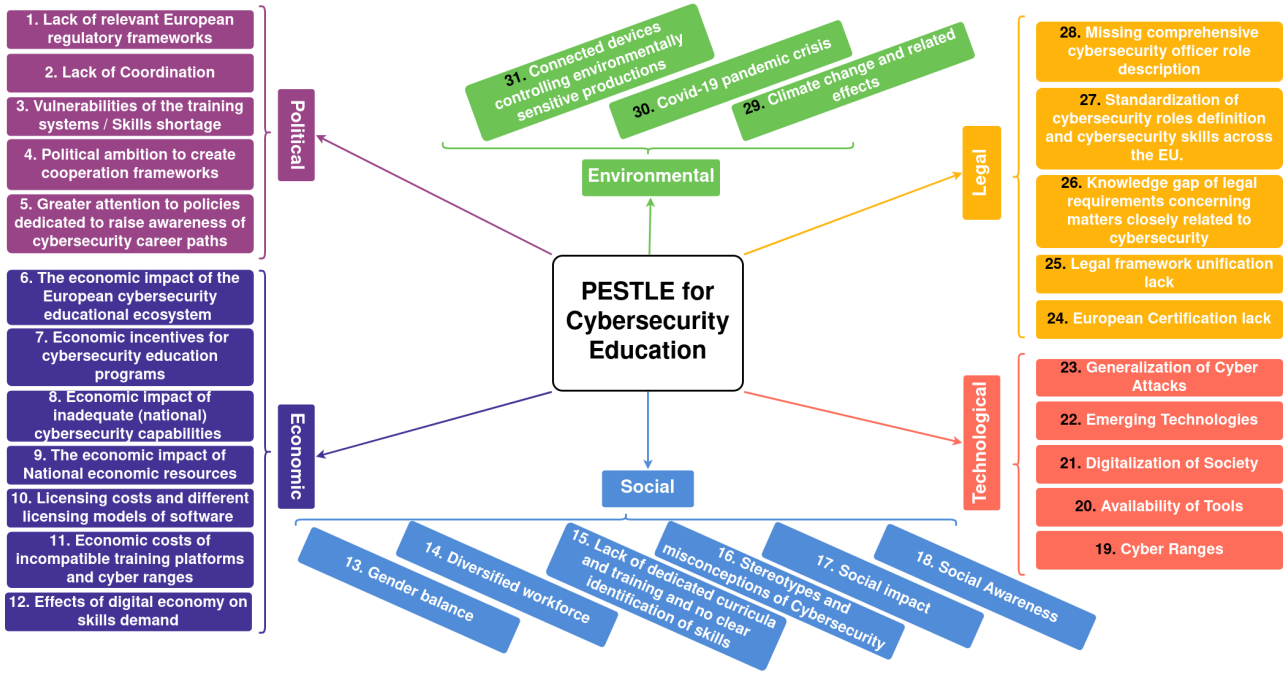

Figure 1: PESTLE analysis in a mind-map.

to raise awareness of cybersecurity career paths exist. Cybersecurity as a lifelong career option is rarely promoted [9].

Economic factors. Economic factors in relation to cybersecurity education represent both the economic challenges associated with developing a cybersecurity education framework as well as the impact of the lack of skilled professionals on the wider economy.

6 *The economic impact of the European cybersecurity educational ecosystem.* The Information Systems Audit and Control Association found that 58% of organizations have unfilled cybersecurity vacancies [7]. One of the biggest reasons for this is the lack of qualified professionals. This skills gap could be improved with an increased availability of degree curricula and training courses across Europe [3].

7 *Economic incentives for cybersecurity education programs.* There has been an increased uptake of university courses that are associated with jobs with good employment opportunities, such as health sciences or law, as well as a rise in the popularity of courses that may lead to a comparatively early source of income such as the military and police academies. Conversely, there has been a drop in interest for those courses that are considered academically challenging, such as engineering and computer science [17]. This has impacted on cybersecurity education since a majority of the current curricula are delivered by engineering and computer science faculties. It is therefore important to incentivise the enrollment of practitioners in cybersecurity programs.

8 *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 victims of cybercrime [36]. Therefore, they are unable to report incidents of cybercrime to the relevant authorities. This may cause a downplaying in the value of cybersecurity and cybersecurity education because the perceived level of cybercrime is not representative of the actual situation.

9 *Economic Impact of National Economic Resources.* The cost of maintaining and developing cybercrime systems have escalated due to a need to match the equipment and capabilities used by perpetrators. This may be economically challenging for some organisations and nations [46, 47].

10 *Licensing costs of cybersecurity education software.* Cybersecurity education often relies on the use of (online) platforms with payable licensing costs. However, these training providers often seek to maximise profitability and capitalise on the high demand for new cybersecurity professionals. This aggravates the lack of skilled workforce by providing a financial barrier to entry [42, 55].

11 *Economic costs of incompatible training platforms and cyber ranges.* Online training platforms and cyber ranges are not designed to easily exchange exercises and scenarios [56]. Multiple teams at different education providers invest in unnecessary effort to develop new scenarios and training exercises which are equivalent. This duplicated effort could be easily eliminated if the scenarios were standardised and interchangeable.

12 *Effects of digital economy on skills demand.* Accenture Strategy research estimates that the digital economy, involving some form of digital skills and digital capital, represents 22.5% of the world economy (2020), and yet this potential is far from being fully exploited [24]. Cybersecurity is foundational to the digital economy and the shortage of skilled professionals will limit economic growth.

Social factors. Social factors consider demographics, population growth rate, age distribution, income distribution, family size, emphasis on safety, health consciousness, trending lifestyle attitudes, and cultural barriers. It can also include general consumer opinions and attitudes, the dominant view of the media, law changes affecting social factors, changes in lifestyle, attitudes towards work, history, and some other important considerations.

13 *Gender balance.* 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 subjects [45]. A 2016 postgraduate study [35] concluded that the main factors that inhibit women's entry into the field are: (a) the militaristic/gendered culture and language; (b) the cultural biases of influencers and decision makers; (c) the realities and perceptions of the work/life balance drive women away from the sector.

14 *Diversified workforce.* Although the cybersecurity sector has been growing quickly, it has not become more culturally diversified. A 2018 American study [48] revealed that minority representation within the cybersecurity profession is slightly higher than in the overall workforce. People with varied life experiences will tackle problems differently and so a highly diversified workforce is likely to improve the effectiveness a cybersecurity system. In terms of fairness, opportunities should be open to all, regardless of their gender, ethnicity, sexuality, or any other factor [44].

15 *Lack of dedicated curricula and training and no clear identification of skills.* There is an insufficient number of cybersecurity specific multidisciplinary curricula that offer the fundamental skills necessary for cybersecurity education. According to the European Network and Information Security Agency (ENISA) [6], the main issues with current curricula are, outdated or unrealistic platforms in educational environments, difficulties in keeping pace with the outside world, a lack of qualified cybersecurity educators, limited interactions with industry, and little understanding of the labour market.

16 *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 or its role in society more widely [45]. The main identified stereotypes are as follows: (a) new curricula are often viewed as an add-on to more mainstream computer science and fail to realise the critical importance of the interdisciplinary nature of this area; (b) young people consider cybersecurity as a field more aimed at the public and less at the private sector; (c) lack of a clear cybersecurity career path; and (d) cybersecurity is an emergent career with a relatively young workforce; there is limited potential for an older generation to encourage and support the development of new workers in this area.

17 *Social impact.* In today's interconnected world, beliefs, opinions and attitudes are increasingly shaped through engagement with social media, and through the Internet. Alongside the rise of online platforms where individuals could gather, spend, and share information, came the rise of online cybercrimes which aims to take advantage of individuals and even whole communities [29]. This has necessitated a greater interaction between society and cybersecurity.

18 *Social Awareness.* Although cybersecurity is one of the most important challenges faced by governments today, the visibility and public awareness of it remains limited. Communicating cybersecurity is confronted with paradoxes, which has resulted in society not taking appropriate measures to deal with the threats [34].

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

19 *Cyber Ranges.* A cyber range [33] is a virtual environment that emulates real-world scenarios for training groups of professionals. These are important means of training groups of security professionals in the areas of ethical hacking and in threat identification and response [58].

20 *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 [2, 19] .

21 *Digitisation of Society.* Digitisation 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 [22]. The digitisation of society increases the potential opportunities for attacks, and enables new attack vectors to be developed which may have, possibly at a massive scale, a very significant impact on society [21].

22 *Emerging Technologies.* There are a number of emerging technologies that have the potential to change the way computers, networks, systems are operated, and would require a redesign of current security curricula. Examples include quantum computing [18], machine learning [32] and cyber-physical systems [8].

23 *Generalisation of Cyber Attacks.* Given the increased digitisation of society, there is a significant broadening of scope and diversity to 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) [23].

Legal factors. Legal factors may be both external and internal to organisations, institutions, and governments. Certain laws

[1] Advanced Persistent Threats

affect cybersecurity or the business environment in a certain country whilst there are also internal security policies that are self-defined and maintained. The legal analysis takes into account both, and charts out the strategies taken in light of these regulations. For example, cybersecurity laws, personal data protection laws, consumer laws, and computer laws. During our analysis, five aspects were identified. In the following section, we briefly describe these aspects and how they impact upon cybersecurity education.

24 *Lack of European Certification.* Certification [30, 43] is a well-established and traditionally-used means to define and formalise desired properties and the best practices to achieve them. Cybersecurity certification of products, services, and processes [13] is currently only used to a limited extent. Existing certification schemes are at times severely lacking and there are many differences in terms of product coverage, levels of guarantees, essential criteria and actual use, that hampers mutual recognition mechanisms within the European Union (EU).

25 *Lack of legal framework unification.* Europe lags behind other regions in the development of a comprehensive approach to define a set of roles and skills relevant to the cybersecurity field [6, 52].

26 *Knowledge gap of legal requirements in personal data protection.* Europe's General Data Protection Regulation (GDPR) [4] is perhaps the most wide-ranging and comprehensive piece of data privacy legislation. The GDPR requires data controllers and processors to use proportionate security measures when working with personal data; this can be seen as a risk-based approach. Students should therefore be aware of possible risks to the protection of personal data as stated in legislation.

27 *Standardisation of cybersecurity roles definition and cybersecurity skills across European Union (EU).* Cybersecurity roles [6] with respect to cybersecurity skills is currently a grey area as no specific map of what skills are needed for certain cybersecurity roles exist. Both universities and associations have created a maze of possible qualifications that may or may not be suitable for certain cybersecurity roles. The existence of specific qualification bundles [37] linked with specific cybersecurity roles and equivalents is considered a pending issue that needs to be mitigated through standardisation initiatives.

28 *Missing comprehensive cybersecurity officer role description.* Whilst data protection officers have a clear definition in the GDPR [1], there is not a similar comprehensive role description for cybersecurity officers. As cybersecurity is becoming a more important and integral part of Europeans' security [6], cybersecurity roles in organizations require greater attention. The legal requirements for cybersecurity roles are also not defined in law.

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, environmental factors how the conditions at the time of this project influence cybersecurity and cybersecurity education.

29 *Climate change and related effects.* The International Organization for Migration estimates that 200 million people could be forced to leave their homes due to environmental changes by 2050 [15]. This does not only have implications on physical security, but in a digital modern society, will also have an impact on cybersecurity. An increased number of cybersecurity professionals will be needed to provide solutions and services.

30 *Covid-19 pandemic crisis.* Due to the COVID-19 pandemic, curfews, quarantines, and similar restrictions (variously described as stay-at-home orders, shelter-in-place orders, cordons sanitaires, shutdowns, or lockdowns) have been implemented in numerous countries and territories around the world. The pandemic crisis increased the necessity for IT and cybersecurity education to move online [54].

31 *Connected devices controlling environmentally sensitive productions.* Legacy Supervisory Control and Data Acquisition (SCADA) devices are being replaced by new connected devices allowing for an increased control over their processes and less environmentally-harmful operation. Future cybersecurity incidents could therefore lead to significant environmental disasters [27].

3 ANALYSIS OF IDENTIFIED FACTORS AND THEIR CORRELATIONS

The previous phase of the PESTLE analysis generated 31 factors that appeared to affect cybersecurity education on the European level. To determine if was truly reflective of the situation, representatives from 11 European countries were requested to review these factors, identify if and how they affect cybersecurity education within their country, and identify possible existing dependencies. The countries were: Austria, Cyprus, the Czech Republic, France, Lithuania, Greece, Hungary, Portugal, Serbia, Spain, and Sweden. Remarkably, each country had already identified a majority of the skills shortages, gaps, and mismatches identified on European level. Only "12. Diversified workforce", "25. Missing comprehensive cybersecurity officer role description", and "26. Climate change and related effects" were not previously identified within the national data (see REWIRE project Deliverable R2.1.1 [20] for more details).

On average the PESTLE categories were identified equally as shown in Figure 2. Technological factors were mentioned most frequently, 22% of identified factors across all nations are in this category. This could be due to the strong association and dependency between cybersecurity and technology. Although the percentages of identified factors in each PESTLE category do not differ substantially, there were noticeable differences in the factors identified by country. For example, Austria and Serbia had a greater focus on political factors, while the Czech Republic, Hungary, and Spain tended to highlight technological factors. We hypothesise that a country's major concerns, and overall political

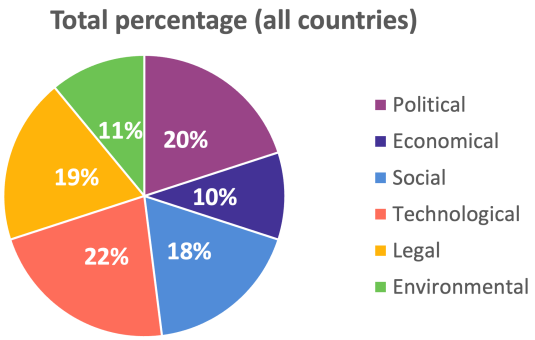

Figure 2: Average of identified PESTLE analysis percentages for all countries.

direction, may skew the results towards one or more PESTLE category.

Some factors are strongly interconnected and as such could be interpreted as sub-factors of broader factors that span multiple categories. For instance, a lack of a skills framework can be deduced from the political, social, and legal categories. In particular, the factors "1. Lack of relevant European regulatory frameworks", "15. Lack of dedicated curricula and training and no clear identification of skills", "25. Legal framework unification lack", highlight this overarching lack of a skills framework. Similarly, cyber ranges and the lack of training tools are primarily connected to economic and technological issues, that is "10. Licensing costs and different licensing models of software", "11. Economic costs of incompatible training platforms and cyber ranges", "20. Availability of Tools", and "19. Cyber Ranges", respectively.

Once relevant factors were identified, we analysed the linkages between them. This helped to reveal which factors are connected and to describe how they are mutually dependent in a particular country. Note that the linkages are validated by national references.

For instance, Figure 3 depicts the PESTLE analysis performed for Serbia. Each numbered rectangle represents one factor. The correspondence between numbers and factors can be found in Section 2 and Figure 1. In Figure 3, coloured rectangles depict factors recognised as being of primary relevance, grey rectangles with coloured borders represent factors that are mutually dependent on the primary factors, and plain grey rectangles are factors not identified in the country. The lines show factors that are linked. In Serbia, political factors are the most significant, indeed all political factors were identified or linked to and they present the greatest number of connections in the mind map.

The large number of connections between political factors and others that focus on cooperation coordination suggests that there may be a broad overarching factor relating to a lack of cybersecurity governance at national and European level. Undoubtedly this is an area requiring further research in the future. This finding highlights how a PESTLE analytical approach can help focus future research by identifying broad issues that may be obscured if researchers focus on individual factors or do not analyse data from multiple contexts.

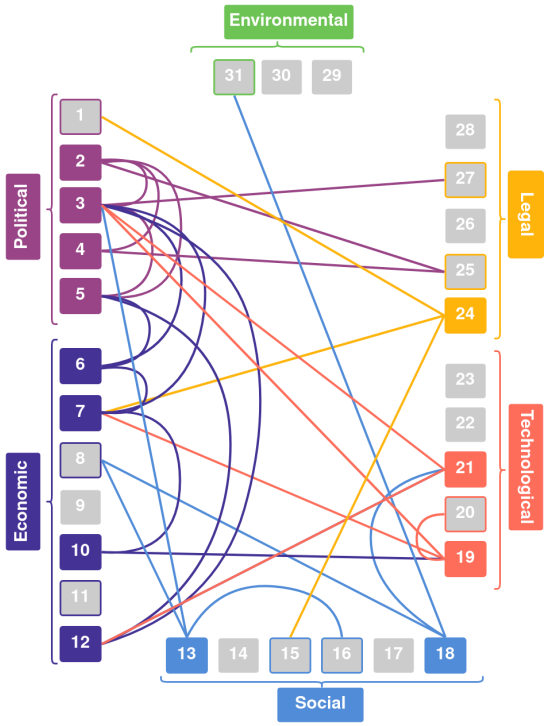

Figure 3: PESTLE analysis of cybersecurity education run in Serbia.

4 CONCLUSION

The main objective of this article was to present the results of a Political, Economic, Social, Technological, Legal, and Environmental (PESTLE) analysis for cybersecurity education. A basic analysis was conducted for each of the 6 characteristics of the PESTLE analysis, revealing 31 different factors affecting cybersecurity education and skills development. This analysis highlights areas that should be addressed in the future. The factors identified also demonstrate the vital importance of cybersecurity, and thereby cybersecurity professionals, to increasingly digitised economics and governments. The Social and Economic categories contained the greatest number of identified factors. Nevertheless, Technological factors were mentioned most frequently in the reviews performed by representatives from 11 European countries.

A second stage of analysis involved the identification of the connections between the different aspects. For this stage, representatives from 11 European countries were asked to review the PESTLE analysis. On average, 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 to resolve these challenges must adapt to local contexts. Furthermore, this analysis also revealed that the identified aspects are intrinsically correlated.

It is notable that a lack of cybersecurity governance, i.e. a lack of European coordination and cooperation was strongly identified by every country surveyed.

ACKNOWLEDGMENTS

The following funding source is gratefully acknowledged: the ERASMUS+ programme of the European Union (grant 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B "REWIRE") and the Ministry of the Interior of the Czech Republic (grant VJ01030001).

REFERENCES

[1] [n.d.]. Data Protection Officer (DPO). https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en
[2] [n.d.]. QEMU. www.qemu.org
[3] 2018. ENISA programming document 2019-2021. In *ENISA* (01 ed.), Vol. 2018. ENISA, 1–95. https://doi.org/10.2824/97038
[4] 2018. Recitals 75-77 and Articles 24.1 and 32 of the GDPR. https://www.privacy-regulation.eu/en/article-24-responsibility-of-the-controller-GDPR.htm
[5] 2019. Cybersecurity Skills Development in the EU. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[6] 2019. CYBERSECURITY SKILLS DEVELOPMENT IN THE EU. In *ENISA*. EU. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[7] 2019. ISACA: State of Cybersecurity 2019 Part 1: Current Trends in Workforce Development. *Isaca.org* 2019 (2019), 1–40. https://media.milanote.com/p/files/1Ilftg1qhN4615/Rzf/Week%201-state-of-cybersecurity-ISACA%202019.pdf
[8] 2020. Adversarial ML Threat Matrix. https://github.com/mitre/advmlthreatmatrix)
[9] 2020. Cybersecurity Education. https://www.enisa.europa.eu/topics/cybersecurity-education
[10] 2020. Cybersecurity Professionals Stand Up to a Pandemic. https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B
[11] 2020. Digital Education Action Plan (2021-2027). https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[12] 2020. European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework
[13] 2020. Evropský rámec certifikacekybernetické bezpečnosti. , 5 pages. https://www.nukib.cz/download/publikace/vyzkum/Evropsky_ramec_certifikace_kyberneticke_bezpecnosti.pdf
[14] 2020. Joint communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018&from=EN
[15] 2020. Migration Data Portal: The bigger picture. https://migrationdataportal.org/themes/environmental_migration
[16] 2020. REWIRE: Cybersecurity Skills Alliance - A new Vision for Europe. https://rewireproject.eu/
[17] 2020. Statistics - European Statistical System (ESS). https://ec.europa.eu/eurostat/web/ess
[18] 2021. Post-Quantum Cryptography PQC. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals
[19] 2021. Rootme. https://www.root-me.org/
[20] 2021. WP2 PESTLE analysis of Cybersecurity Education. https://rewireproject.eu/wp-content/uploads/2021/04/R2.1.1_PESTLE_analysis_results.pdf
[21] February 2020. Cidadão Ciberseguro (Cybersecure Citizen). https://www.nau.edu.pt/curso/cidadao-ciberseguro/
[22] January 2013. Essential measures for a healthy network. https://www.ssi.gouv.fr/uploads/2013/01/guide_hygiene_v1-2-1_en.pdf
[23] January 2021. The 15 biggest data breaches of the 21st century. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
[24] Omar Abbosh and Kelly Bissell. 2019. Securing the Digital Economy. https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf
[25] Danita Baghdasarin. 2019. MRO Cybersecurity SWOT. *International Journal of Aviation, Aeronautics, and Aerospace* (2019). https://doi.org/10.15394/ijaaa.2019.1318
[26] Dan Blum. 2020. Create Your Rational Cybersecurity Success Plan. In *Rational Cybersecurity for Business*. Springer, 297–313.
[27] Steve Bullard. 20 November 2019. *A Practical Approach To Using IoT Devices To Support Legacy SCADA Field Systems In The Transition To Internet-Based Industrial Automation Systems*. https://www.wateronline.com/doc/a-practical-approach-to-using-iot-devices-to-support-legacy-scada-field-systems-0001
[28] James Cadle, Debra Paul, and Paul Turner. 2010. *Business analysis techniques: 72 essential tools for success*. BCS, The Chartered Institute.
[29] Kathleen M. Carley. 2020. Social cybersecurity. *Computational and Mathematical Organization Theory* 26, 4 (2020), 365–381. https://doi.org/10.1007/s10588-020-09322-9
[30] European Commision. September 2017. The EU cybersecurity certification framework. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
[31] Aitor Couce-Vieira and Siv Hilde Houmb. 2016. The role of the supply chain in cybersecurity incident handling for drilling rigs. In *International Conference on Computer Safety, Reliability, and Security*. Springer, 246–255.
[32] Dipankar Dasgupta, Zahid Akhtar, and Sajib Sen. [n.d.]. Machine learning in cybersecurity. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* ([n. d.]). https://doi.org/10.1177/1548512920951275
[33] Jon Davis and Shane Magrath. 2013. A survey of cyber ranges and testbeds. (2013).
[34] Hans de Bruijn and Marijn Janssen. 2017. Building Cybersecurity Awareness. *Government Information Quarterly* 34, 1 (2017), 1–7. https://doi.org/10.1016/j.giq.2017.02.007
[35] Katharine D'Hont. 2016. Women in Cybersecurity. (2016). https://wappp.hks.harvard.edu/files/wappp/files/dhondt_pae.pdf
[36] David P. Fidler. 2013. Final Acts of the World Conference on International Telecommunications. *International Legal Materials* 52, 3 (2013), 843–860. https://doi.org/10.5305/intelegamate.52.3.0843
[37] Peter James Fischer. 2019. A Cybersecurity Skills Framework. In *Cybersecurity Education for Awareness and Compliance*. IGI Global, 202–221. https://doi.org/10.4018/978-1-5225-7847-5.ch011
[38] Abhishek Gupta. 2013. Environment & PEST analysis: an approach to the external business environment. *International Journal of Modern Social Sciences* 2, 1 (2013), 34–43.
[39] Steve Hiscock. 2013. User Guardian. (2013). https://sites.google.com/site/userguardian1/investigation-and-market-research/2-6-pestle-analysis?authuser=0
[40] ISACA. 2020. State of CYbersecurity 2020: Part 1: Global Update on Workforce Efforts and Resources. https://leadcomm.com.br/wp-content/uploads/2020/03/State-of-Cybersecurity-2020-Part-1.pdf
[41] ISO 31000:2018 2018. *Risk management — Guidelines*. Standard. International Organization for Standardization, Geneva, CH. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
[42] D. Katsianis, I. Neokosmidis, A. Pastor, L. Jacquin, and G. Gardikis. 2018. Factors Influencing Market Adoption and Evolution of NFV/SDN Cybersecurity Solutions. Evidence from SHIELD Project. *2018 European Conference on Networks and Communications (EuCNC)* (2018), 1–5. https://doi.org/10.1109/EuCNC.2018.8442845
[43] Volkmar Lotz. 2020. Cybersecurity Certification for Agile and Dynamic Software Systems – a Process-Based Approach. IEEE, 85–88. https://doi.org/10.1109/EuroSPW51379.2020.00021
[44] Xenia Mountrouidou, David Vosen, Chadi Kari, Mohammad Q. Azhar, Sajal Bhatia, Greg Gagne, Joseph Maguire, Liviana Tudor, and Timothy T. Yuen. 2019-12-18. Securing the Human. *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education* (2019-12-18), 157–176. https://doi.org/10.1145/3344429.3372507
[45] European Cyber Security Organisation. 2018. Gaps in European Cyber Education and Professional Training.
[46] Alexandros Papanikolaou, Vasileios Vlachos, Anastasios Papathanasiou, Konstantinos Chaikalis, Maria Dimou, and Magdalini Karadimou. 2014. A survey of cyber crime in Greece. *Telfor Journal* 6, 2 (2014), 86–91. https://doi.org/10.5937/telfor1402086P
[47] Anastasios Papathanasiou, Alexandros Papanikolaou, Vasileios Vlachos, Konstantinos Chaikalis, Maria Dimou, Magdalini Karadimou, and Vaia Katsoula. 2014. Legal and Social Aspects of Cyber Crime in Greece. *E-Democracy, Security, Privacy and Trust in a Digital World* (2014), 153–164. https://doi.org/10.1007/978-3-319-11710-2_14
[48] Jason Reed and Jonathan Acosta-Rubio. 2018. Innovation Through Inclusion: The Multicultural Cybersecurity Workforce. (2018). https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx
[49] Sara RICCI, Jan HAJNY, Edmundas PIESARSKAS, Simon PARKER, and Vladimir JANOUT. [n.d.]. Challenges in Cyber Security Education. ([n. d.]).
[50] B Senaratne. 2017. Dynamics in Cybersecurity: Challenges to Sri Lankas National Security. (2017).
[51] Edward Simpson, John Hart, Andrew Phillips, and David Angus. 2015. Higher Education: Environmental Analysis & Industry Scenarios: Scottish Universities. (08 2015). https://doi.org/10.13140/RG.2.1.2814.1281
[52] William M. Stahl. [n.d.]. The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. *Int'l & Comp.* 40Ga ([n. d.]), L.247. https://digitalcommons.law.uga.edu/gjicl/vol40/iss1/9

[53] Open Group Standart. 2013. Risk analysis (O-RA). (2013). https://publications.opengroup.org/c13g
[54] Jeff Styles. 2020. *The unseen COVID-19 ripple effect: Security misconfiguration risk*. hhttps://www.securityinfowatch.com/covid-19/article/21137323/the-unseen-covid19-ripple-effect-security-misconfiguration-risk
[55] Elochukwu Ukwandu, Mohamed Amine Ben Farah, Hanan Hindy, David Brosset, Dimitris Kavallieros, Robert Atkinson, Christos Tachtatzis, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. 2020. A Review of Cyber-Ranges and Test-Beds. *Sensors* 20, 24 (2020). https://doi.org/10.3390/s20247148
[56] Vincent E Urias, William MS Stout, Brian Van Leeuwen, and Han Lin. 2018. Cyber range infrastructure limitations and needs of tomorrow: A position paper. In *2018 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 1–5.
[57] Kieran Walsh, Lalitha Bhagavatheeswaran, and Elisa Roma. 2019. E-learning in healthcare professional education: an analysis of political, economic, social, technological, legal and environmental (PESTLE) factors. *MedEdPublish* 8 (2019).
[58] ECSO WG5. [n.d.]. Understanding Cyber Ranges: From Hype to Reality. 1–31. https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf