REWIRE
CYBERSECURITY SKILLS ALLIANCE

Co-funded by the Erasmus+ Programme of the European Union

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R2.1.1 PESTLE analysis results

Title	R2.1.1 PESTLE Analysis results
Document description	This report presents an analysis for each participating country containing Political, Economic, Social, Technological, Legal and Environmental factors, which can impact the cybersecurity sector and may be affecting in turn skills shortages, gaps and mismatches.
Nature	Public
Task	T2.1 PESTLE Analysis
Status	Final
WP	WP2
Lead Partner	BUT
Partners Involved	All
Date	08 April 2021

Revision history	Author	Delivery date	Summary of changes and comments
Version 01	BUT	22/03/2021	draft for reviewing
Version 02	BUT	30/03/2021	Improvement of executive summary and conclusions after partners' review.
Final Version	BUT	08/04/2021	Notified improvements after Quality Assurance review

Disclaimer:

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CONTENTS

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

1. EXECUTIVE SUMMARY

In order to develop a sectoral skills strategy, it is necessary to determine the current status quo of skills shortages, gaps and mismatches affecting cybersecurity education. This status quo analysis can also support the objectives of the established growth strategy for the cybersecurity industry. Indeed, skills shortages have a direct impact on the cybersecurity job market.

This report presents a Political, Economic, Social, Technological, Legal and Environmental (PESTLE) analysis of the whole skills shortages, gaps, and mismatches, namely aspects, affecting cybersecurity education. These aspects were identified collaboratively by experts in each field among the REWIRE partners (Chapter 3 on "PESTLE analysis of Cybersecurity Education"). This first analysis is important to have a European-level overview and to synchronize future steps.

Inputs from all four pilots are included in this identification and a deep overview of pilots' outcomes was also developed (Chapter 4 on "Overview of pilots' outcomes"). During their lifetime, each project has already identified many skills shortages, gaps and mismatches that affect cybersecurity education. The purpose is to show which aspects are considered of main relevance by the pilots' projects. In fact, REWIRE project is built upon these inputs. Moreover, the pilots' outcomes can be viewed as a rough European PESTLE analysis.

Furthermore, a deep PESTLE analysis of 11 European countries was developed (Chapter 5 on "Statistical Analysis of Questionnaire"). This step allows to obtain a more comprehensive and accurate view of the situation in a particular country while the aspects identification and pilots' outcomes represent a wider analysis on a European level.

This report gives a first overview of which factor would require a deeper analysis in the future and a bigger effort to be resolved during the lifetime of the project.

This report has the following structure and brings the following findings:

- Chapter 2 describes the five-step methodology followed during the whole process of PESTLE analysis preparation.
- Chapter 3 reports the PESTLE analysis of cybersecurity education. This chapter presents a cybersecurity PESTLE analysis overview and reports all identified aspects from Political, Economic, Social, Technological, Legal and Environmental factors. Each aspect is described in detail and accompanied by examples of its possible effects on cybersecurity education.
- Chapter 4 contains the PESTLE analysis results of the four pilots' projects, namely Concordia, Cybersec4Europe, Echo and Sparta. This analysis revealed that pilots focus mostly on Social and Technological aspects. However, other areas of factors are also covered.
- Chapter 5 summarizes the PESTLE analysis results from the 11 European countries. It is remarkable that each country has already identified many skills shortages, gaps, and mismatches, which can have impact not only on a national level but also in the European-level scale. The linkages between factors are the main objective of this analysis. The results vary significantly depending on the country and it makes an interesting insight into the perception of the cybersecurity education shortcomings.
- Chapter 6 represents the main summary of this report including important conclusions revealed from the analysis.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

- Chapters 7,8,9 and 10 contain “References”, “List of Abbreviations and Acronyms”, “List of Figures”, and “List of Tables”, respectively.
- Finally, Chapter 11 presents the details from all 11 questionnaires (presented in unmodified form) from each of the participating country. In each case, there are national-level references that support the statements and justify the connections among the aspects.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

2. METHODOLOGY

This report was prepared with the help of a five-step methodology starting from scope definition in cybersecurity education area (1), identifying collaboratively the aspects gathered first from the Cyber Security Competence for Research and Innovation (CONCORDIA), Cyber Security competence centres for Europe (CyberSec4Europe), European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO) and Strategic Programs for Advanced Research and Technology in Europe (SPARTA) projects inputs and, then, from REWIRE partners (2), preparing the questionnaire per country and pilots (3), analyzing the results (4) and writing this report (5) as shown by Figure 1.

Figure 1. Steps used in the methodology of this report.

Description of the steps follows.

- ## Scope definition
  The very first step was to establish the scope of this report. It was also necessary to do the research of the available literature, investigate existing reports in the cybersecurity field, search for examples of the PESTLE analysis in the educational area and gather this knowledge in relation to the aims of this report. It was also important to identify what kind of questions should be answered by this report. The main goal of this report is to try to answer the following questions:
  a. Which aspects have an impact on cybersecurity (education-oriented)?
  b. How are all these aspects linked together in each country?

- ## Identification of the aspects
  Aspects are shortages, mismatches and gaps identified for each of the PESTLE factors and impacting cybersecurity education. These aspects were identified collaboratively by experts in each field (Political, Economic, Social, Technological, Legal and Environmental) among the partners. This step allows us to obtain a more

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

comprehensive and accurate view of the situation in a particular country. We started with the identification, definition and description of the aspects of all the factors (Political, Economic, Social, Technological, Legal and Environmental). This search was split into two phases: (1) input from the pilots, and (2) revision and extension by REWIRE partners. Firstly, REWIRE members from Concordia, Echo, Sparta, and Cybersec4Europe projects identify and briefly describe the main cybersecurity skills issues considered in each pilot. Lastly, all REWIRE partners were divided into 6 groups covering PESTLE factors. Each group started a deeper analysis of the respective factor extending the description provided by the pilots and identifying new aspects. Relevant, up-to-date and mostly European-level references are provided for all identified aspects. A total of 31 aspects were identified at this second stage. The results of this step are summarized in Chapter 3.

- **Preparation of the questionnaire**

  Based on the results of Step (2), an online questionnaire for each of the countries in the project and for each pilot was prepared. A total of 16 questionnaires were created, of which 15 were filled in properly by REWIRE partners, as shown in Chapter 11 (Annexes). The purpose of the questionnaire is to identify the connections among aspects, their importance and to recognize which aspects among the identified ones have an impact on cybersecurity education in each country. The questionnaire also allowed to create a new aspect if needed. Moreover, the importance (Low, Medium, High) of each aspect could be ranked.

  The most important outcome of this questionnaire is the linkage between identified aspects. This helps to reveal which aspects are connected to each other and to describe how they are mutually dependent in a particular country or pilot. References to each connection are provided on national and pilot levels. An example of a questionnaire is shown in Figure 2, where a part of one of the questionnaires is depicted. In order to make the list of the identified aspect visual and clear, a mind map of all 31 aspects with a short description of each of the aspects is drawn. A part of this mind map is shown in Figure 3, where the identified Legal aspects are shown with a short description as an example.

- **Analysis of the results**

  All obtained aspects, their description in relevant documents, questionnaires, justifications and assigned references are studied, analyzed in detail, and aligned with the objectives of this report. Critical assessment of all contributions is made. A statistical approach is used to view the results in a more general and comprehensive way and to reveal interesting findings. Gained results are validated and important conclusions are drawn from them.

- **Preparation of the report**

  The last step synthesizes all the findings in this report. All REWIRE partners were involved in the commenting and improving process of the report before publishing its final version.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Factor group (have to be selected first)	Aspect name in selected group (cannot be selected before Group selection)	Importance of the particular Aspect (please select Low / Medium / High)	Linking with other Aspect(s). If there are more than 3, feel free to add lines or modify the Table (you have to add new line (row) in the middle of the section)
Legal	24. European Certification lack	Medium	2. Political - Lack of coordination
			20. Technological - Availability of Tools
			4. Political - Political ambition to create cooperation frameworks

Figure 2. Example of a small part of one of filled questionnaires: one identified aspect and its linking to other aspects.

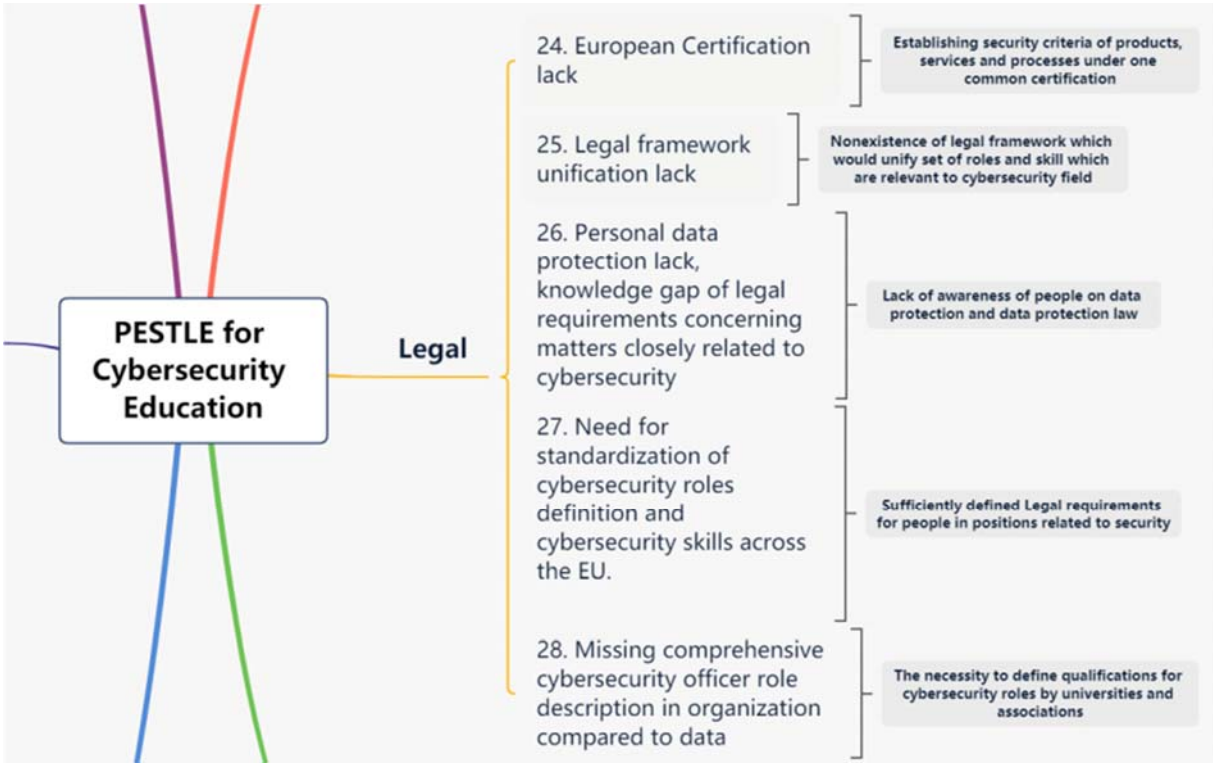

Figure 3. Small part of the developed mind map (showing only the identified Legal aspects and their short description).

3. PESTLE ANALYSIS OF CYBERSECURITY EDUCATION

PESTLE is an acronym, which stands for 6 different factors: Political, Economic, Social, Technological, Legal, and Environmental. It is a systematic approach used by companies and organizations for environment analysis to give a broad overview of a given field of scope. PESTLE is a common part of development frameworks and provides a method to reveal and understand various gaps and challenges from multiple points of view. Information gathered from PESTLE can be used to provide relevant input for questionnaires which can obtain further reflection on identified aspects and assign their priority. Part of the analysis results are PESTLE mind-maps, which serve as a graphical representation of collected data and are further used and developed to represent interconnections between aspects addressed by pilot projects.

PESTLE is used for market analysis [52], or as a part of the risk management process, which is a common interest in cybersecurity. It can be conducted alongside Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis, which gives a slightly different perspective by dividing the environment into internal and external parts. As part of the search for examples, it was found that some SWOT analysis is used to find cybersecurity weaknesses and gaps within the safety management system of the Maintenance, Repair, and Overhaul (MRO) industry [21]. Out of our knowledge, analyses, that would specifically target cybersecurity education are non-existent.

Therefore, it was necessary to define the scope of each factor before advancing with research for aspects of each factor. The descriptions and concrete design of the adapted PESTLE analysis focused on cybersecurity education are described in the following subsections.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

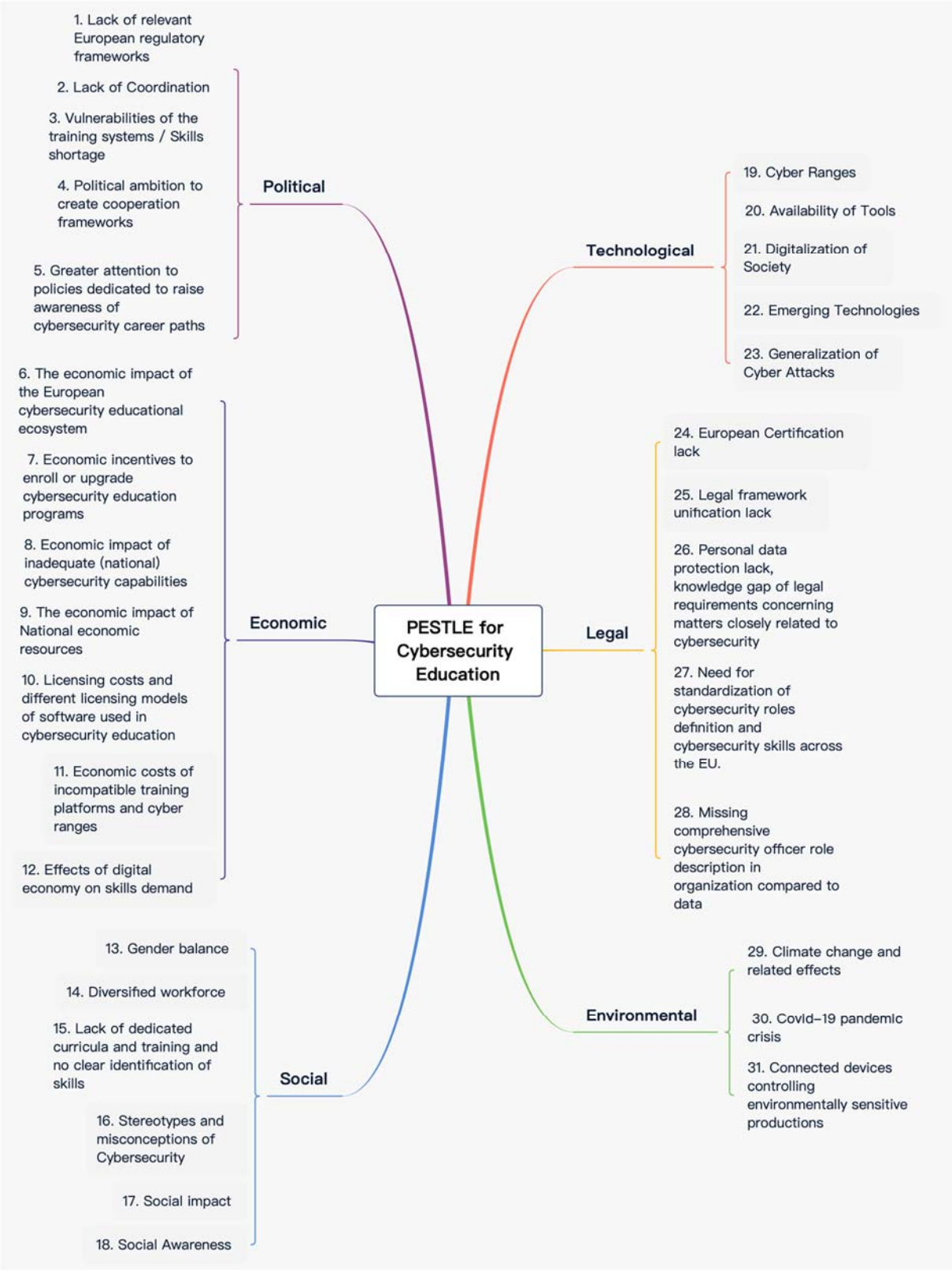

Figure 4. REWIRE aspects along with short description in a mind-map.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.1. Political Factor

The Political analysis assesses existing legal and other regulatory frameworks (status and trends) that can affect the delivery of the activities and services being planned to be developed in the framework of the REWIRE SSA project. Political factors analysis may include elements as regulations at national, European and global level as well as issues related with political stability; government priorities, strategic frameworks related to the sector being analyzed, taxes and fiscal policies and labor/environmental/copyright/consumer protection laws, competition regulation, and funding grants and initiatives. During the analysis five aspects have been found. In the following sections, we briefly describe these aspects and their identified effects on cybersecurity education.

3.1.1. Lack of relevant European regulatory frameworks

In the EU, several frameworks have been developed to support, guide and promote Vocational Education and Training Systems (VET) in Europe [43]. These frameworks have been put in place in acknowledgement of the role of VET in the lifelong learning systems and in equipping citizens with the knowledge, skills and competences required for the labor market as well as of its contribution towards the mutual understanding and transparency regarding recognition and validation of qualifications, transferability and certification. The main aim of these frameworks is to address pitfalls that the VET sector faces related to various factors and to respond to challenges (such as, the diversity and great differences between VET systems across the EU countries, the quality and relevance of the training offer to the market needs etc.) by providing to all relevant stakeholders, recommendations to be used as reference across sectors in the vocational education and training systems. Nevertheless, it is important to note that existing frameworks fail to address in detail cybersecurity in education and training, which showcases the lack of relevant regulatory frameworks to support education providers in their provision of training in the cybersecurity sector [66].

Examples of possible effects on cybersecurity are:

1. Lack of clarity of the specific occupational profiles and skills linked to cybersecurity.
2. Lack of a standardized approach to aspects such as learning outcomes, quality of training; validation, recognition and certification of skills and competencies.
3. Difficulty to identify competent professionals from the market.

3.1.2. Lack of coordination

From the vocational education and training perspective, the European skills agenda demands an articulated and concerted action from all key stakeholders at all different levels (European, National, Regional and Local), engaging policy and decision makers, industry representatives, employers and VET providers to come together to actively put the skills agenda into action [25]. While this offers tremendous opportunities it also brings additional challenges related to the coordinated effort needed. All activities need to be coordinated by leading institutions, for example the European Cybersecurity Agency (ENISA) [43]. Despite the efforts made at the European level in the development of a Cybersecurity Skills Framework, the lack of

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

coordination between the most relevant stakeholders is still an issue causing roadblocks in its implementation [13].

An example of a possible effect on cybersecurity is:

1. Lack of understanding of the intersectionality nature of the sector (cybersecurity) that will lead to training curricula that do not respond to the needs of the market.

3.1.3. Vulnerabilities of the training systems / Skills shortage

The interest in cybersecurity education and skills is a long standing priority the EU and it has been a policy concern since the publication by the European Commission of the first EU cybersecurity strategy in 2013 [15]. In the current time, the cybersecurity education system shows a concrete inability to attract more students in studying cybersecurity and to produce graduates with ''the right cybersecurity knowledge and skills". Many of the current issues in cybersecurity education could be lessened by equipping teachers/trainers with the necessary competences and redesigning educational and training pathways that define knowledge and skills, which students should possess upon graduation and after entering the labour market [13]. The Corona Virus Disease 2019 (COVID-19) pandemic has shown the resiliency of the vocational educational systems, but it has also highlighted its vulnerabilities. As stressed in the communication of the New Skills Agenda, challenges to Information Technology (IT) infrastructure and e-systems have revealed the need to improve our human capacity for cybersecurity preparedness and response [25]. The need to modernize the vocational educational systems so that learners acquire the skills needed in the labor market is critical.

Examples of possible effects on cybersecurity are:

1. Lack of infrastructure (equipment and skills).
2. Inability to attract more students in studying cybersecurity and to produce graduates with ''the right cybersecurity knowledge and skills".
3. Difficulty of education and training institutions to adjust and respond to changes in a timely manner.

3.1.4. Political ambition to create cooperation frameworks

It is important to achieve political ambition to create cooperation frameworks, where academia, employers and governments continuously review and improve educational programs of cybersecurity. Cybersecurity is an essential area in modern society. Cyber threats and necessity to have reliable protections highlights the need for educational cybersecurity frameworks based on closed cooperation of all interested counterparties [13], [56]. This would help to maintain a relevant studies curriculum.

Examples of possible effects on cybersecurity are:

1. Lack of framework for relevant cybersecurity skills development.
2. Shortage of skilled cybersecurity specialists creates potential vulnerabilities in sectors where digitalization is becoming one of the key elements.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.1.5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths

More attention should be given to support of interest in cybersecurity career paths, i.e. by campaigns, challenges, competitions, conferences. Though current initiatives are undoubtedly useful and help to improve cybersecurity skills and knowledge, cybersecurity as a life career path with fundamental principles as such is not so widely promoted [11].

An example of a possible effect on cybersecurity is:

1. Missing opportunity to promote a cybersecurity career path and highlight its benefits and overlap to almost all sectors of industry and administration.

3.2. Economic Factor

Economic factors in relation to cybersecurity education represent a unilateral causality between economic notions on the one hand, and on the other hand, outcomes reflected on cybersecurity education on the other hand approaches, projects, decisions, policies, and frameworks. During the analysis seven aspects have been found. In the following sections, we briefly describe these aspects and their identified effects on cybersecurity education.

3.2.1. Economic impact of the European cybersecurity educational ecosystem

The Information Systems Audit and Control Association found that 58% of organizations have unfilled cybersecurity vacancies [53]. One of the biggest reasons is lack of qualified professionals. In 2017, the European Commission suggested that the main reason why some Member States had been better able to establish computer emergency response teams was a ‘cybersecurity skills gap’ throughout the EU. Member States had identified a ‘cybersecurity awareness and skills gap in the population’ as being among the key obstacles to building a secure cyberspace. Notwithstanding the availability of almost 500 university and training courses across Europe, ‘the cybersecurity skills gap across all sectors remains a major challenge and the talent pool is not keeping up the pace’ [33]. The 2019 (ISC)2 cybersecurity workforce study asserted that there is a shortage of approximately 291 000 cybersecurity professionals in Europe up from the previous estimate of 142 000 professionals that had been given in the 2018 report [80], [12]. This result is complemented by what participants in the Symantec CISO Forum said in February, when they concluded that hiring cybersecurity personnel takes at least 6 months (9 and 12 months not being unusual) [22]. On a similar note, a survey commissioned by the cybersecurity firm Trend Micro discovered that 33 % of 1 125 chief information security officers in the United States and the EU have difficulty hiring new talent [12].

Examples of possible effects on cybersecurity are:

1. Lack of understanding: the shortage is really dominated by a lack of understanding and adaption on our way of training people and fostering their development in the industry based on the way cybersecurity is evolving [83].
2. The failure to produce candidates: with the right knowledge and skills [33].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3. The 2020 global cybersecurity workforce: currently estimated to be close to 3 million people, and that needs to grow by around 4 million in order to meet current demand. Therefore, policymakers understand that cyber education should start at an early age and that educating young people about cybersecurity could lead to them, one day, becoming cybersecurity professionals, so badly needed in the industry nowadays.

3.2.2. Economic incentives to enroll or upgrade cybersecurity education programs

There has been an increase in university majors that are tied to jobs with good employment opportunities, such as healthcare or law, and a rise in the popularity of courses that provide an early source of income such as the military and police academies. But there has also been a drop in those courses that are academically challenging, such as engineering and computer science [78]. This also has impact on cybersecurity education since most of the curricula are provided by engineering and computer science faculties. It is important to incentive the enrollment of practitioners in cybersecurity programs.

Examples of possible effects on cybersecurity are:

1. Public spending reduction on education: in Greece, the public spending has been reduced by 40% and more than 100 schools have been closed since 2009 as well as some universities Suspend Operations Due to Budget Cuts. Eurostat, the EU's statistics office, said that public expenditure on education accounted for 4.5% of GDP in 2013. However, it was just 3.2% of GDP, according to (official statistics by the State General Accounting Office). It's worth noticing that a 1.3% GDP difference is excessively high [78], [72].
2. During the crisis, the rate of Greek NEETs reached 29.5% in 2014, the highest percentage in the EU [74], [60].

3.2.3. Economic impact of inadequate (national) cybersecurity capabilities

Based on [1], [24] there is a very high chance that various companies and organizations do not even realize that they are falling victims of cybercrime and were therefore not able to report it due to the law measurements being taken against cybercrime. The European Cyber Security Organization argues that governments should tackle the cybersecurity skills gap through more educational and training offers. Curriculum designers are failing to realize the importance of having a multidisciplinary curriculum [42]. National authorities place importance on external outreach activities and collaboration opportunities that degrees have in place. From various education-to-labor market initiatives, such as workplace training, business mentoring or internships and traineeships, to more academic forms of collaborations with similar institutions, states seem to sponsor those degrees that enhance and enrich a vigorous national cybersecurity ecosystem. Finally, governments are interested in knowing about academic and employment outcomes. Most notably, they seek to know how many students enroll each year, how many graduates a course produces and possibly the types of jobs they end up securing after obtaining the degree [3], [6], [48].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Examples of possible effects on cybersecurity are:

1. Lack of awareness: This threat is noticed by professionals in both education and the public, as a lack of awareness of accidents. This makes us believe that this lack of awareness in cyber-crimes can be in the field of education, related to cybersecurity courses and the required skills, on the part of the academic staff and national authorities who are not sufficiently informed or trained [81].
2. A chance for an Innovative and financially profitable approach: Above the economic benefits of education is an ROI that investors cannot overlook. The global rate of ROI in schooling is approximately 10 percent for primary education, five percent for secondary education, and 16 percent for university education. The social ROI of education for the world is 18.9 percent for primary education, 13.1 percent for secondary education, and 10.8 for higher education. Finally, the private ROI of education for the world is 26.6 percent for primary education, 17 percent for secondary education, and 19.0 for higher education. The 10 percent ROI for education investments is higher than alternatives: 1.4 percent for treasury bills, 5.3 percent for treasury bonds, 4.7 percent for savings accounts, 3.8 percent for housing, and 7.4 percent for physical assets [47], [14].

3.2.4. Economic Impact of National Economic Resources

The cybercrime industry has especially escalated following the understaffing of government agencies mandates with cybersecurity, their lack of equipment that could match that used by the perpetrators, and the tons of workload they have to pile through to address these issues [3], [6].

An example of a possible effect on cybersecurity is:

1. Attempts have been put in motion regarding the need of upgrading government agencies in order to increase the quality of their outcomes when it comes to fighting cybercrimes (Papanikolaou et al., 2014b; Vaxevanakis, Zahariadis and Vogiatzis, 2003). These actions closely relate to educational cybersecurity in Greece [4].

3.2.5. Licensing costs of training platforms and cyber ranges

Cybersecurity education often relies on the use of (online) training platforms and/or cyber ranges. Some education providers have decided to develop their own platforms. In most of the above cases, there are licensing costs payable by the education providers for the training platform/range and in some cases even for the commercial off-the-shelf (COTS) software (e.g., Microsoft Office, Adobe products) incorporated into the training platforms/cyber ranges. These costs can be unnecessarily high. It would be beneficial to push for specific licensing programs when the training platforms/cyber ranges are used by education providers (especially non-commercial education providers) towards training the minimum necessary cybersecurity professionals. It is clear that the cyber range and similar cybersecurity training solution providers want to capitalize big on the high demand for new cybersecurity

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

professionals, but they also further aggravate the lack of skilled workforce by keeping their prices high [16], [32].

Examples of possible effects on cybersecurity are:

1. *High training platform costs*. Education providers need to be able to gain access to high-quality training platforms and cyber ranges without paying exorbitant one-time or regular licensing fees [20].
2. *High COTS costs*. Cyber range providers need to have deals with COTS solution providers (e.g., Microsoft, Adobe) if they plan to incorporate COTS in their scenarios. This increases the final costs of their range/training platforms and raises the bar for entering the cyber range market with novel platforms. Essentially, the prohibitive costs of COTS are hampering range/platform development [20].
3. *Outdated licensing models*. The licensing models of cyber range and COTS software providers usually do not envisage licensing models which would be aligned with their use in training platforms/ranges and utilized at and by cybersecurity education providers [20].
4. *Reluctance to incorporate COTS*. Training platform/range developers are often reluctant to incorporate scenarios involving COTS solutions, although they are the software components most frequently targeted by cyber adversaries. For example, most CTF challenges are on the Linux platform. This reluctance can be partially attributed to licensing costs [20].

3.2.6. Economic costs of incompatible training platforms and cyber ranges

Online cybersecurity training platforms and/or cyber ranges are incompatible, and they are not designed to easily exchange exercise blueprints and migrate challenges and/or scenarios to other platforms. This can be explained by the high costs of novel scenario development, but overall, it significantly increases the costs to train the next generation of cybersecurity professionals. It would be beneficial to develop standards or at least recommendations for standardizing scenario development. Docker Compose and similar containerization tools could be a thing to start with (on the technical front) [19], [32].

Examples of possible effects on cybersecurity are:

1. *Vendor lock-in*. This negative effect disallows education providers investing in a training platform or cyber range to easily switch to a different solution provider, e.g., to change from the Cyberbit cyber range to another platform [37].
2. *Duplicated effort*. Multiple teams at different education providers invest in unnecessary effort to develop new scenarios and training exercises which are the same. This duplicated effort could be easily eliminated if the scenarios were standardized and exchangeable. This effect might be observable even inside the REWIRE consortium, i.e., different institutions might develop highly similar training/CTF scenarios [37].

3.2.7. Effects of digital economy on skills demand

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

The digital economy is the share of total economic output derived from several broad "digital" inputs. These digital inputs include digital skills, digital equipment (hardware, software, and communications equipment) and the intermediate digital goods and services used in production. Such broad measures reflect the foundations of the digital economy [61]. The digital economy is a term that captures the impact of digital technology on patterns of production and consumption. This includes how goods and services are marketed, traded, and paid for. It is an activity that results from billions of everyday online connections among people, businesses, devices, data, and processes. The backbone of the digital economy is hyperconnectivity which means growing interconnectedness of people, organizations, and machines that results from the Internet, mobile technology, and the internet of things (IoT) [17]. Accenture Strategy research estimates that the digital economy, involving some form of digital skills and digital capital, represents 22.5 percent of the world economy (2020), digital's ability to unlock value is far from being fully exploited [64]. Besides the definition of digital economy, from a broader perspective, practically any economic activity cannot be performed without the involvement of digital technology. The rate of technology adoption and innovation has outpaced the ability to secure them and ensure a resilient digital economy. Cybersecurity is one of the pillars of the digital economy and without relevant skills there cannot be growth. Regarding the most recent (ISC)2 Cybersecurity Workforce Study 2020, there is an estimated shortage of 3.12 million cybersecurity professionals globally. That lack of skilled/experienced cybersecurity personnel is the top concern which challenges the approach to the adequate cybersecurity education [80].

Examples of possible effects on cybersecurity are:

1. *Skill gap*. The global shortage is estimated to 3.12 million cybersecurity professionals, without appropriate educational building blocks to ensure current and future needs [50].
2. *Capability gap*. Cyber security capability is more than simply the number of cyber security professionals - it is about the level and blend of skills required across the economy. Cybersecurity is a fast moving and ever-evolving area with a multidisciplinary nature as a domain with several specialisms [50].

3.3. Social Factor

Social factors consider demographics, population growth rate, age distribution, income distribution, family size, safety emphasis, health consciousness, trending lifestyle attitudes and cultural barriers. They can also include general consumer opinions and attitudes, dominant views of the media, law changes affecting social factors, change in lifestyle, attitude towards work, history and some other important considerations.
In the context of evaluating main factors, making impact on cybersecurity skills at any level, it is assumed that the subject is relatively new and quickly evolving. Therefore, the structure of factors, importance and effects are changing very rapidly and vary in different environments. During the analysis six aspects have been found. In the following sections, we briefly describe these aspects and their identified effects on cybersecurity education.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.3.1. Gender balance

Gender balance issue or lack of women involved in cybersecurity studies is addressed in different studies. Limited number of women enter CS studies and a significant part 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 cyber security jobs entail, and in some cases, how easy or difficult they find the subjects [42]. According to research [29] women working in cybersecurity in 2019 accounted for about one quarter (24%) of the overall workforce. Even though men outnumber women in cybersecurity by three to one, women in cybersecurity possess higher level of education and more certifications than their male counterparts and reach leadership positions [29]. For Europe, the percentage of women working in cybersecurity is estimated at only 7% [35].
A 2010 study [75] based on interviews with a small number of women that had reached the level of chief security officers and chief information officers has categorized the factors affecting the careers of cybersecurity professionals by social factors and institutional/structural factors. Social factors include work–family conflicts, informal networks, and social expectations for women. Institutional/structural factors include a lack of role models and mentors, occupational culture, institutional structure, and demographic composition. The study concluded that addressing the needs of women at the beginning of their careers-starting at educational institutions-is crucial to their successful entry and success in the field.
Similarly, a 2016 postgraduate [58] concluded that the main reasons that inhibit women's entry in the field are (a) the militaristic/gendered culture and language; (b) the cultural biases of influencers and decision makers (women's formative experiences, teachers, parents, and mentors may consciously or unconsciously steer them away from fields seen as more masculine); (c) realities and perceptions of work/life balance drive women away from the field. The study recommends that organizations should (a) qualitatively and quantitatively assess the current efficacy of workplace policies to increase the recruitment and retention of women in their cybersecurity operations; (b) create inclusive branding; (c) fund the talent through scholarships and continuing education programs tied to current or future employment to serve as a key success factor in getting and keeping women in the field; (d) reduce the use of militaristic language; (e) identify and control the hiring biases and (f) provide structured opportunities for mentorship, for women to have a safe space to discuss these challenges.
Gender balance is seen as a key to success in strengthening security capacities to safeguard European digital society, economy, and democracy. REWIRE should support the Women4Cyber initiative of the European Cybersecurity Organization (ECSO); the first online registry of European women in cybersecurity that will connect expert groups, businesses and policymakers to talents in the field [87].

Examples of possible effects on cybersecurity are:

1. No diversity in thinking and problem-solving. A traditional way of doing things prevails.
2. More complicated career paths for women, resulting in less attractive specialization.
3. The involvement of women represents an untapped resource.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.3.2. Diversified workforce

Although the Cybersecurity sector has been growing fast, it seems that it has not become culturally diversified. A 2018 U.S. study [54] has revealed that minority representation within the cybersecurity profession (26%) is slightly higher than the overall U.S. minority workforce (21%). Employment among cybersecurity professionals who identify as a racial or ethnic minority tends to be concentrated in non-management positions, with fewer occupying leadership roles, despite being highly educated. Diversity entails talent, representation, and fairness. Talent is equally distributed among the population, so when one or more social groups in a business or industry are under-represented, it is expected to have less talent than there is in the world at large. Diversity also facilitates the representation of different worldviews and different experiences. People with varied life experiences will come to problems differently. In terms of fairness, opportunities should be open to all and capable individuals should be able to thrive in a fascinating and rewarding field such as cybersecurity, regardless of their gender, ethnicity, sexuality, or any other factor [88].

Examples of possible effects on cybersecurity are:

1. Attracting fewer talented professionals.
2. Parts of society not represented in the industry.
3. Discriminatory work environment.

3.3.3. Lack of dedicated curricula and training and no clear identification of skills

There is an insufficient number of cybersecurity specific multidisciplinary curricula which would offer fundamental skills necessary for cybersecurity education. According to ENISA [14], the main issues with curricula are outdated or unrealistic platforms in education environments, difficulties in keeping pace with the outside world, lack of qualified cybersecurity educators, poor interaction with the industry, and little understanding of the labor market. These aspects could be further extended to lack of hands-on experience, which is pivotal in cybersecurity and balancing up to date information with the foundation of transferable skills that graduates can build on and can further extend in their careers. Moreover, employees are not being offered the right level of training, which is crucial for keeping pace with constant innovation in the industry and it is especially important for junior or mid-level professionals, who need to further develop their specialized knowledge in cybersecurity. In addition, there are no educational institutions, promoting cybersecurity as one of the key specializations in their portfolio. Cybersecurity remains a narrow specialization, not communicated as an attractive profession for diverse groups of young people.

Examples of possible effects on cybersecurity are:

1. Lack of applicants for cybersecurity degrees [14].
2. Mismatch between industry expectations and skills of graduates (qualitative issue) [42].
3. Shortage of qualified cybersecurity professionals (quantitative issue) [80].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.3.4. Stereotypes and misconceptions of cybersecurity

This aspect refers to the existence of several cybersecurity stigmas and misconceptions which have a negative impact on industry but also the outside world (society). The main identified stereotypes are as follows:

- Curricula focused on cybersecurity are currently emerging all over the world. However, these new degrees are often viewed as an add-on to computer science ones and fail to realize the critical importance of the interdisciplinary nature of this area [42].
- Most of the communication about cyber incidents appears from official public institutions. Thus, young people consider cybersecurity as a field of more public and less private sectors. The public sector in some cases is considered less appealing and not the path to be selected.
- There is a dominant attitude that cybersecurity subjects are mainly for experts. You can become an expert only after a relatively long career in the field. No clear career path is communicated.
- Parents play a significant role in directing children towards a certain career. Cybersecurity is left unknown to the older generation and they are not able and willing to encourage the younger generation to study this subject.

Examples of possible effects on cybersecurity are:

1. Mismatch between industry expectations and skills of graduates [42].
2. Shortage of qualified cybersecurity professionals [42].
3. Less interest in cybersecurity studies.
4. Insufficient number of women and diversity among workforce [80].

3.3.5. Social impact

In today's high-tech world, beliefs, opinions and attitudes are shaped as people engage with others in social media, and through the internet. With the rise of online platforms where individuals could gather and spread information came the rise of online cybercrimes aimed at taking advantage of not just single individuals but also collectives [59]. In response to these cyber-mediated threats to democracy, a new scientific discipline has emerged—social cybersecurity. 'Social Cybersecurity' focuses on the science to characterize, understand, and forecast changes in human behavior, social, cultural and political outcomes, and to build the cyber-infrastructure needed for society to persist in its essential character in a cyber mediated information environment under changing conditions and actual or imminent cyber threats [49], [76].

Examples of possible effects on cybersecurity are:

1. Spread of disinformation and false data.
2. Technology used to distort public opinion.
3. The threat to democracy.
4. The free exchange of views and ideas should be supported.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.3.6. Social Awareness

Although cybersecurity is one of the most important challenges faced by governments today, visibility and public awareness remains limited. Almost everybody has heard of cybersecurity, however, the urgency and behavior of people do not reflect a high level of awareness. Communicating cyber-security is confronted with paradoxes, which has resulted in society not taking appropriate measures to deal with the threats [46], [10].

Examples of possible effects on cybersecurity are:

1. Cybersecurity is a public concern receiving insufficient awareness.
2. End-users of the internet are the ones who are most vulnerable to cyber threats. Awareness should be raised among children, teenagers, parents, and teachers on good practices on the internet and social networks.
3. Developing clear, evidence-based messages can contribute to informed policymaking and policy decisions.

3.4. Technological Factor

Technological factors are variables that concern the existence, availability, and development of technology relevant to the target of analysis. In the case of REWIRE, the relevant technological aspects are those that influence the need for and the possibilities of cybersecurity education. During the analysis six aspects have been found. In the following sections, we briefly describe these aspects and their identified effects on cybersecurity education.

3.4.1. Cyber Ranges

A cyber range [57] is a virtual environment used for cyber warfare training and evaluation of new software components. These are inherently complex, automated IT environments that make it possible to emulate real-world scenarios for training groups of professionals. There are important means of training groups of security professionals in the areas of ethical hacking and in threat identification and response [30].

Examples of possible effects on cybersecurity are:

1. The lack of state-of-the-art cyber ranges makes it difficult to provide hands-on experience during education.
2. Limited levels of automation in cyber ranges make education and training human labor intensive and hence expensive.
3. The usability of cyber ranges is significantly hindered by disunity [84]. This inconsistency then means that teams cannot share the content created with each other and thus continue to collaborate unless one of the teams moves completely to a competitive platform.
4. Another interesting aspect is licensing. Sometimes it is necessary to use licensed software or firmware, which must be licensed online.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.4.2. Availability of Tools

Hardware and software tools are essential for providing hands on experience about the configuration and the potential vulnerabilities of software systems and of networks and are also essential for the demonstration of solutions for mitigation. Tools should be as simple as possible so as to allow students to maintain focus on essential features that are at the core of the educational curriculum [68], [73].

Examples of possible effects on cybersecurity are:

1. The availability of tools, e.g., Virtual Labs, sandbox environments, designed for the educational curriculum can help in achieving the learning objectives more efficiently than textbook only education [30].
2. Common virtualized training platforms would enable sharing best experiences among education providers [30].

3.4.3. Digitalization of Society

Digitalization of society refers to the proliferation of connectivity and computing in basic societal functions, such as critical infrastructures, home automation, finances, home entertainment, personal communication, and business transactions [38]. Digitalization of society increases the attack surface and enables new attack vectors to be developed and used, possibly at a massive scale, with significant societal impact [8].

Examples of possible effects on cybersecurity are:

1. An increased level of digitalization of societal systems will involve increased risk due to cyber-attacks [34] and an increased demand for cyber security professionals, hence for cybersecurity education. It will possibly also increase the amount of financial support for cybersecurity education.
2. Digitalization creates a need for universal security education for the masses, not only expert education.

3.4.4. Emerging Technologies

There are a number of emerging technologies that have the potential to change the way computers, networks, systems are operated, and may have a fundamental effect on the vulnerabilities, threat models, and attacker capabilities, and would require a redesign of security curricula. Examples include quantum computing, machine learning and cyber-physical systems [27], [2], [67].

Examples of possible effects on cybersecurity are:

1. The emergence of economically feasible quantum computing would have a disruptive effect on software systems and would require re-education of professionals [67].
2. The emergence of new technologies will increase the demand for “Availability of Tools” aspect, as new hardware and software tools will be needed for state-of-the-art education [39], [45].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.4.5. Generalization of Cyber Attacks

Given the increased digitalization of society, we are witnessing a significant extension and diversity of cyber-attacks. Some of these attacks (e.g., spam, phishing, even ransomware) are relatively low-tech, but can be realized at a very large scale, creating significant damage and even cascading effects [77]. These low-tech attacks may target even educated users (such as doctors) who fall victims to traps despite high education. Other attacks are highly sophisticated and difficult to detect; therefore, the damage is significant due to the skills of the attacker and due to the duration of the attack [82].

Based on [36], examples of possible effects on cybersecurity are:

1. Education has to be continuously updated with respect to the new threat landscape.
2. The new threat landscape makes the cybersecurity curriculum richer and allows a more general discussion about the relationship between technological and societal factors.

3.5. Legal Factor

This factor has both external and internal sides. There are certain laws that affect cybersecurity or business environment in a certain country while there are certain policies that companies maintain for themselves. Legal analysis takes into account both angles and then charts out the strategies in light of these legislations. For example, cybersecurity laws, personal data protection law, consumer laws, and computer law. During the analysis five aspects have been found. In the following sections, we briefly describe these aspects and their identified effects on cybersecurity education.

3.5.1. European Certification lack

Certification [85], [40] is a well-established traditional means to define and formalize desired properties and behaviors or best practices to achieve them – by establishing criteria – and to gain confidence about the validity of such properties and behaviors – by evaluation of a system or service against the criteria. The European Cybersecurity Act [70] became effective in June 2019 and establishes the European Cybersecurity Certification Framework, targeting the security of products, services, and processes under which the European Cybersecurity Agency (ENISA) is expected to propose several harmonized schemes in the coming years, including a scheme for cloud services. Cyber security certification of products, services, and processes [44] is currently used only to a limited extent. If it exists, then mainly at Member State level or within systems defined by the needs of industry. In this context, certification granted by one national cyber security certification body is in principle not recognized in other Member States. Existing certification schemes show significant lacks and differences in terms of product coverage, levels of guarantees, essential criteria and actual use, which hampers mutual recognition mechanisms within the Union.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Examples of possible effects on cybersecurity are:

1. Students/employers should be aware of cybersecurity certification, which ensures that products, services, and processes meet established security requirements in terms of protection of availability, confidentiality, and integrity.
2. The certification can be obtained by the company/university for its IT products or services upon application to the relevant national security authority. It is thus possible to obtain one of the levels of guarantees (security levels): "basic", "significant" or "high" based on the level of potential risk for the whole company in the event of data leakage.

3.5.2. Legal framework unification lack

Europe lags [14], [86] behind in the development of a comprehensive approach to define a set of roles and skills relevant to the cybersecurity field. Though cybersecurity is a worldwide matter affecting all countries, there are a number of differences between national states. For this reason, existing cybersecurity frameworks may be incompatible with or in general not targeted to the European needs [26], laws and regulations. Even though many attacks are carried out across multiple jurisdictions and often originate in foreign countries, current international law does not recognize nations as duty bound to assist in investigating a cyberattack that allegedly originated within their jurisdiction. As a result, nations attempting to develop and enforce cybersecurity measures often lack international support from nations where a given cyberattack likely originated [41].

An example of a possible effect on cybersecurity is:

1. Unification of cyber laws in different countries will lead to simplification of international cooperation in the case of cybercrime and other cyber activities. Staff/students should be aware of the differences in protection measures in different countries and should be trained in the new unified cyber security legislation, data flow mapping, and privacy.

3.5.3. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity

People's concerns about digital privacy extend to those who collect, store, and use their personal information. Additionally, the majority of the public are not confident that corporations are good stewards of the data they collect. Europe's GDPR [69] is the most wide-ranging, comprehensive piece of data privacy legislation. The GDPR requires appropriate security measures and therefore takes a risk-based approach. Students should be aware of possible risk to the protection of personal data related to data storage, according to applicable legislation. About the right way of data processing, adequate storage period, access rules, authorized purpose, etc. This is not limited to GDPR but all related fields have to be included in this scope [7].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

An example of a possible effect on cybersecurity is:

1. GDPR awareness is one of the possible effects. To be aware as a person/student of personal data protection and privacy. To better understand what kind of personal information could be processed and provided with consent [28].

3.5.4. Standardization of cybersecurity roles definition and cybersecurity skills across EU

Cybersecurity roles [14] with respect to cybersecurity skills is currently a grey area as no specific map of what skills are needed for certain cybersecurity roles exists. There is a considerable number of qualifications, both university and association driven qualifications that create a maze 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 that needs to be mitigated through Standardization initiatives. Common understanding is crucial for co-operation in developing and improving cybersecurity skills and educational programs, and in evaluating cybersecurity skills across EU member states.

Examples of possible effects on cybersecurity are:

1. Unclear career paths due to uncertainty of the envisaged cybersecurity role.
2. Cybersecurity roles assigned to people who are not fully prepared to excel in that role. Increased liability and legal risks due to unclear role definition.

3.5.5. Missing comprehensive cybersecurity officer role description

Comprehensive cybersecurity officer role description in organizations is missing compared to data privacy officer defined in GDPR [23]. Along with cybersecurity becoming a more important integral part of Europeans' security [14], cybersecurity roles in organizations require more attention. Legal requirements for cybersecurity roles are not defined in law. They could be looking to data privacy officer role definition in GDPR. Moreover, cybersecurity roles may need different roles in organizations to be fully capable of addressing all cybersecurity topics.

An example of a possible effect on cybersecurity is:

1. Missing common understanding of cybersecurity roles definitions and required skills for such roles.

3.6. Environmental Factor

Environmental factors in PESTLE Analysis 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, geographical location, global changes in climate, environmental offsets, etc. Like all other factors, environmental factors will provide specific knowledge regarding how the conditions at the time of the project influence

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

cybersecurity and cybersecurity education. During the analysis three aspects have been found. In the following sections, we briefly describe these aspects and their identified effects on cybersecurity education.

3.6.1. 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 [62]. Environmental migrants are defined as "persons or groups of persons who, predominantly for reasons of sudden or progressive changes in the environment that adversely affect their lives or living conditions, are obliged to leave their habitual homes, or choose to do so, either temporarily or permanently, and who move within their country or abroad" [51].

Examples of possible effects on cybersecurity are:

1. Environmental migrants will need to find jobs in their new locations. A viable career opportunity would be cybersecurity related jobs since there is a growing need for such professionals. In order to be able to procure such jobs, the skills and knowledge on the subject should be internationally agreed upon and standardized.
2. Climate change and its implications will act as a destabilizing factor on society. When livelihoods are in danger, this will spark insecurity and drive resource competition. This does not only have implications on physical security, but in modern society, this also has an impact on cybersecurity and its associated threats. More and more cybersecurity professionals would be needed to provide solutions and services.

3.6.2. Covid-19 pandemic crisis

Coronavirus disease (COVID-19) is an infectious disease caused by a newly (2019) discovered coronavirus. Most people infected with the COVID-19 virus will experience mild to moderate respiratory illness and recover without requiring special treatment. Older people, and those with underlying medical problems like cardiovascular disease, diabetes, chronic respiratory disease, and cancer are more likely to develop serious illness. The best way to prevent and slow down transmission is to be well informed about the COVID-19 virus, the disease it causes and how it spreads [9]. 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. These were established to prevent the further spread of the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), which causes COVID-19. By April 2020, about half of the world's population was under lockdown, with more than 3.9 billion people in more than 90 countries or territories having been asked or ordered to stay at home by their governments.

Examples of possible effects on cybersecurity are:

1. Cybersecurity education has moved mainly to online education due to the limitations caused by the COVID-19 pandemic. This made it difficult to teach cybersecurity in

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

topics that require the physical presence of students at school (e.g., topics related to securing hardware devices) [55].

2. The pandemic crisis increased the dependency on IT (especially remote and cloud services and tools) and thus their exposure to cyber related threats. Many organizations were unprepared for the transition both from a technical perspective and from a human/awareness perspective.

The need for Cybersecurity education at various levels is more increased than ever [31], [18].

3.6.3. Connected devices controlling environmentally sensitive productions

The smart factory [71] represents a leap forward from more traditional automation to a fully connected and flexible system-one that can use a constant stream of data from connected operations and production systems to learn and adapt to new demands [5]. Legacy Supervisory control and data acquisition (SCADA) devices are being replaced by new connected devices allowing for an increased control over the processes and a greener operation. Possible cybersecurity incidents could lead to huge environmental disasters [79].

Examples of possible effects on cybersecurity are:

1. Cybersecurity education should evolve to cover also practical issues concerning not only the IT environment but also the OT.
2. There is an increased demand for cybersecurity professionals with practical and related knowledge.

3.7. Summary

Many aspects from all areas of the PESTLE factors are identified and described in detail. REWIRE project experts in each field (i.e., Political, Economic, Social, Technological, Legal and Environmental) cooperated on this demanding task. This is an important step which allows us to obtain a comprehensive view of the situation across Europe. Moreover, during the aspect's identification, their main effects were defined. It is remarkable that many identified effects of aspects from different groups of factors overlap, at least partially, as is clear from their descriptions. It is natural and helpful in the next stage, where the connections between the identified aspects were searched and their importance was evaluated carefully.
All identified aspects are referenced with relevant, up-to-date, and mostly European-level references. A total of 31 aspects are identified at this stage. This number proves the importance of the cybersecurity education and presence of many lacks that should be addressed in the future.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

4. OVERVIEW OF PILOTS' OUTCOMES

This chapter contains questionnaire results for each pilot project. The purpose is to show which aspects were already identified by pilot projects since REWIRE is based on input from these projects. Identified aspects are shown along with their linkages to other aspects. Collected data is structured into tables along with justification and a mind-map for each pilot project for a more comfortable overview and graphical representation of the table contents. These findings can help in getting a better overview of the current situation in European cybersecurity education analysis.

4.1. CONCORDIA

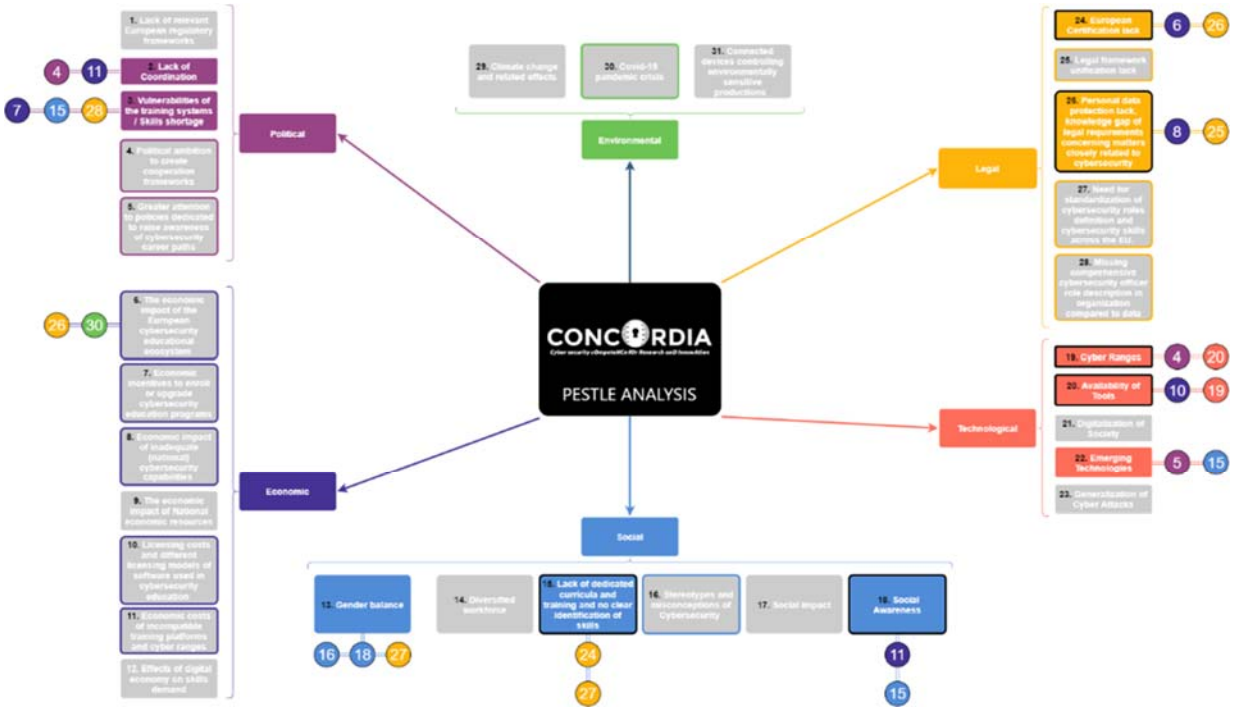

Figure 5. Mind-map representing aspects identified by REWIRE which were also identified by CONCORDIA pilot project and their respective connection(s) to other aspects.

Factor group	Aspect name	Importance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	2. Lack of coordination	High	4. Political ambition to create cooperation frameworks	It aims to provide organizations a way to engage discussion on cybersecurity-related topic and set up groups like the Observer group with standardization and certification entities [1].
			11. Economic costs of incompatible training platforms and cyber ranges	It aims to provide organizations and individuals a way to promote their courses, trainings, cyber-ranges, tools, and open positions [1]

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	3. Vulnerabilities of the training systems / Skills shortage	Medium	15. Lack of dedicated curricula and training and no clear identification of skills	The majority of the courses help develop skills applicable to at least 4 CONCORDIA industry sectors. Nevertheless, a number of other courses are targeting different other industries such as cloud, IoT, critical information infrastructure or operating systems, while almost a quarter of the courses are not related to any industry in particular [2].
			7. Economic incentives to enroll or upgrade cybersecurity education programs	They provide structured information on the courses/trainings they are organizing for Cybersecurity professionals [2].
			28. Missing comprehensive cybersecurity officer role description in organization compared to data	Methodology pledges for the idea of developing the course based on specific industry needs; getting involved with the corporates from the targeted industry from the beginning of the process is paramount [3].
E	No identified aspects for Economic Factor			
S	13. Gender balance	High	18. Social Awareness	Raise awareness about the cybersecurity culture, stress-ing its impact on society and state sovereignty and, therefore, its profound influence on one's everyday life [4].
			27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	The European Charter of Fundamental Rights explicitly provides for the principle of equality between men and women in all areas including employment, work and pay; the Charter, also, provides for the '' maintenance or adoption of measures providing for specific ad-vantages in favour of the under-represented sex'' [4]
			16. Stereotypes and misconceptions of Cybersecurity	Cybersecurity is a field that requires not only technical experts but proactive people with strong managerial and soft skills. This is where we can best engage with and attract girls and women to the profession and how we can ultimately fill the skills gap and ensure fair and equal representation in cybersecurity [4].
	15. Lack of dedicated curricula and training and no clear identification of skills	High	24. European Certification lack	In the top of the most important qualifications for employment, cybersecurity certifications are ranked in Top 3, after relevant cybersecurity work experience and knowledge of advanced cybersecurity concepts [5] [6].
			27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	Companies agree that an EU harmonized taxonomy related to the cybersecurity skills linked to different job positions would be useful in the process of recruitment [6].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	18. Social Awareness	Medium	15. Lack of dedicated curricula and training and no clear identification of skills	Focus on developing methodologies and frameworks to design, certify, and teach courses for cybersecurity professionals, mid-managers, executives, and teachers as well as describe processes for using them [7].
			11. Economic costs of incompatible training platforms and cyber ranges	Discussion among all project partners with the goal of defining requirements and objectives for Threat Intelligence (TI) sharing. Later on, the collected feedback guided the search for TI platforms available on the market that could fulfill CONCORDIA's needs [7].
T	19. Cyber Ranges	Medium	20. Availability of Tools	A steadily growing inventory of tools, cyber range platforms, and training offerings have been created [8].
			4. Political ambition to create cooperation frameworks	Establish the groundwork for information sharing of cyber threats. The Threat Intelligence Platform is under development and utilizes the MISP open-source threat intelligence platform that was successfully validated at DFN-CERT [8].
	20. Availability of Tools	Medium	19. Cyber Ranges	Reinforce Europe's cybersecurity leadership by developing and evaluating building blocks for a European cross-sector cybersecurity infrastructure, specifically for collaborative threat handling, technology and service experimentation, training and education, and starting up new businesses [9]
			10. Licensing costs and different licensing models of software used in cybersecurity education	Services activity aims to create a curated portfolio of public and proprietary tools and available cybersecurity labs to create a cutting-edge advantage for the partners to speed up research and development of cybersecurity systems [10].
	22. Emerging Technologies	Medium	15. Lack of dedicated curricula and training and no clear identification of skills	Cyber range platforms, CR-based training, and related tools are the main focus of the Training activity. Initial discussions were started with technical topics such as technical federation, exchange of scenarios, automatic execution of attack scenarios, scoring mechanisms and network simulation/emulation [11].
			5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Aims at collecting feedback regarding specific needs in terms of Education for Cybersecurity professionals. In view of doing so we will share with the participants our work so far in terms of Skills Certification Schemes and on developing courses for cybersecurity professionals while also seeking their

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				views on the concrete pilots we plan to run together this year and targeting the Cybersecurity Consultant profile [12].
L	24. European Certification lack	Medium	6. The economic impact of the European cybersecurity educational ecosystem	Check for the existing courses addressing the different needs of the target audience. Look into the online offer and the face-to-face offer, on courses offered for free or against a fee, on general courses and tailored made courses, on location, timing and language used for teaching [13][14].
			26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	Proposed methodology addressing these gaps by considering the actual needs of both the industry impacted by cybersecurity (e.g., Telecom, eHealth, Transport, Defense) and the industry professionals [14].
	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	Low	25. Legal framework unification lack	Lawmakers in the EU submitted a proposal for a new privacy regulation with the view of updating existing rules relating to privacy and electronic communications and building trust and security in the Digital Single Market [15].
			8. Economic impact of inadequate (national) cybersecurity capabilities	There is a greater need for companies and nations for higher protective measures concerning their cyber activities [15].
E	No identified aspects for Environmental Factor			

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

[1] CONCORDIA has identified a number of key stakeholders, including the Member States, ENISA, Europol, EDA, and ECSO, with which it has established and foster liaisons. This close collaboration with stakeholders aims at achieving a constant alignment of activities, to match the security needs of Europe. T.4.6 Liaison with Stakeholders. Antonio Iannillo et al., Concordia Deliverable 4.7 - Year 1 Report on the Liason with Stakeholders. https://www.concordia-h2020.eu/wp-content/uploads/2020/05/D4.7-Year1ReportOntheLiaisonwithStakeholders.pdf , 2019 .

[2] CONCORDIA has assessed the courses for Cybersecurity professionals already developed by CONCORDIA partners, a well as asked the CONCORDIA industry about their needs in terms of skills and technical people. T3.4 - Establishing an European Education Ecosystem for Cybersecurity. Felicia Cutas et al., Assessing the Courses for Cybersecurity Professionals Already Developed by CONCORDIA Partners, https://www.concordia-h2020.eu/wp-content/uploads/2020/04/CONCORDIA-AssessmentOfCoursesT3.4-ForWebsite.pdf, 2019.

[3] The skill shortage leads to the identification of skills that are used for the creation and deployment of new cybersecurity courses. Felicia Cutas et al., Concordia Methodology for the Creation and Deployment of New Courses and/or Teaching Materials for Cybersecurity Professionals, https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-methodology-courses-professionals-for-publication.pdf, 2020.

[4] CONCORDIA is promoting workforce diversity in the field of cybersecurity, in particular by incentivizing women to join the field of cybersecurity, via positive measures including dedicated events and information days. Task T4.5 - Women in cybersecurity. Barbara Carminati et al., Woman in Cybersecurity: A Manifesto for Today, https://www.concordia-h2020.eu/wp-content/uploads/2019/09/WomenInCyberMANIFESTO.pdf, 2019.

[5] CONCORDIA has assessed the courses for Cybersecurity professionals already developed by CONCORDIA partners, a well as asked the CONCORDIA industry about their needs in terms of skills and technical people. T3.4 - Establishing an European Education Ecosystem for Cybersecurity. Felicia Cutas et al., Assessing the Courses for Cybersecurity Professionals Already Developed by CONCORDIA Partners, https://www.concordia-h2020.eu/wp-content/uploads/2020/04/CONCORDIA-AssessmentOfCoursesT3.4-ForWebsite.pdf, 2019.

[6] The skill shortage leads to the identification of skills that are used for the creation and deployment of new cybersecurity courses. Felicia Cutas et al., Concordia Methodology for the Creation and Deployment of New Courses and/or Teaching Materials for Cybersecurity Professionals, https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-methodology-courses-professionals-for-publication.pdf, 2020.

[7] CONCORDIA has a Teach-The-Teacher activity aiming at producing cybersecurity courses for teachers, guidelines and teaching methodologies. T3.4 - Establishing an European Education Ecosystem for Cybersecurity. Felicia Cutas et al., Concordia Deliverable D3.1: 1st Year Report on Community Building and Sustainability, https://www.concordia-h2020.eu/wp-content/uploads/2020/05/D3.1-1stYeaReportOnCommunityBuildingandSustainability.pdf, 2019.

[8] CONCORDIA is working on the development of cyber-range platforms, and the organization of capture-the-flag / cyber training events. T.3.3 Developing the CONCORDIA's Ecosystem: Virtual Lab, Services, and Trainings. Felicia Cutas et al., Concordia Deliverable D3.1: 1st Year Report on Community Building and Sustainability, https://www.concordia-h2020.eu/wp-content/uploads/2020/05/D3.1-1stYeaReportOnCommunityBuildingandSustainability.pdf, 2019.

[9] CONCORDIA is working on the creation of a curated portfolio of public and proprietary tools and available cybersecurity labs to create a cutting-edge advantage for the partners to speed up research and development of cybersecurity systems. T.3.3 Developing the CONCORDIA's Ecosystem: Virtual Lab, Services, and Trainings. Deliverable 3.1. https://www.concordia-h2020.eu/wp-content/uploads/2020/05/D3.1-1stYeaReportOnCommunityBuildingandSustainability.pdf

[10] The identified tools can be deployed over / enrich cyber-range platforms. Felicia Cutas et al., Concordia Deliverable D3.1: 1st Year Report on Community Building and Sustainability, https://www.concordia-h2020.eu/wp-content/uploads/2020/05/D3.1-1stYeaReportOnCommunityBuildingandSustainability.pdf, 2019.

[11] CONCORDIA is working on the identification of emerging cybersecurity threats based on working groups in technology domains of interest. T.4.1. Working groups in technology domains of interest. Claudia Ardagna et al., Deliverable D4.1: 1st Year Report on Cybersecurity Threats. https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf, 2020. [12] The identified technologies and threats may contribute to the elaboration of curricula and training. https://www.concordia-h2020.eu/workshops/workshop-education-2020/ [13] CONCORDIA is working on a feasibility study with respect to a course certification framework for cybersecurity skills. T3.4 - Establishing an European Education Ecosystem for Cybersecurity. Argyro Chatzopoulou et al., Feasibility Study "Cybersecurity Skills Certifications", https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-SkillsFeasibilityStudy-forpublication.pdf, 2020. [14] The identified skills are then used by the certification framework to assess competencies. .Felicia Cutas et al., Concordia Methodology for the Creation and Deployment of New Courses and/or Teaching Materials for Cybersecurity Professionals, https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-methodology-courses-professionals-for-publication.pdf, 2020. [15] CONCORDIA is looking into the associated legal considerations from the point of view of privacy and security, as being addressed in the context of EU Law. The objective is to address how the relevant legal obligations influence in reality organizational practices that link to fundamental principles of data processing (e.g. privacy by design) and data subjects' rights (e.g. data portability). T4.2 Legal Aspects. Claudia Ardagna et al., Deliverable D4.1: 1st Year Report on Cybersecurity Threats. https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf, 2020.

Table 1. Concordia.

4.2. CyberSec4Europe

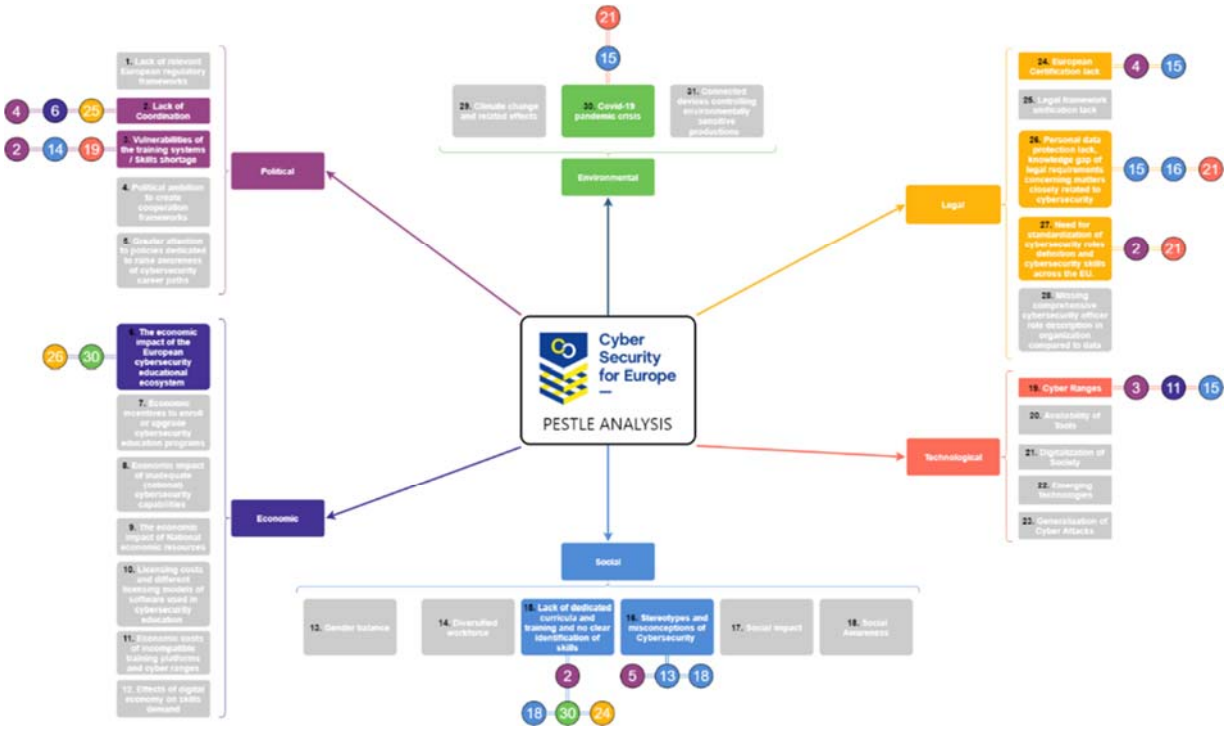

Figure 6. Mind-map representing aspects identified by REWIRE which were also identified by CYBERSEC4EUROPE pilot project and their respective connection(s) to other aspects.

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	2. Lack of coordination	High	4. Political ambition to create cooperation frameworks	Lack of coordination and common governance is in part the result of lack of political will to support such initiatives [1].
			25. Legal framework unification lack	Cybersec4Europe proposed legal framework that would enhance coordination and cooperation among EU member states and their governmental and professional bodies and institutions [1].
			6. The economic impact of the European cybersecurity educational ecosystem	The CyberSec4Europe project identifies that the European Union must ensure that a sufficient number of highly qualified technicians, scientists and other professionals in all areas of cyber security are trained and prepared to support and lead to address current and future industrial, scientific, social and policy challenges related to cyber security. Which can be very costly for some countries [2].
E	6. The economic impact of the European cybersecurity	Medium	26. Personal data protection lack, knowledge gap of legal requirements	IT costs are expected to increase due to new, strong security requirements and the opening of APIs. This - in addition to changing customer expectations, increased

	educational ecosystem		concerning matters closely related to cybersecurity	digitization and privacy - could be why we see banks experimenting with their APIs, in collaboration with financial technology companies (also known as FinTechs) and focused on customer orientation and security. For this reason, there is a need to thoroughly train and educate employees in these new technologies with more advanced security [3].
			30. Covid-19 pandemic crisis	The Covid-19 pandemic crisis has increased online human interactions, leading to increased demands on IT technology and cybersecurity. Awareness should be taken to provide the necessary IT technologies for quality training and education of employees or students [2].
S	16. Stereotypes and misconceptions of Cybersecurity	Medium	18. Social Awareness	Awareness of cybersecurity risks is clearly lacking and therefore, there are many stereotypes and misconceptions in this area. The project dealt with identifying issues and proposing effective program to deal with lack of awareness specifically among SMEs [4].
			5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	One of the reasons why there are many misconceptions is because we are lacking policies that would promote cybersecurity as a part of anyone's career [4].
			13. Gender balance	It is necessary to ensure fair diversity and gender balance and Member States' representation in cybersecurity [1].
	15. Lack of dedicated curricula and training and no clear identification of skills	Medium	2. Lack of coordination	There is no governance of cooperation between education and training providers both at the level of individual member states and the whole EU. This leads to unavailability of comprehensive and compatible skills frameworks and curricula [2].
			30. Covid-19 pandemic crisis	The Covid-19 pandemic crisis has increased online human interactions, leading to increased demands on IT technology and cybersecurity. Awareness should be taken to provide the necessary IT technologies for quality training and education of employees or students [2].
			24. European Certification lack	There is a need to enforce the education and training the security of the developed IT products (security enforcement) at European level [2]. Certification is a common mean used to validate whether a product has proper security levels in industry (certification security products) [5].
			18. Social Awareness	CyberSec4Europe focused on designing a new metric for the evaluation of a cybersecurity awareness programme. The proposition provides factors to be measured and their respective measurement methods in order to realise each of the indicators:

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				measuring positive changes in cybersecurity knowledge, measuring the changes in organizational policies, measuring the quality of awareness materials and effectiveness of delivery channels, measuring audience interest and active participation in the awareness programme [6].
T	19. Cyber Ranges	Medium	15. Lack of dedicated curricula and training and no clear identification of skills	There are some cyber ranges available throughout the EU, but these are not cross-compatible, in most cases proprietary and often cannot be commonly used. So, there is lack of coordination and knowledge on what purpose should cyber ranges serve and how should be interconnected and commonly implemented [2].
			3. Vulnerabilities of the training systems / Skills shortage	Lack of commonly available cyber ranges with shared training scenarios leads to shortage of commonly available training systems and tools for professionals [2].
			11. Economic costs of incompatible training platforms and cyber ranges	Unavailability of commonly used and available cyber ranges and scenarios leads to greater and unnecessary costs [7].
L	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	Medium	16. Stereotypes and misconceptions of Cybersecurity	The project conducted a comparative study of legal frameworks dealing with cybersecurity and data protection. It found there are discrepancies in these frameworks which could lead to misconceptions in this area [3].
			15. Lack of dedicated curricula and training and no clear identification of skills	Increase the level of cybersecurity skills, both across EU institutions and between them and member states. This can be seen from an institutional perspective, in terms of institutional coordination, but also as a deeper understanding of the protection of personal data and how it should be approached [3].
			21. Digitalization of Society	Increase the level of cybersecurity skills, both across EU institutions and between them and member states. This can be seen from an institutional perspective, in terms of institutional coordination, but also as a deeper understanding of the protection of personal data and how it should be approached [3] [5].
	27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	Medium	2. Lack of coordination	The project states a clear need to implement standardization in the cybersecurity area both in terms of technologies, services and processes as well as in terms of education. Lack of coordination leads to problems which prevent effective implementation of standardization among EU member states [8].
			21. Digitalization of Society	Deployment of modern technology and the development of modern tools of digital transformation, which in tun require

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				advanced secure solutions for processing data and not only for secure payments [3]
	24. European Certification lack	Medium	4. Political ambition to create cooperation frameworks	Global interest, participation and influence of other countries in cybersecurity standardization and certification, especially from Asia, poses a challenge to appropriately cover all projects in order to make sure that the European voice is heard. European Standardization is important also for the Common Market, but it should not reduce paying attention to global standardization [8].
			15. Lack of dedicated curricula and training and no clear identification of skills	Education and training should be more effective in gaining greater awareness and skills regarding certification at a European level. It is necessary to involve instructors who are sufficiently qualified in this area [1].
E	30. Covid-19 pandemic crisis	Medium	15. Lack of dedicated curricula and training and no clear identification of skills	MOOCs would be effective tool to provide good online education on cybersecurity in the pandemic situation, but if there is no skills framework and available curricula and training, it is difficult to base MOOCs on any substantive content [2].
			21. Technological - Digitalization of Society	Deployment of modern technology and development of modern digital transformation tools that require modern secure solutions for data processing to suppress cyber-attacks during a pandemic [3].

[1] Kadenko Natalia, CyberSec4Europe D2.1 Governance Structure v1.0, January 2020
https://cybersec4europe.eu/wp-content/uploads/2020/02/D2.1-Governance-Structure-final-Submitted.pdf

[2] Dragoni Nicola, CyberSec4Europe 6.2 Education and Training Review, January 2020
https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf

[3] Mantelero Alessandro, CyberSec4Europe D4.2Legal Framework, January 2020
https://cybersec4europe.eu/wp-content/uploads/2020/09/CS4E-D4.2-Legal-Framework_post-rev_20200914_v1.1.pdf

[4] Chaudhary Sunil, CyberSec4Europe D9.6 SME cybersecurity awareness program 1, March 2020
https://cybersec4europe.eu/wp-content/uploads/2020/04/D9.6-SME-cybersecurity-awareness-program-1-V-1.0-Submitted-1.pdf

[5] Skarmeta Antonio, CyberSec4Europe D3.1 –Common Framework Handbook 1, October 2019
https://cybersec4europe.eu/wp-content/uploads/2020/06/D3.1-Handbook-v2.0-submitted-1.pdf

[6] Chaudhary Sunil, CyberSec4Europe D9.13 Awareness effectiveness study, January 2021
https://cybersec4europe.eu/wp-content/uploads/2021/02/D9.13-Awareness-effectiveness-study-v1.0-submitted.pdf

[7] Suni Elina, CyberSec4Europe D7.1 Report on existing cyber ranges, requirements, August 2020 https://cybersec4europe.eu/wp-content/uploads/2020/09/D7.1-Report-on-existing-cyber-ranges-and-requirement-specification-for-federated-cyber-ranges-v1.0_submitted.pdf
[8] Miller Mark, CyberSec4Europe D8.1 Cybersecurity Standardization Engagement Plan, July 2019 https://cybersec4europe.eu/wp-content/uploads/2019/11/CS4E-Deliverable-D8.1_v2.1_2019_08_05_final.pdf

Table 2. CyberSec4Europe.

Aspect name	Notes
2. Lack of coordination	The CyberSec4Europe project developed a bottom-up cybersecurity governance framework, that would enhance coordination, cooperation and governance throughout the EU. The project also proposed the introduction of MOOCs as a pilot project for the governance model.
15. Lack of dedicated curricula and training and no clear identification of skills	There is a clear lack of common understanding of skills required in cybersecurity fields - the deliverable deals with this question as well. The project plans to issue Deliverable 6.3 that will deal with this in detail.
19. Cyber Ranges	Cybersec4europe recognizes lack of available cyber ranges briefly within their analysis of available MOOCs in the deliverable 6.2.
30. Covid-19 pandemic crisis	Cybersecu4europe promotes higher availability of distance learning and MOOCs as a prevention in pandemic situations. They are considering preparing a deliverable specifically dealing with this challenge.
3. Vulnerabilities of the training systems / Skills shortage	The deliverable deal specifically with the availability of training in cybersecurity in individual member states. The conclusions state that there is a lack of coverage, specifically in smaller member states.
26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	There are clear discrepancies in how cybersecurity is ensured in individual legal frameworks. The CyberSec4Europe project conducted a comparative study of these frameworks to pin out these discrepancies and propose solutions in individual deliverables of the project.
27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	The project analyzed available standardization efforts and frameworks within and outside the EU to propose a coordination approach to standardization in cybersecurity.

Table 3. CyberSec4Europe Notes.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

4.3. ECHO

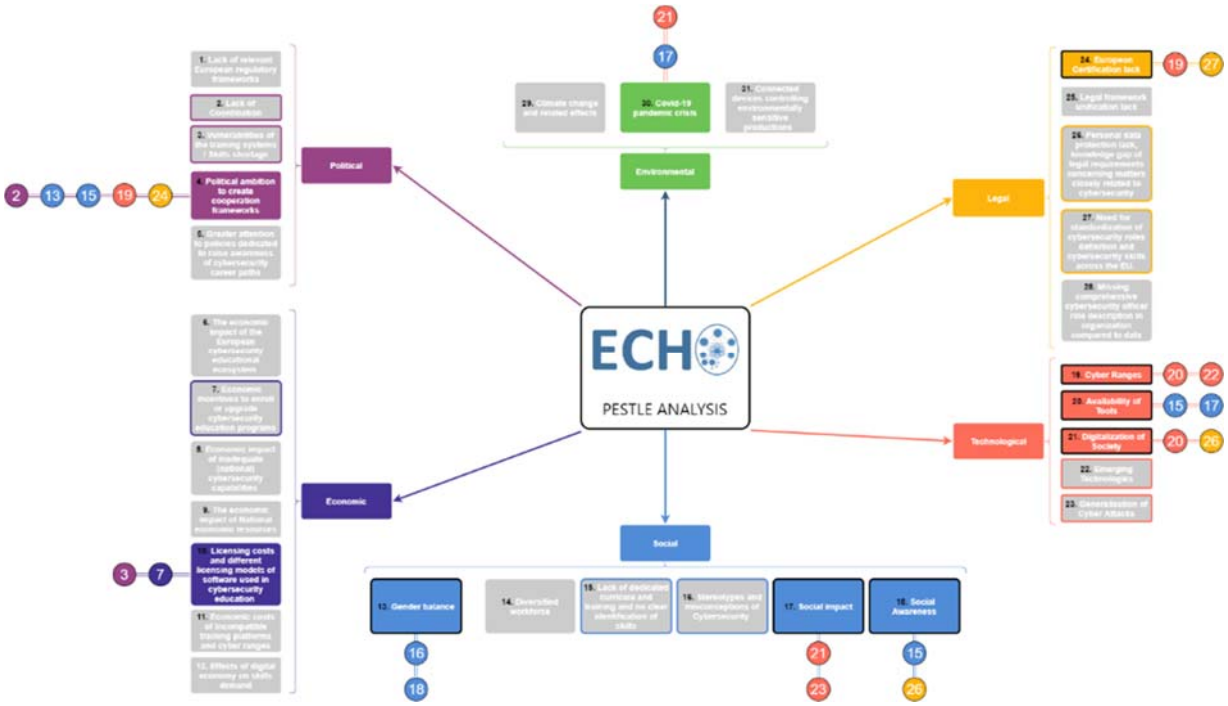

Figure 7. Mind-map representing aspects identified by REWIRE which were also identified by ECHO pilot project and their respective connection(s) to other aspects.

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	4. Political ambition to create cooperation frameworks	Medium	24. European Certification lack	ECHO observed a push in certification standards "Agreeing with the need for internal and external audits, one interviewee recommends that they are complemented by certification, e.g., ISO 27001 certification, which also increases the confidence in the network organization." These are important in internal and external audits in European level [1].
			13. Gender balance	In interviewees on governance aspect, the advantages to ensuring diversity of the cybersecurity workforce (women in leadership position) has been recognized [2].
			15. Lack of dedicated curricula and training and no clear identification of skills	In ECHO plan for a governance model, one of the milestones is the creation of "ECHO CyberSkills Framework" [1].
			2. Lack of coordination	In ECHO project the authors observed that on the European level there is a lack of coordination between governance and their needs [1], "Therefore, an additional

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				and complementary coordination instruments often need to be created" [2].
			19. Cyber Ranges	In ECHO plan for a governance model, one of the milestones is create a federated cyber range [1].
E	10. Licensing costs and different licensing models of software used in cybersecurity education	High	7. Economic incentives to enroll or upgrade cybersecurity education programs	"Older and unpatched Windows systems are particularly vulnerable because attackers do not need to exploit a zero-day vulnerability to successfully compromise them; they simply need to exploit known vulnerabilities that are publicly documented in open sourced databases." The main challenge is to acquire enough economic resources to upgrade programs to the latest versions, e.g., "Different versions of MS Windows undoubtedly dominate when it comes to operating systems used on personal computers and, although the latest version of this operating system, Windows 10, has exceeded 50% market share, older versions (such as Windows 7) are still in use and Microsoft directly recommends the transition to Windows 10; unfortunately, though, the process of free upgrades to the latest version of the system was completed in 2016, and therefore such a transition will require a substantial license fee" [3].
			3. Vulnerabilities of the training systems / Skills shortage	The updates of the training systems are important to avoid vulnerability and threat management. It is important to gather as much information as possible from different sources (OSINT, CLOSINT) [4]. If the systems are not properly updated the impact can be very dangerous [4].
S	18. Social Awareness	Medium	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	Society feels a lack of personal data protection and other sensitive or classified information. Most of the people refer to confidentiality as a crucial consideration for the proper functioning of a network organization in the field of cybersecurity [2].
			15. Lack of dedicated curricula and training and no clear identification of skills	ECHO intends to raise awareness of the need for cybersecurity amongst EU citizens and better-inform them of potential threats and best practices [1].
	17. Social impact	High	23. Generalization of cyber attacks	The ECHO project identifies the security risks in the increasing usage of the variety of devices in society. "The ever-expanding digitalization of all devices (i.e., smart watches, smart fridges, smart heart pacemakers), require real-time connection to a data network, which will be done massively through 5G, will again increase the exposure of virtually any person,

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				animal or thing on Earth to be cyber-attacked" [4].
			21. Digitalization of Society	Since the digitalization of society is increasing, and it seems foreseeable that the number of attacks will skyrocket as there is trend to massively connect any device to the Internet. Since the cyberattack has a high impact, it impacts also the society (e.g., hospitals, etc.) [4].
	13. Gender balance	Medium	18. Social Awareness	The gender balance is an important part of future research and fully functional education in cybersecurity. The gender balance usually increases the culture, stressing its impact on society. "Some CNOs made positive steps towards ensuring gender balance by establishing initiatives and charters to encourage and retain female personnel in the cyber-security domain. However, the primary analysis phase of these CNOs highlighted that the vast majority of networks did not make any significant contributions towards addressing gender balance. [2]".
			16. Stereotypes and misconceptions of Cybersecurity	In the terms of gender balance: "Just over half of the interviewees elaborate on this governance aspect, some clearly stating that this is “not a fundamental aspect; [we need to] put the merit in front of gender equality.” Others are content with adherence to “applicable EU policy.”. That approach usually decreases the effort in that area, however, some of the interviews in ECHO projects "emphasized the advantages in ensuring diversity of the cybersecurity workforce and gave examples in delivering courses, incl. e-learning courses, aimed at girls to contribute to skills’ objectives, as well as at having women in leadership positions." [2].
T	19. Cyber Ranges	Medium	22. Emerging Technologies	The ECHO project considers the important part of Cyber Range platform should be the Gamification in Cyber Ranges that requires the development of a new ways or technologies to support such an option [4].
			20. Availability of Tools	In cybersecurity education using cyber ranges it is especially important to improve the platform and other aspects of education supporting technology. The important part of this is the "Online survey tools that make it very easy to gather feedback. These are typically fast, efficient, and inexpensive. They automatically tabulate data and do not require a techie to launch." [4]

CYBERSECURITY SKILLS ALLIANCE
ON FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	20. Availability of Tools	Medium	15. Lack of dedicated curricula and training and no clear identification of skills	The increasing usage of collaboration tools and other online services that are nowadays widely used by society are increasing cybersecurity threats. For that reason, we see the lack in the society to provide a specialized trainings and other supports to decrease the attacker's opportunity to attack the users' devices [2].
			17. Social impact	The availability of tools has a high impact on society, people are widely using collaboration tools, online education platforms, and other systems. Using all these tools that are usually freely available is increasing the cybersecurity risks that the people are undertaking usually without any deeper knowledge [1].
	21. Digitalization of Society	High	20. Availability of Tools	Since society is increasingly using tools for communication channels the threats increase. This widely increases the cybersecurity risks that have to be undertaken when the digitalization of the society increases [5].
			26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	In the recent past, in the European union the General Data Protection Regulation (GDPR) was submitted. This was a way to the right directions in terms of personal data protection in the digitalized society, however, there is still missing a wider cybersecurity mechanism to increase the personal data protection on the internet, e.g., to protect the intellectual property (IP) [2].
L	24. European Certification lack	Medium	27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	The proposal in Regulation 630 (R630, 2018) is to establish: a Network of National Coordination Centres, a Cybersecurity Competence Community, a European Cybersecurity Industrial, Technology and Research Competence Centre. Further the roles and responsibilities are described in detail in [1]. Further, in terms of certification scheme The European CCC will adhere to Cybersecurity Act (CA, 2019) and will be grounded on the EU cyber security certification scheme to be developed by ENISA [2].
			19. Cyber Ranges	The ECHO projects quite widely elaborate on how to use Cyber Ranges to certificate products. "cyber ranges can be used by a wide range of target users: Corporates (private and government), Strategic decision makers (private and government), Security professionals, Military agencies and CNOs, Security Operations Centres(SOCs), Educators, Students, Researchers, Event organizers." With the respect to certification, the following

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				application area are envisaged: Conformity Assessment, and Building competence and security education [4].
E	30. Covid-19 pandemic crisis	Medium	21. Digitalization of Society	The Covid-19 pandemic crisis increases the usage of technologies that usually requires a real-time connection to a data network. This increases the exposure of virtually any person or thing on the Earth to be cyber-attacked. This situation significantly increases the importance of cybersecurity for the society [4].
			17. Social impact	Since the Covid-19 pandemic crise increases online interactions, it increases the attacker's ability to track the user's online interactions. This can have a wide negative impact on society since these data are usually processed further and can be used against us [3] [5].

[1] Márton Kis, D9.1 Project leaflets, March 2020 https://echonetwork.eu/wp-content/uploads/2020/02/ECHO_D9.1-Project-Leaflets-v1.0.pdf

[2] Todor Tagarev, D3.1 Governance needs and objectives, March 2020 https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D3.1-Governance-Needs-and-Objectives_v1.1.pdf

[3] Notis Mengidis, D4.1 Transversal technical cybsersecurity challenges report, March 2020 https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D4.1_Transversal-Technical-Cybersecurity-Challenges-Report_v1.0.pdf

[4] Peter Kirkov, D4.3 Inter-sector cybersecurity technology roadmap, March 2020 https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D4.3-INTER-SECTOR-CYBERSECURITY-TECHNOLOGY-ROADMAP-v1.0.pdf

[5] Marton Kis, D9.18 Communication collateral, social media channels set-up, March 2020 https://echonetwork.eu/wp-content/uploads/2020/02/ECHO_D9.18_Communication-collateral-social-media-channels-set-up_v1.1.pdf

Table 4. ECHO.

4.4. SPARTA

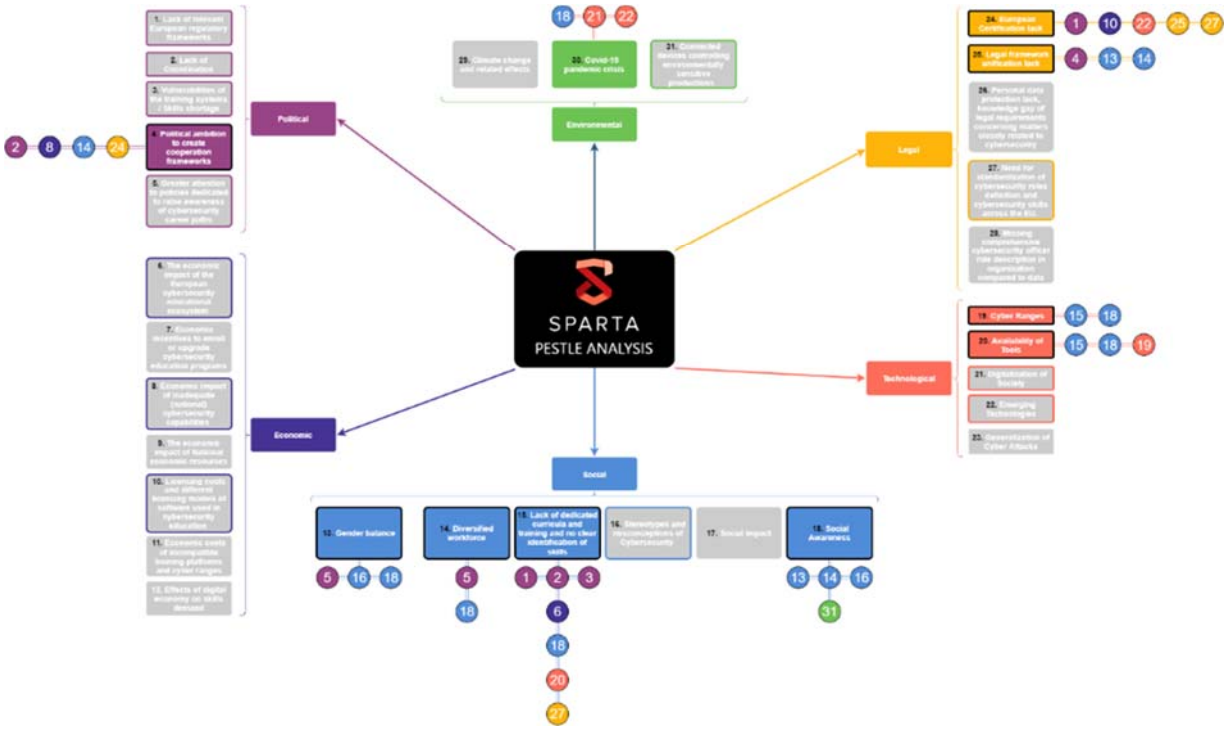

Figure 8. Mind-map representing aspects identified by REWIRE which were also identified by SPARTA pilot project and their respective connection(s) to other aspects.

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	4. Political ambition to create cooperation frameworks	High	2. Lack of coordination	SPARTA is part of the Cybersecurity Competence Network (CCN). It is designed to build efficient relationships across the European cybersecurity ecosystem [10]. However, there is no political and very little scientific guidance for determining the future role, scope, and focus of a European CCN [2].
			24. European Certification lack	Sparta observed a political push for introducing a scheme of IT security certification at European level [13].
			8. Economic impact of inadequate (national) cybersecurity capabilities	As SU-ICT-03-2018 call for proposal draws, SPARTA recognizes the "needs to do more in terms of investment and overcome the fragmentation of capacities spread across the EU". SPARTA is committed to demonstrate that a research governance can out-innovate Europe's competition [10].
			14. Diversified workforce	SPARTA embraces the European motto "united in diversity" and consider diversity as a SPARTA governance principle [10].
E	No identified aspects for Economic Factor			

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

S	15. Lack of dedicated curricula and training and no clear identification of skills	High	1. Lack of relevant european regulatory frameworks	"We find that currently, EU lacks a comprehensive cybersecurity skills framework, which would allow policymakers to gather actionable data on the existing and emerging skills gaps" [1].
			6. The economic impact of the European cybersecurity educational ecosystem	"The Education Web App serves as a way of visualizing data about existing cybersecurity study programs worldwide. It has been produced to provide easier and more user-friendly representation of research results to the general public" [2].
			27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	"The SPARTA CS Framework will serve as a common denominator for communication to the academia of the skills needed for a comprehensive cybersecurity approach that aims to develop curricula to respond to the needs of emerging threats." [1].
			20. Availability of Tools	"New methods of teaching and training, especially the hands-on training activities, need to be developed and tested" [3].
			2. Lack of coordination	"Individual academic and professional programs are already available at many universities and training institutions, but there is a lack of coordination and understanding, what courses and topics should be included in these programs so that they reflect the current trends on the job market" [1].
			3. Vulnerabilities of the training systems / Skills shortage	"One solution to this problem is to enhance cybersecurity education and training so that more experts in cybersecurity can fill in the vacancies [2]. "There is a lack of bachelor study programs focused on cybersecurity. In fact, among 89 cybersecurity curricula, only 19 bachelors had been found" [2].
			18. Social Awareness	During our research, we also observed that the security community is very altruistic, and several researchers publish online their findings" [2]. "Significant part of the content regarding cybersecurity education can be found online and quite often is described in blog posts, which makes it available to everyone independent of being enrolled in some academic program" [5].
	13. Gender balance	Medium	16. Stereotypes and misconceptions of Cybersecurity	During Gender & Diversity Breakfast Webinars event, several stereotypes and misconceptions related to gender issue have been discussed [4].
			5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Given the growing cybersecurity skills gap, it has never been more important for businesses to attract and maintain women in cybersecurity [4] [5] [6].
			18. Social Awareness	Campaigns for Diversity in cybersecurity: promote diversity practices and awareness on gender and diversity issues [4] [5] [6].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	14. Diversified workforce	Medium	18. Social - Social Awareness	Campaigns for Diversity in cybersecurity: promote diversity practices and awareness on gender and diversity issues [5] [6]. In particular, SPARTA focuses on European outermost regions with the "Go Cyber with SPARTA" campaign.
			5. Political - Greater attention to policies dedicated to raise awareness of cybersecurity career paths	" Task 12.4 and 12.5 – Closing the Gender and Diversity Gap and Engagement of the Outermost Regions of Europe" [6].
	18. Social Awareness	High	16. Stereotypes and misconceptions of Cybersecurity	"SPARTA goes to high school" campaign - One of the SPARTA cybersecurity awareness goals are to trigger students' curiosity to pursue their studies on the field of cybersecurity [5,6].
			31. Connected devices controlling environmentally sensitive productions	Engage with critical infrastructure operators to stimulate them to adopt state-of-the-art cybersecurity technology [5,6].
			13. Gender balance	"SPARTA goes to high school" campaign - Raise awareness on the importance of cybersecurity and on the need for a diverse workforce on cybersecurity [6].
			14. Diversified workforce	"Go Cyber with SPARTA" campaign - Engagement of the Outermost Regions of Europe and encouragement to adopt cybersecurity measures [5,6].
T	19. Cyber Ranges	High	18. Social Awareness	Cyber-attacks require an increase cyber security awareness in public and development of security skills for security professionals [7]. Cyber ranges training can help with this issue.
			15. Lack of dedicated curricula and training and no clear identification of skills	Following Enisa recommendation: more training offerings need to be developed, in particular, the current market needs in cyber threat intelligence training [7]. Cyber ranges training can help with this issue.
	20. Availability of Tools	Medium	19. Cyber Ranges	Cyber Security Training Platform – cyber ranges will be part of this platform [7].
			15. Lack of dedicated curricula and training and no clear identification of skills	Cyber Security Training Platform - Enhancement of the educational offering since much more training offerings need to be developed [7].
			18. Social Awareness	Cyber Security Training Platform - cyber-security training of digital natives, security awareness of key stakeholders such as educators and parents, young talent identification and recruitment [7].
L	24. European Certification lack	High	10. Licensing costs and different licensing models of software used in cybersecurity education	Licensed laboratories and certified software are important for creating a unified base for education [8].
			25. Legal framework unification lack	"International and national cybersecurity certification initiatives" - Europe lacks behind in the development of a comprehensive

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				approach to define a set of roles and skills relevant to the cybersecurity field [8,9].
			22. Emerging Technologies	"Cybersecurity certification is one way to help engineers design more secure systems." Moreover, "Artificial intelligence can be used by to attack and to protect systems from attack" [3].
			1. Lack of relevant European regulatory frameworks	NIST CSF Framework aims to provide a common and accessible language for dealing with cybersecurity risk [8].
			27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	Identification of commonalities and differences between national cybersecurity certification initiatives and recommendations for convergence at European Level [10].
	25. Legal framework unification lack	Medium	4. Political ambition to create cooperation frameworks	There is a lack of precision, starting with the "legal" definition of cybersecurity [14], and ethical, legal, and societal aspects (ELSA) are important components of governance [15].
			13. Gender balance	ELSA mechanisms and activities should provide coverage for gender and diversity dimension [15].
			14. Diversified workforce	ELSA mechanisms and activities should provide coverage for gender and diversity dimension [15].
E	30. Covid-19 pandemic crisis	Medium	22. Emerging Technologies	The COVID-19 pandemic pushes the need to find ICT solutions to slow down the virus spreading using people tracing solutions. These tracing solutions can alert the people that they meet someone infected and to take proper action. Regarding the cybersecurity area the main topics are touching the privacy-aware contact tracing and its (dis)advantages [12].
			21. Digitalization of Society	The outbreak of the covid-19 pandemic impacts the sudden switching to working, communicating, learning, etc. online. That requires the availability of suitable collaborative tools to provide education in general. During the COVID-19 pandemic 73% of employers helped employees with the transition to online working [11].
			18. Social Awareness	The level of digital competence increased during the COVID-19 pandemic, that was reported by 61% of respondents. Meanwhile, only 26% of respondents reported that their cybersecurity awareness increased since the beginning of the COVID-19 pandemic (during the pandemic there were a sharp increase in cyber-attacks) [11].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

[1] Edmundas Piesarskas, D9.1 Cybersecurity skills framework, January 2020, https://www.sparta.eu/deliverables/

[2] Jan Hajný, D9.2 Curricula descriptions, January 2020, https://www.sparta.eu/deliverables/

[3] Sergej Proskurin, D3.1 Initial SPARTA SRIA (Roadmap v0.1), July 2019,https://www.sparta.eu/deliverables//

[4] Gender & Diversity Breakfast Webinars, https://www.sparta.eu/news/2020-09-03-gender-diversity-breakfast-webinars.html

[5] Catarina Valente, D12.1 Dissemination and communication plan, updates, and evaluation, April 2019, https://www.sparta.eu/deliverables/

[6] Catarina Valente, D12.3 Updated dissemination and communication plan and evaluation – v1, January 2020, https://www.sparta.eu/deliverables/

[7] Algimantas Venčkauskas, D9.4 – Pilot of Cyber training & exercise Framework, in progress, https://www.sparta.eu/deliverables/

[8] Jeremy Grandclaudon, D11.1 International and national cybersecurity certification initiatives, January 2020, https://www.sparta.eu/deliverables/

[9] Volkmar Lotz, D11.2 Cybersecurity compliant development processes, July 2020, https://www.sparta.eu/deliverables/

[10] Florent Kirchner, D1.1 Bootstrapping a CCN Pilot, February 2020 https://www.sparta.eu/deliverables/

[11] Aleksandra Pawlicka, PhD, Digital Literacy and Cybersecurity Awareness During the COVID-19 pandemic https://sparta.eu/demos/digital-literacy-and-cybersecurity-awareness-during-the-covid-19-pandemic.html

[12] Qiang Tang, Privacy-Preserving Contact Tracing: current solutions and open questions, https://sparta.eu/papers/privacy-preserving-contact-tracing-current-solutions-and-open-questions-1.html

[13] Dirk Kuhlmann, D1.2 Lessons learned from internally assessing a CCN pilot, January 2020, https://www.sparta.eu/deliverables/

[14] Manon Knockaert, D2.1: Ethical legal and societal aspects, January 2019, https://www.sparta.eu/deliverables/

[15] Gonçalo Cadete, D2.2 First internal ELSA audit and supervision report, January 2020, https://www.sparta.eu/deliverables/

Table 5. SPARTA.

4.5. Summary

This chapter contains the questionnaire results of each pilot project, namely Concordia, CyberSec4Europe, ECHO and SPARTA. During their lifetime, each project had already identified many skills shortages, gaps and mismatches that can affect cybersecurity education. The purpose is to show which aspects were already identified by pilot projects since REWIRE is based on input from these projects. Moreover, these pilots' outcomes can be viewed as a rough European PESTLE analysis.
Identified aspects are shown along with their linkages to other aspects. References to pilots' documents are given in the sections above.

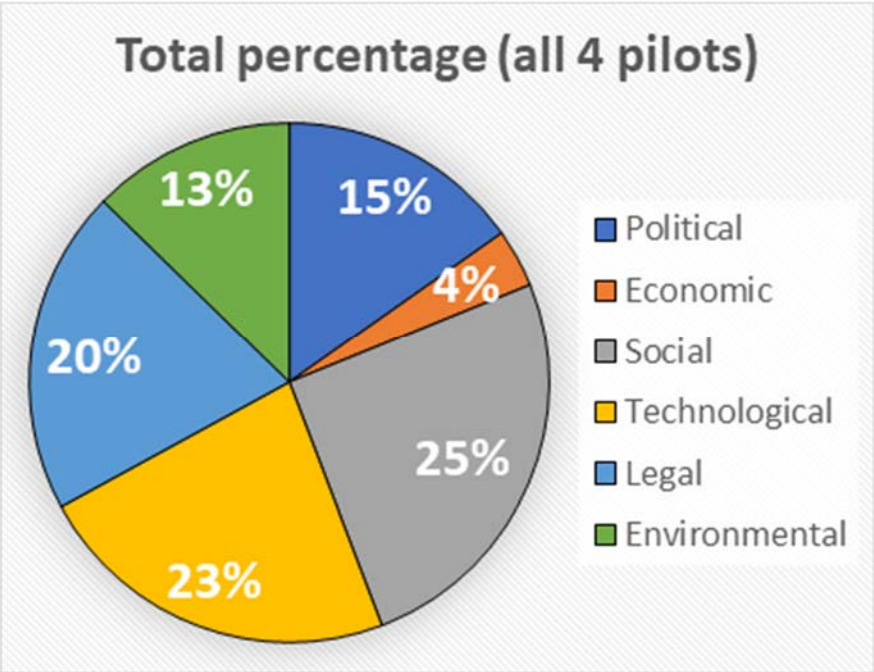

Figure 9. Total average percentages of PESTLE analysis of all four pilots identified and linked also by REWIRE.

Figure 9 depicts the overall percentage of identified aspects per factor. This figure shows that pilots focused particularly on Social aspects which have the highest percentage, i.e., 25%, among them. This result is biased by the SPARTA project result where only 4 social aspects out of 6 were mentioned.
The Technological factor follows with 23%. Concordia, CyberSec4Europe and ECHO projects are strongly focused on this factor with 3 aspects identified out of 5 while SPARTA project has 2.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

5. STATISTICAL ANALYSIS OF QUESTIONNAIRE

In order to develop a sectoral skills strategy, the current status quo of skills shortages, gaps and mismatches needs to be analyzed. This strategy can also support the growth strategy of the cybersecurity industry.

In this chapter, we summarize the results on the collected data from the 11 European countries questionnaires (see Chapter 2 for details on the collection strategy). It is remarkable that each country has already identified many skills shortages, gaps and mismatches which can have impact not only on a National level but also on the European level. In Annexes you can find the filled National questionnaires.

5.1. Analysis

During the questionnaire filling in, each partner provides referenced linkages between the identified aspects. This connection helps to reveal the aspects mutual dependency, i.e., how they can affect each other. It is important to notice that the linkages are the main objective of this analysis.

Political			
Aspects	**Number of connections**	**Importance of the aspect**	**Country**
1. Lack of relevant European regulatory frameworks	12	Medium	Austria, Cyprus, Czech Republic, Spain, Sweden
2. Lack of coordination	13	Medium	Austria, Greece, Hungary, Serbia
3. Vulnerabilities of the training systems / Skills shortage	11	Medium	Austria, Greece, Czech Republic, Portugal, Hungary, Serbia, Sweden
4. Political ambition to create cooperation frameworks	3	High	Portugal, Serbia
5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	5	Medium	Austria, Serbia
Political connections in total	44		

Table 6. Identified Political aspects with number of connections and their importance.

Table 6, Table 7, Table 8, Table 9, Table 10, Table 11 show (1) the identified PESTLE aspects on a National level, (2) the number of referenced connections found with the other aspects, (3) importance of each aspect, and (4) the list of countries which identify at least one of these connections. Each table contains a specific PESTLE factor summary. For instance, Table 6. Identified Political aspects with number of connections and their importance. depicts political aspects. Moreover, aspects with more than 10 connections are highlighted in gray. The aspect

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

that reveals more dependency is "31. Connected devices controlling environmentally sensitive productions" with its 14 connections as shown in Table 11. Identified Environmental aspects with number of connections and their importance.. This aspect can be considered the main issue recognized in the analysis. Of interest are also "2. Lack of coordination" and "26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity" which count 13 connections.

Economic			
Aspects	**Number of connections**	**Importance of the aspect**	**Country**
6. Economic impact of the European cybersecurity educational ecosystem	3	Medium	Hungary, Serbia
7. Economic incentives to enroll or upgrade cybersecurity education programs	7	Medium	Austria, Serbia
8. Economic impact of inadequate (national) cybersecurity capabilities	6	High	Cyprus, Greece
9. Economic impact of National economic resources	1	High	Lithuania
10. Licensing costs and different licensing models of software used in cybersecurity education	3	Medium	Serbia, Sweden
11. Economic costs of incompatible training platforms and cyber ranges	1	Medium	Sweden
12. Effects of digital economy on skills demand	4	Medium	Serbia, Sweden
Economic connections in total	25		

Table 7. This table shows the list of identified Economic aspects, their importance, the number of their connections with other aspects, and which countries recognize each aspect as relevant.

We can see the number of connections of each PESTLE factor checking the last row of each table. In particular, Political factor counts the greatest number of connections, strictly followed by Social, Technological and Legal factors, while Economic and Environmental factors present the cases with least connections. This count gives a rough idea of which factor would require a deeper analysis in the future and a bigger effort to be resolved during the lifetime of the project. Indeed, a lack of cybersecurity governance can be deducted from Table 6. Identified Political aspects with number of connections and their importance.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Social			
Aspects	**Number of connections**	**Importance of the aspect**	**Country**
13. Gender balance	6	Medium	Portugal, Hungary, Serbia, Spain, Sweden
15. Lack of dedicated curricula and training and no clear identification of skills	10	Medium	Austria, Lithuania, Czech Republic, Portugal, Spain
16. Stereotypes and misconceptions of Cybersecurity	6	Medium	Austria, Cyprus
17. Social impact	6	Medium	Austria, Cyprus, Portugal
18. Social Awareness	12	High	Lithuania, Cyprus, Greece, Portugal, Hungary, Serbia,
Social connections in total	40		

Table 8. Identified Social Aspects with number of connections and their importance.

It is important to notice that if an aspect is not mentioned in Column 1, it is not equivalent to no connection being identified with it. For example, "14. Diversified workforce" is not mentioned in Table 8. Identified Social Aspects with number of connections and their importance.. However, the Legal aspect "27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU" has been linked to the social aspect "14. Diversified workforce" in the Czech Republic questionnaire (see Annex ...). The meaning of this situation is that Aspect 27 is of main importance, and Aspect 14 is only mentioned as a secondary issue in the Czech document.

Technological			
Aspects	**Number of connections**	**Importance of the aspect**	**Country**
19. Cyber Ranges	7	Medium	Czech Republic, Greece, Portugal, Hungary, Serbia, Spain
20. Availability of Tools	6	Medium	Czech Republic, Hungary, Spain, Sweden
21. Digitalization of Society	6	Medium	Austria, Czech Republic, Hungary, Spain
22. Emerging Technologies	9	High	Czech Republic, Greece, Portugal, Sweden
23. Generalization of cyber attack	12	High	Austria, Cyprus
Technological connections in total	40		

Table 9. Identified Technological aspects with number of connections and their importance.

Note that the Legal aspect "24. European Certification lack" was identified by the biggest number of countries. Therefore, it is of relevance even if it affects less aspects with respect to others, i.e., it has less connections. Column 3 of each table shows the importance assigned on average to the specific identified aspect. We can see that columns "Number of Connections" and "Importance of Aspect" look proportionally related. In most cases, a big

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

number of connections is associated to greater importance. However, as shown in Table 11. Identified Environmental aspects with number of connections and their importance. aspect "30. Covid-19 pandemic crisis" has only 7 connections but high importance. This is due to the fact that the covid-19 pandemic is a new issue that appeared during the projects' lifetime only recently.

Legal			
Aspects	**Number of connections**	**Importance of the aspect**	**Country**
24. European Certification lack	10	Medium	Austria, Lithuania, Czech Republic, Serbia, Spain, Sweden
25. Legal framework unification lack	5	Medium	Austria, Greece, Sweden
26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	14	Medium	Lithuania, Cyprus, Czech Republic, Greece, Portugal, Hungary, Spain
27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	10	High	Cyprus, Czech Republic, Greece
Legal connections in total	39		

Table 10. Identified Legal aspects with number of connections and their importance.

Figure 10 depicts the percentage of identified PESTLE factors per country. These charts differ substantially depending on the country. For instance, Austria and Serbia give bigger attention to Legal aspects, while Czech Republic, Hungary and Spain to Technological ones. The country's main interest and political directions can bias the results.

Environmental			
Aspects	**Number of connections**	**Importance of the aspect**	**Country**
30. Covid-19 pandemic crisis	7	High	Cyprus, Greece, Hungary, Spain
31. Connected devices controlling environmentally sensitive productions	14	High	Austria, Cyprus
Environmental connections in total	21		

Table 11. Identified Environmental aspects with number of connections and their importance.

Figure 11 shows the average percentage for all countries of identified PESTLE factors. Technological aspects are the ones mentioned most with a 22%. However, the related percentages among factors do not differ substantially.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

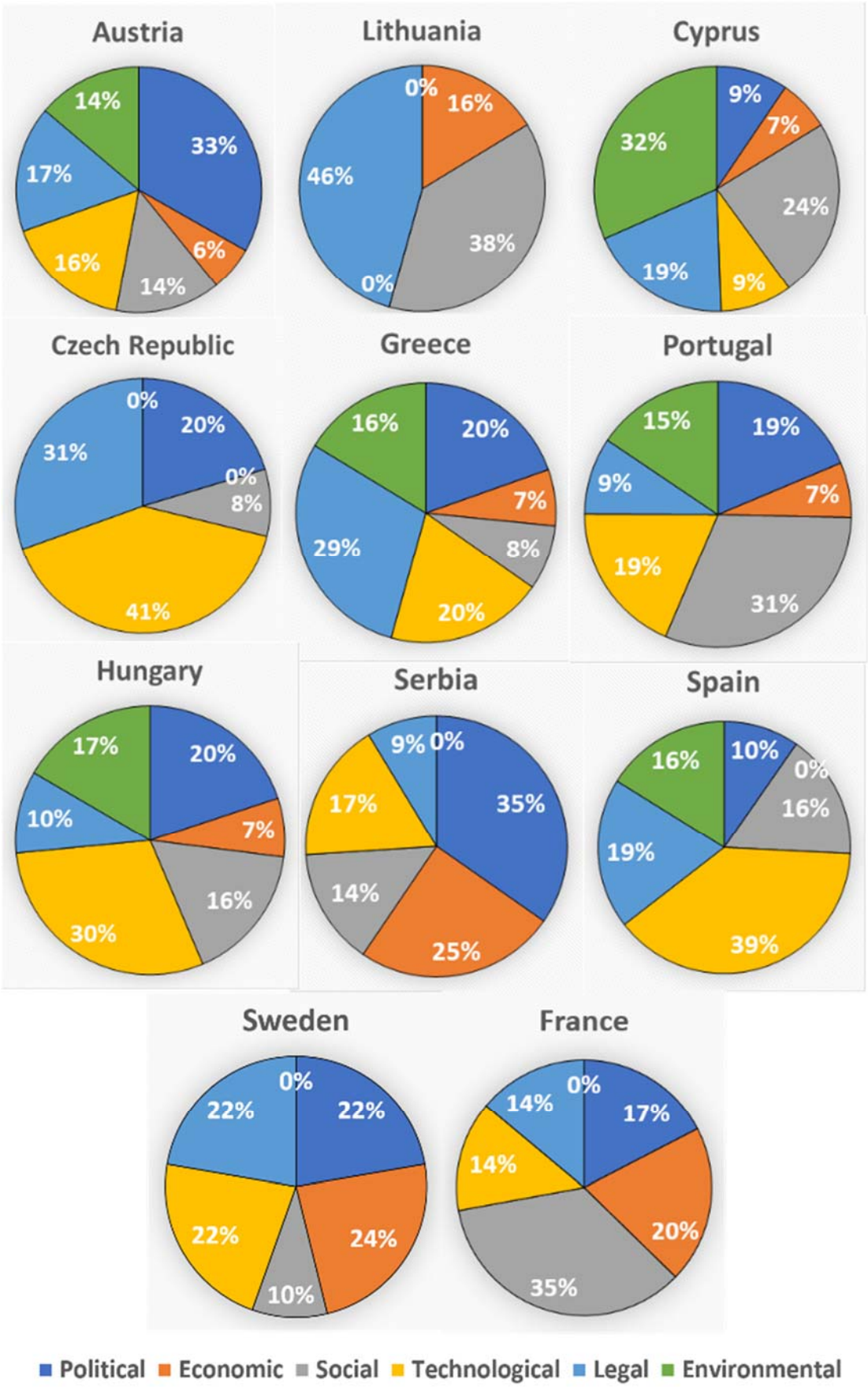

Figure 10. Identified PESTLE factors' percentages given per country.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

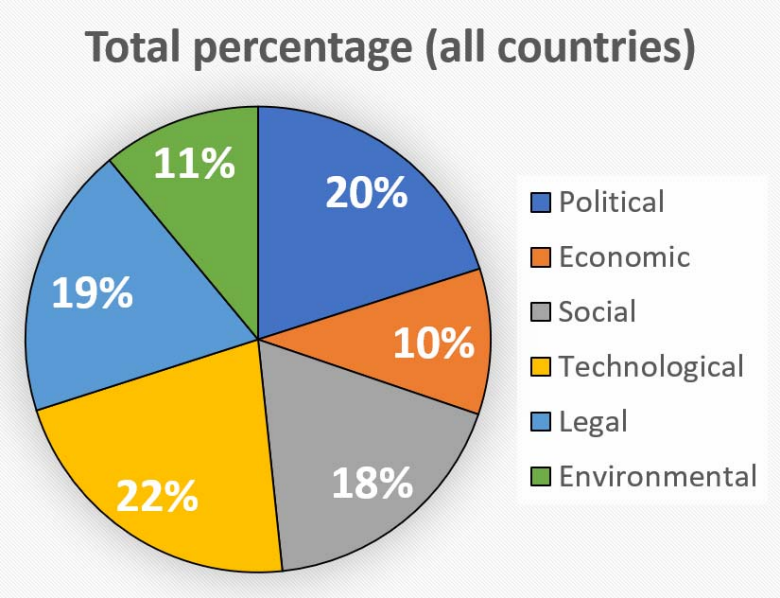

Figure 11. Average of identified PESTLE analysis percentages for all countries

5.2. Summary

The collected 11 European countries' questionnaires results give an initial overview of the identified skills shortages, gaps and mismatches currently affecting cybersecurity education. The analysis by PESTLE factors permits to have a view of the whole cybersecurity education environment from different angles.

In average the PESTLE factors were equally identified. However, differences in importance and identification can be found depending on the country.

It is remarkable that a lack of cybersecurity governance can be deduced due to the greatest number of connections of the Political Factor. This count gives a rough idea of which factor would require a deeper analysis in the future and a bigger effort to be resolved during the lifetime of the project.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

6. SUMMARY AND CONCLUSIONS

The main objective of this report was to present a Political, Economic, Social, Technological, Legal, and Environmental (PESTLE) analysis of the skills shortages, gaps, and mismatches affecting cybersecurity education.

Based on the methodology designed and implemented by the REWIRE project, the following steps were implemented sequentially:

- A basic analysis was conducted for each of the 6 characteristics of the PESTLE analysis, revealing 31 different aspects affecting the subject of cybersecurity education and skills.
- A second level of analysis involved the identification of the interconnections between different aspects. In average the PESTLE factors were equally identified. However, differences in importance and identification can be found depending on the country. Moreover, this analysis revealed that the identified aspects are intrinsically correlated.
- A third level of analysis is related to the identification of aspects of the 4 pilot projects, since REWIRE will be based also on the input of these projects. The results of this analysis revealed that the pilot projects also identified all factors with an emphasis on the Social and the Technological factors.
- As a last step, all gathered information was consolidated. Weighed and a prioritized list of aspects was derived.

It is remarkable that a governance shortage, i.e., a lack of European coordination and cooperation is strongly identified by all pilots' projects and countries surveys.

This report gives a first overview of which factor would require a deeper analysis in the future and a bigger effort to be resolved during the lifetime of the project.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

7. REFERENCES

[1] 2013 21st Telecommunications Forum (TELFOR). November 2013.
[2] Adversarial ML Threat Matrix. 2020. url: https://github.com/mitre/advmlthreatmatrix).
[3] Alexandros Papanikolaou et al. "A survey of cyber crime in Greece". In: Telfor Journal 6.2 (2014), pp. 86–91. issn: 1821-3251. doi: 10.5937/telfor1402086P. url: http://scindeks. ceon.rs/Article.aspx?artid=1821-32511402086P.
[4] Alexandros Papanikolaou et al. "Cyber crime in Greece. How bad is it?" In: 2013 21st Telecommunications Forum Telfor (TELFOR) (2013), pp. 1–4. doi: 10.1109/TELFOR.2013.6716156. url: http://ieeexplore.ieee.org/document/6716156/.
[5] Alexia Elejalde-Ruiz. Manufacturing's big challenge: Finding skilled and interested workers. 17 December 2016. url: https : / / www . chicagotribune . com / business / ct - manufacturing - talent-gap-1218-biz-20161217-story.html.
[6] Anastasios Papathanasiou et al. "Legal and Social Aspects of Cyber Crime in Greece". In: E-Democracy, Security, Privacy and Trust in a Digital World (2014), pp. 153–164. doi: 10.1007/978- 3- 319- 11710- 2_14. url: http://link.springer.com/10.1007/978- 3- 319- 11710-2_14.
[7] Article 5.1 d). Principles relating to processing of personal data. Brussel, 2018. url: https : //gdpr-info.eu/art-5-gdpr/.
[8] Cidadão Ciberseguro (Cybersecure Citizen). Portugal, February 2020. url: https://www.nau. edu.pt/curso/cidadao-ciberseguro/.
[9] Coronavirus. url: https://www.who.int/healthtopics/coronavirus\#tab=tab_1.
[10] Cybersecurity awareness. San Francisco (CA), 2001-. url: https://en.wikipedia.org/wiki/ Cyber_security_awareness.
[11] Cybersecurity Education. Attiki, Greece, 2020. url: https://www.enisa.europa.eu/topics/ cybersecurity-education.
[12] Cybersecurity Professionals Stand Up to a Pandemic. (ISC)2 CYBERSECURITY WORKFORCE STUDY, In: Isc2 2020, pp. 1–43. url: https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en\&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B.
[13] Cybersecurity Skills Development in the EU. Attiki, Greece, 2019. url: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[14] Cybersecurity Skills Development in the EU. The certification of cybersecurity degrees and ENISA's Higher Education Database. In: ENISA. EU, 2019. url: https://www. enisa.europa.eu/publications/the- status- of- cyber- security- education- in- the-european-union.
[15] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels/Belgium, 2013. url: https://data.consilium.europa.eu/doc/document/ST\%206225\%202013\%20INIT/EN/pdf.
[16] D. Katsianis et al. "Factors Influencing Market Adoption and Evolution of NFV/SDN Cybersecurity Solutions. Evidence from SHIELD Project". In: 2018 European Conference

on Networks and Communications (EuCNC) (2018), pp. 1–5. doi: 10 . 1109 / EuCNC . 2018 . 8442845. url: https://ieeexplore.ieee.org/document/8442845/.

[17] Damian Heath and Ludwig Micallef. What is digital economy? url: https://www2.deloitte. com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html.

[18] Dan Lohrmann. 2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic. 19 December 2020. url: https : / / www . govtech . com / blogs / lohrmann - on - cybersecurity / 2020 - the - year-the-covid-19-crisis-brought-a-cyber-pandemic.html.

[19] Daniel Conte de Leon et al. "ADLES. Specifying, deploying, and sharing hands-on cyber-exercises". In: 74 (2018), pp. 12–40. issn: 01674048. doi: 10 . 1016 / j . cose . 2017 . 12 . 007. url: https://linkinghub.elsevier.com/retrieve/pii/S0167404817302742.

[20] Daniel Conte de Leon et al. "Tutorials and laboratory for hands-on OS cybersecurity instruction". In: 2018.34 (), pp. 242–254.

[21] Danita Baghdasarin. "MRO Cybersecurity SWOT". In: International Journal of Aviation, Aeronautics, and Aerospace (2019), *6*(1). url: https://doi.org/10.15394/ijaaa.2019.1318

[22] Darren Thomson. "Cybersecurity skills gap: An industry in crisis or something even worse?" In: Itproportal 2019 (). url: https://www.itproportal.com/features/an-industry- in-crisis-symantec-cto-darren-thomson-on-tackling-the-critical-skills-gap/.

[23] Data Protection Officer (DPO). url: https:/ /edps.europa. eu/data- protection/ data-protection/reference-library/data-protection-officer-dpo_en.

[24] David P. Fidler. "Final Acts of the World Conference on International Telecommunications". In: International Legal Materials 52.3 (2013), pp. 843–860. issn: 0020-7829. doi: 10 . 5305 / intelegamate.52.3.0843. url: https://www.cambridge.org/core/product/identifier/ S0020782900001418/type/journal_article.

[25] Digital Education Action Plan (2021-2027). Brussels / Belgium, 2020. url: https : / / ec . europa.eu/education/education-in-the-eu/digital-education-action-plan_en.

[26] Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert. "The new EU cybersecurity framework. The NIS Directive, ENISA's role and the General Data Protection Regulation". In: 35.6 (2019). issn: 02673649. doi: 10.1016/j.clsr.2019.06.007. url: https://linkinghub. elsevier.com/retrieve/pii/S0267364919300512.

[27] Dipankar Dasgupta, Zahid Akhtar, and Sajib Sen. "Machine learning in cybersecurity. a comprehensive survey". In: The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology (). issn: 1548-5129. doi: 10.1177/1548512920951275. url: http://journals. sagepub.com/doi/10.1177/1548512920951275.

[28] Domenico Orlando and Pierre Dewitte. "The 'by Design' Turn in EU Cybersecurity Law. Emergence, Challenges and Ways Forward". In: Security and Law (2020-01-23), pp. 239–252. doi: 10. 1017/9781780688909.010. url: https://www.cambridge.org/core/product/identifier/ CBO9781780688909A076/type/book_part.

[29] ECSO WG5. "Gaps in European Cyber Education and Professional Training. WG5I Education, training, awareness, cyber ranges". In: pp. 1–16.. url: https : //www.ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf.

[30] ECSO WG5. "Understanding Cyber Ranges: From Hype to Reality. SWG 5.1 I Cyber Range Environments and Technical Exercises". In: pp. 1–31. url: https://ecs-org.eu/documents/ publications/5fdb291cdf5e7.pdf.

[31] Edlyn V. Levine and Algirde Pipikaite. Hardware is a cybersecurity risk. Here's what we need to know. 19 December 2019. url: https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/.

[32] Elochukwu Ukwandu et al. "A Review of Cyber-Ranges and Test-Beds. Current and Future Trends". In: Sensors 20.24 (2020). issn: 1424-8220. doi: 10 . 3390 / s20247148. url: https : //www.mdpi.com/1424-8220/20/24/7148.

[33] ENISA programming document 2019-2021. Including multiannual planning, work programme 2019 and multiannual staff planning MB decision number MB/2018/20. In: ENISA. Vol. 2018. ENISA, 2018, pp. 1–95. isbn: 978-92-9204-269-1. doi: 10 .2824 /97038. url: https :/ /www . enisa.europa.eu/publications/corporate- documents/enisa-programming- document-2019-2021.

[34] ENISA Threat Landscape - 2020. EU, April 2020. url: https : / / www . enisa . europa . eu / topics/threat-risk-management/threats-and-trends.

[35] ENISA Women in Cybersecurity Brochure. In: (2019). url: https://www.enisa.europa.eu/news/enisa-news/women-in-cybersecurity-1.

[36] ENISA. "ENISA Threat Landscape 2020 - Phishing". In: (), pp. 1–24. url: https : / / www . enisa.europa.eu/publications/phishing.

[37] Ernst and Young. Cybersecurity incident simulation exercises - EY. 2017. url: https : / / pdf4pro.com/view/cybersecurity-incident-simulation-exercises-ey-2d8a.html.

[38] Essential measures for a healthy network. ANSSI - 51, boulevard de la Tour-Maubourg, January 2013. url: https://www.ssi.gouv.fr/uploads/2013/01/guide_hygiene_v1-2-1_en.pdf.

[39] Ethics Guidelines for Trustworthy AI. In: Europien Commission: HIGH-LEVEL EXPERT GROUP ONARTIFICIAL INTELLIGENCE (April 2019), pp. 1–41. url: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

[40] European Commision. The EU cybersecurity certification framework. EU, September 2017. url: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

[41] European Commission: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Brussel, 2017.

[42] European Cyber Security Organisation. Gaps in European Cyber Education and Professional Training. 2018.

[43] European Cybersecurity Skills Framework. Cybersecurity Education. Attiki, Greece, 2020. url: https : / / www . enisa . europa . eu / topics / cybersecurity - education / european - cybersecurity-skills-framework.

[44] Evropský rámec certifikace kybernetické bezpečnosti. European framework for cyber security cer-tification. url: https : / / www . nukib . cz / download / publikace / vyzkum / Evropsky_ramec_certifikace_kyberneticke_bezpecnosti.pdf.

[45] Fabio Di Franco. "Analysis of the European R&D priorities in cybersecurity. Strategic priorities in cybersecurity for a safer Europe". In: (December 2018). doi: 10.2824/14357. url: https: //www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity.

[46] Hans de Bruijn and Marijn Janssen. "Building Cybersecurity Awareness. The need for evidence-based framing strategies". In: Government Information Quarterly 34.1 (2017), pp. 1–7. issn: 0740624X. doi: 10.1016/j.giq.2017.02.007. url: https://linkinghub.elsevier.com/ retrieve/pii/S0740624X17300540.

[47] Harry Patrinos. "Trends in returns to schooling. why governments should invest more in people's skills". vol. 1. 2017-05-11, pp. 261–263. doi: 10.12681/elrie.792. url: http://eproceedings.epublishing.ekt.gr/index.php/inoek/article/view/792.
[48] Harry Patrinos. Why education matters for economic development. 2016. url: https://blogs. worldbank.org/education/why-education-matters-economic-development.
[49] Human-Computer Interaction Institute, School of Computer Science, Carnegie Mellon University. url: https://socialcybersecurity.org/.
[50] Initial National Cyber Security Skills Strategy. INCREASING THE UK'S CYBER SECURITY CA-PABILITY". In: 2019 (). url: https://assets.publishing.service.gov.uk/government/uploads / system / uploads / attachment_data / file / 949211 / Cyber_security_skills_strategy_211218_V2.pdf.
[51] Internal Displacement Monitoring Centre. Global Report on Internal displacement. 2020. url: https : / / www . internal - displacement . org / sites / default / files / publications / documents/2020\%20Mid-year\%20update.pdf.
[52] IPACSO. "Privacy and Cyber Security Industry Market analysis". url: https://ipacso.eu/about/project-ipasco/objectives/market-analysis.html
[53] ISACA: State of Cybersecurity 2019 Part 1: Current Trends in Workforce Development. In: Isaca.org 2019 (2019), pp. 1–40.
[54] Jason Reed and Jonathan Acosta-Rubio. "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce. An (ISC)2 Global Information Security Workforce Study". In: (2018).url: https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx.
[55] Jeff Styles. The unseen COVID-19 ripple effect: Security misconfiguration risk. If eliminating
[56] Joint communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade. Brussels / Belgium, 2020. url: https : / / eur - lex . europa . eu / legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018\&from=EN.
[57] Jon Davis and Shane Magrath. "A survey of cyber ranges and testbeds". In: (2013).
[58] Katharine D'Hont. "Women in Cybersecurity". In: (2016). url: https://wappp.hks.harvard. edu/files/wappp/files/dhondt_pae.pdf.
[59] Kathleen M. Carley. "Social cybersecurity. an emerging science". In: Computational and Mathematical Organization Theory 26.4 (2020), pp. 365–381. issn: 1381-298X. doi: 10.1007/s10588-020-09322-9. url: http://link.springer.com/10.1007/s10588-020-09322-9.
[60] Makki Marseilles. In Greece, Major Universities Suspend Operations Due to Budget Cuts. 2013. url: https://www.chronicle.com/article/in-_greece-_major-_universities-suspend-operations-due-to-budget-cuts/.
[61] Mark Knickrehm, Bruno Berthon, and Paul Daugherty. "Digital disruption: The growth multiplier". In: Accenture 2016 (), pp. 1–12. url: https://www.accenture.com/_acnmedia/pdf-14/accenture-strategy-digital-disruption-growth-multiplier-brazil.pdf.
[62] Migration Data Portal: The bigger picture. 27 October 2020. url: https : / / migrationdataportal.org/themes/environmental_migration.

[63] misconfiguration risk is the question, automation is the answer. 2020. url: https : / / www . securityinfowatch . com / covid - 19 / article / 21137323 / the - unseen - covid19 - ripple - effect-security-misconfiguration-risk.
[64] Omar Abbosh and Kelly Bissell. Securing the Digital Economy. Reinventing the Internet for Trust. 2019. url: https://www.accenture.com/ acnmedia/Thought- Leadership-Assets/ PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust. pdf.
[65] Peter James Fischer. "A Cybersecurity Skills Framework". In: Cybersecurity Education for Awareness and Compliance. IGI Global, 2019, pp. 202–221. isbn: 9781522578475. doi: 10.4018/978- 1- 5225- 7847- 5.ch011. url: http://services.igi-global.com/resolvedoi/ resolve.aspx?doi=10.4018/978-1-5225-7847-5.ch011.
[66] POSITION PAPER: Gaps in European Cyber Education and Professional Training. WG5 I Education, training, awareness, cyber ranges. Brussels / Belgium, 2020. url: https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf.
[67] Post-Quantum Cryptography PQC. Gaithersburg US, 2021. url: https : / / csrc . nist . gov / Projects/post- quantum- cryptography/post- quantum- cryptography-standardization/ Call-for-Proposals.
[68] QEMU. the FAST! processor emulator. url: www.qemu.org.
[69] Recitals 75-77 and Articles 24.1 and 32 of the GDPR. Brussel, 2018. url: https : / / www. privacy-regulation.eu/en/article-24-responsibility-of-the-controller-GDPR.htm.
[70] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019. 2019.
[71] Rick Burke et al. The smart factory. 31 August 2017. url: https://www2.deloitte.com/us/ en/insights/focus/industry-4-0/smart-factory-connected-manufacturing.html.
[72] Rigissa Megalokonomou. How the economic crisis is affecting higher education in Greece. url: https://www.weforum.org/agenda/2015/08/how- the- economic- crisis- is-affecting-higher-education-in-greece/.
[73] Rootme. Hacking and Information Security learning platform. 2021. url: https://www.rootme.org/.
[74] Sarantis Michalopoulos. Greece on the brink of 'education tragedy'. 2016. url: https://www. euractiv.com/section/social-europe-jobs/news/greece-on-the-brink-of-education-tragedy/.
[75] Sharmistha Bagchi-Sen et al. "Women in Cybersecurity. A Study of Career Advancement". In: IT Professional 12.1 (2010), pp. 24–31. issn: 1520-9202. doi: 10.1109/MITP.2010.39. url: http://ieeexplore.ieee.org/document/5403174/.
[76] Social Cybersecurity Working Group. url: SocialCybersecurityWorkingGroup.
[77] Sophisticated attack examples. SolarWinds/Orion, Stuxnet. January 2021. url: https://www. newyorker.com/news/daily- comment/after- the- solarwinds- hack- we-have- no- idea-what-cyber-dangers-we-face.
[78] Statistics - European Statistical System (ESS). EU, 2020. url: https : / / ec . europa . eu / eurostat/web/ess.
[79] Steve Bullard. A Practical Approach To Using IoT Devices To Support Legacy SCADA Field Systems In The Transition To Internet-Based Industrial Automation Systems. 20 November 2019. url: https://www.wateronline.com/doc/a- practical- approach- to-using- iot-devices-to-support-legacy-scada-field-systems-0001.

[80] Strategies for Building and Growing Strong Cybersecurity Teams. (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2019. In: Isc2 2019 (), pp. 1–37. url: https://www.isc2.org/-/media / ISC2 / Research / 2019 - Cybersecurity - Workforce - Study / ISC2 - Cybersecurity - Workforce-Study-2019.

[81] Tabetha Newman, Helen Beetham, and Sara Knight. Digital experience insights survey 2018: findings from students in UK further and higher education. September 2018. Jisc, 2018. url: https://repository.jisc.ac.uk/6967/1/Digital_experience_insights_survey_2018. pdf.

[82] The 15 biggest data breaches of the 21st century. United Kingdom, January 2021. url: https: / / www . csoonline . com / article / 2130877 / the - biggest - data - breaches - of - the - 21st - century.html.

[83] Tommaso De Zan. "Mind the Gap: the Cyber Security Skills Shortage and Public Policy Interventions". In: Global Cyber Security Center https://gcsec.org/wp-content/uploads/201 (2019), pp. 1–108. url: https : / / ora . ox . ac . uk / objects / uuid : e9699fc6 - 279c - 4595 - b707 - 7fd0acc487b3.

[84] Vincent E Urias et al. "Cyber range infrastructure limitations and needs of tomorrow: A position paper". In: 2018 International Carnahan Conference on Security Technology (ICCST). IEEE. 2018, pp. 1–5.

[85] Volkmar Lotz. "Cybersecurity Certification for Agile and Dynamic Software Systems – a Process-Based Approach". In: IEEE, 2020, pp. 85–88. isbn: 978-1-7281-8597-2. doi: 10.1109/ EuroSPW51379.2020.00021. url: https://ieeexplore.ieee.org/document/9229655/.

[86] William M. Stahl. "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity". In: Int'l & Comp. 40Ga (), p. L.247. url: https://digitalcommons.law.uga.edu/gjicl/vol40/iss1/9.

[87] Womean4Cyber. url: https://women4cyber.eu/.

[88] Xenia Mountrouidou et al. "Securing the Human". In: Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education (2019-12-18), pp. 157–176. doi: 10.1145/3344429.3372507. url: https://dl.acm.org/doi/10.1145/3344429.3372507.

8. LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/ Definition
API	Application Programming Interface
CCN	Cybersecurity Competence Network
CISO	Chief Information Security Officer
CNO	Chief of Naval Operations
COTS	Commercial Off-The-Shelf
COVID-19	Corona Virus Disease 2019
CONCORDIA	Cyber security cOmpeteNce fOr Research anD Innovation
CSF	Cybersecurity Framework
CTF	Capture the Flag
CyberSec4Europe	Cyber Security competence centres for Europe
PESTLE	Define Political, Economic, Social, Technological, Legal and Environmental factors
ELSA	ethical, legal, and societal aspects
ENISA	European Cybersecurity Agency
ECSO	European Cybersecurity Organization
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
EU	European Union
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IoT	Internet of Things
IP	Intellectual Property
(ISC)2	International Information System Security Certification Consortium
IT	Information Technology
MOOC	Massive Open Online Courses
MISP	Malware Information Sharing Platform

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

MRO	Maintenance, Repair, and Overhaul
NEET	Not in Education, Employment or Training
NIST	National Institute of Standards and Technology
OT	Operational Technology
PESTLE	Political, Economic, Social, Technological, Legal and Environmental
ROI	Return on Investments
SARS-CoV-2	Severe Acute Respiratory Syndrome Coronavirus 2
SOC	Security Operations Centers
SCADA	Supervisory control and data acquisition
SME	Small and Medium-sized Enterprises
SPARTA	Strategic Programs for Advanced Research and Technology in Europe
SWOT	Strengths, Weaknesses, Opportunities, and Threats
VET	Vocational Education and Training

Table 7. List of abbreviations and acronyms.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

9. LIST OF FIGURES

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

10. LIST OF TABLES

11. ANNEXES

ANNEX 1. Austria

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Impor-tance of the parti-cular Link	Justification of linking of aspects and its dependence
P	2. Lack of coordina-tion	High	1. Political - Lack of relevant european regulatory frameworks	High	Lack of coordination on political layer <=> lack of relevant European regulatory frameworks [2,6,7]
			5. Political - Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Low	Political coordination is not a prerequisite for awareness of career paths; awareness of career paths does not influence political coordination [5,8,9,10]
			7. Economic - Economic incentives to enroll or upgrade cybersecurity education programs	Low	Political coordination is not a prerequisite for economic incentives; economic incentives do not influence political coordination [4]
			3. Political - Vulnerabilities of the training systems / Skills shortage	Low	Political coordination does not influence skills shortage; skills shortage does not influence political coordination [5,8,9,10]
			16. Social - Stereotypes and misconceptions of Cybersecurity	Medium	Lack of political coordination increases misconceptions; misconceptions increase lack of political coordination [5,8,9]
			17. Social - Social impact	Medium	Lack of political coordination will increase social impact; social impact will probably trigger improvement of political coordination [2]
			24. Legal - European Certification lack	Medium	Lack of coordination on political layer => lack of European certifications [–]
			21. Technological - Digitalization of Society	Medium	Lack of political coordination delays digitalization; digitalization requires political coordination [–]
			15. Social - Lack of dedicated curricula and training and no clear	none	Political coordination does not influence clear identification of skills; clear identification of skills does not influence political coordination [11]

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			identification of skills		
			25. Legal - Legal framework unification lack	High	Lack of coordination on political layer <=> lack of unification of legal framework [2,6,7]
			18. Social - Social Awareness	Medium	Lack of political coordination will hinder social awareness; social awareness will probably trigger improvement of political coordination [5,8,9]
	1. Lack of relevant european regulatory frameworks	Medium	5. Political - Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Low	Lack of regulatory frameworks reduces awareness of career paths; awareness of career paths does not influence regulatory frameworks [5,8,9,10]
			7. Economic - Economic incentives to enroll or upgrade cybersecurity education programs	Low	Lack of regulatory frameworks disencourages economic incentives; economic incentives do not influence regulatory frameworks [4]
			3. Political - Vulnerabilities of the training systems / Skills shortage	High	Lack of regulatory frameworks increases skills shortage; skills shortage hinders development of regulatory frameworks [5,8,9,10]
			16. Social - Stereotypes and misconceptions of Cybersecurity	High	Lack of regulatory frameworks increases misconceptions; misconceptions hinder development of regulatory frameworks [5,8,9]
			17. Social - Social impact	Low	Low – Regulatory frameworks could reduce social impact; social impact could trigger development of regulatory frameworks [2]
			24. Legal - European Certification lack	Medium	Medium – Regulatory frameworks could increase certifications; certifications might trigger development of regulatory frameworks [–]
			15. Social - Lack of dedicated curricula and training and no clear identification of skills	High	Lack of regulatory frameworks hinders clear identification of skills; no clear identification of skills shortage hinders development of regulatory frameworks [11]
			25. Legal - Legal framework unification lack	High	Regulatory frameworks and legal frameworks are closely related approaches [2,6,7]
			18. Social - Social Awareness	Medium	Medium – Regulatory frameworks could raise social

- CYBERSECURITY SKILLS ALLIANCE
ION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

					awareness; social awareness could trigger development of regulatory frameworks [5,8,9]
	5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Medium	7. Economic - Economic incentives to enroll or upgrade cybersecurity education programs		better education of people who are employed
			24. Legal - European Certification lack		higher legal pressure will come up to the economy (comparable to GDPR)
			27. Legal - Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU		for instance different legal content and references for critical infrastructure in Austria and German [12]
	3. Vulnerabilities of the training systems / Skills shortage	Medium	16. Social - Stereotypes and misconceptions of Cybersecurity	High	very often it´s just linked with an IT-problem and the responsibility of IT
			21. Technological - Digitalization of Society	High	availability of hardware and knowledge in the educational system [13]
			15. Social - Lack of dedicated curricula and training and no clear identification of skills	Medium	based on the educational system [14]
			18. Social - Social Awareness	Low	Awareness on different intellectual knowledge base can help [14]
E	7. Economic incentives to enroll or upgrade cybersecurity education programs	Medium	20. Technological - Availability of Tools	Medium	better tool availability in education could improve the situation
			17. Social - Social impact	Medium	higher educated people with higher sensitivity [13]
			12. Economic - Effects of digital economy on skills demand	Low	the skill demand will become higher if monetary incentives become higher
S	16. Stereotypes and misconceptions of Cybersecurity	Medium	17. Social - Social impact	Medium	very often it´s just linked with an IT-problem and the responsibility of IT [12]
			24. Legal - European Certification lack	Medium	Cloud Security and data in the cloud as example [15]

- CYBERSECURITY SKILLS ALLIANCE
ION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			21. Technological - Digitalization of Society	Medium	often the topic is just based on technology
			18. Social - Social Awareness	High	awareness of technology is important for all groups of age
	17. Social impact	Medium	24. Legal - European Certification lack	High	the national law can be handled in a different way in each EU-country [12]
			21. Technological - Digitalization of Society	Low	high number of people have no technological background of the systems they use
			15. Social - Lack of dedicated curricula and training and no clear identification of skills	Medium	the educational system is currently too slow for integration of all kind of technology [13]
			18. Social - Social Awareness	Medium	awareness of technology is important for all groups of age [16]
T	23. Generalization of cyber attack	High	2. Political - Lack of coordination	High	Lack of coordination on political layer increases generalization of cyber attack [2]
			1. Political - Lack of relevant european regulatory frameworks	Medium	Lack of relevant European regulatory frameworks can increase generalization of cyber attack; generalization of cyber attack can trigger relevant European regulatory frameworks [2,6,7]
			5. Political - Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Medium	Greater attention to polices could reduce generalization of cyber attack; generalization of cyber attack can increase attention to policies [5,8,9,10]
			7. Economic - Economic incentives to enroll or upgrade cybersecurity education programs	Low	Economic incentives could reduce generalization of cyber attack; generalization of cyber attack could increase economic incentives [4]
			3. Political - Vulnerabilities of the training systems / Skills shortage	High	Skills shortage increases generalization of cyber attack [5,8,9,10]
			16. Social - Stereotypes and misconceptions of Cybersecurity	Medium	Misconceptions enable cyber attacks; cyber attacks reduce misconceptions [5,8,9]
			17. Social - Social impact	High	Cyber attacks have social impacts [2]

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			24. Legal - European Certification lack	Medium	Lack of European certifications can increase generalization of cyber attack; generalization of cyber attack can trigger European certifications [–]
			21. Technological - Digitalization of Society	Medium	Digitalization of society could increase generalization of cyber attack; generalization of cyber attack can delay digitalization of society [–]
			15. Social - Lack of dedicated curricula and training and no clear identification of skills	High	No clear identification of skills increases generalization of cyber attack [11]
			25. Legal - Legal framework unification lack	Medium	Lack of European legal framework can increase generalization of cyber attack; generalization of cyber attack can trigger European legal framework [2,6,7]
			18. Social - Social Awareness	Medium	Greater awareness could reduce generalization of cyber attack; generalization of cyber attack can increase awareness [5,8,9]
L	24. European Certification lack	Medium	21. Technological - Digitalization of Society	High	wide range where security events can appear
			15. Social - Lack of dedicated curricula and training and no clear identification of skills	Medium	the educational system is currently too slow for integration of all kind of technology [13]
			25. Legal - Legal framework unification lack	Medium	awareness trainings just started at bigger companies
			18. Social - Social Awareness	Medium	awareness of technology is important for all groups of age [16]
E	31. Connected devices controlling environmentally sensitive productions	High	23. Technological - Generalization of cyber attack	High	Malicious software attack unsecure industrial control systems [2]
			2. Political - Lack of coordination	None	Protection of industrial control systems does not require coordination on political layer; coordination on political layer will not improve protection of industrial control systems [2]
			1. Political - Lack of relevant european	Low	Regulatory frameworks could address protection of industrial control systems [2,6,7]

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			regulatory frameworks		
			5. Political - Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Medium	Higher awareness of cybersecurity career paths can affect protection of industrial control systems [5,8,9,10]
			7. Economic - Economic incentives to enroll or upgrade cybersecurity education programs	Medium	Incentives for cybersecurity education programs can affect protection of Industrial Control Systems [4]
			3. Political - Vulnerabilities of the training systems / Skills shortage	High	Skills shortage affects protection of Industrial Control Systems [5,8,9,10]
			16. Social - Stereotypes and misconceptions of Cybersecurity	None	Social (mis-)conception does not affect protection of Industrial Control Systems [5,8,9]
			17. Social - Social impact	None	Social networks do not affect protection of Industrial Control Systems [–]
			24. Legal - European Certification lack	Medium	Management system, person and product certifications can affect protection of Industrial Control Systems [–]
			21. Technological - Digitalization of Society	None	Digitalization of society does not affect protection of Industrial Control Systems [–]
			15. Social - Lack of dedicated curricula and training and no clear identification of skills	Medium	Clear identification of required skills affects protection of Industrial Control Systems [11]
			25. Legal - Legal framework unification lack	Low	Legal frameworks could address protection of industrial control systems [2,6,7]
			18. Social - Social Awareness	None	Social awareness does not affect protection of Industrial Control Systems [5,8,9]

[1] Austrian Cyber Security Strategy 2013

[2] Austrian Cyber Security Report 2020

[3] High-performance self-sufficient communication network for authorities and operators of critical infrastructures as a practice-oriented government communication network solution (Hammondorgel)

[4] ACCSA – Austrian Cyber Crises Support Activities

REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

[5] European Universities Initiative | Education and Training

[6] Network and Information Systems Security Act – NIS Act – NISG

[7] Network and Information Systems Security Ordinance – NIS Ordinance - NISV

[8] Erasmus+ SecTech

[9] Erasmus+ COLTRANE

[10] AIT Cyber Range

[11] The Cyber Security Body Of Knowledge

[12] https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=cc0d335c-195d-41e3-ba1e-5d66340c2e4e&Position=1&SkipToDocumentPage=True&Abfrage=Erv&Titel=&Quelle=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=nis&Dokumentnummer=ERV_2018_1_111

[13] https://coltrane.ait.ac.at/

[14] https://www.bmbwf.gv.at/Themen/schule/schulpraxis/zentralmatura.html

[15] https://www.techrepublic.com/article/what-is-gaia-x-a-guide-to-europes-cloud-computing-fight-back-plan/#:~:text=Gaia%2DX%20is%20an%20initiative,ves-sel%20for%20data%20across%20industries.

[16] https://ec.europa.eu/eusurvey/files/09d899dd-969a-4f72-a9b3-042391e938ca/7216f17f-463c-4ca2-bdfe-1f499710828b

Table 12. Austria.

Aspect name	Notes
31. Connected devices controlling environmentally sensitive productions	AT-02. Unsecure industrial control systems (e.g. SCADA) [1] Trends 2020: + Internet of Things [2]
23. Generalization of cyber attack	AT-AT-06. Malicious software [1] AT-AT-12. Manipulation of cloud service systems [1] Trends 2020: + (Targeted) ransomware [2]
2. Lack of coordination	AT-09. Unclear responsibility across governmental institutions [1]
1. Lack of relevant european regulatory frameworks	AT-07. Incomplete Cyber Governance [1] Trends 2020: – Cybersecurity Act, NIS Act [2]
5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	AT-13. Missing focus on regulations for IT-security [1]
7. Economic incentives to enroll or upgrade cybersecurity education programs	AT-14. Not enough incentives for security investments [1]

3. Vulnerabilities of the training systems / Skills shortage	AT-16. Lack of experts [1]
16. Stereotypes and misconceptions of Cybersecurity	AT-17. Inadequate understanding of the cyberattack status [1]
17. Social impact	AT-18. Social networks and their manipulation [1] AT-34. Cybercrime [1]
24. European Certification lack	AT-19. No security seal of quality/audits [1]

Table 13. Austria Notes.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

ANNEX 2. Cyprus

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	1. Lack of relevant european regulatory frameworks	High	2. Political - Lack of coordination	Lack of coordination between stakeholders is directly related to the lack of relevant EU frameworks. Possible coordination between EU and international stakeholders towards a unified EU regulatory framework would be beneficial for the development of cybersecurity educational framework with commonly agreed standards [1].
			27. Legal - Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	Since there is no standard job description for cybersecurity roles, there is no unified curriculum for cybersecurity education and skills development [2].
			25. Legal - Legal framework unification lack	Since there is no standard job description for cybersecurity roles, there is no unified curriculum for cybersecurity education and skills development [3]
			Social - Fragmentation of cybersecurity training and certification for professionals	Various professional qualifications are currently offered, which create a fragmentation of cybersecurity training and certifications. This is related to the fact that there is not a standard EU regulatory framework [3].
E	8. Economic impact of inadequate (national) cybersecurity capabilities	Medium	23. Technological - Generalization of cyber attack	inadequate cyber security capabilities could lead to risk omissions of and risk priorities, leading to economic impacts as soon as the overlooked risks are materialized [1].
			15. Social - Lack of dedicated curricula and training and no clear identification of skills	The more explicit curriculums and training provided the more precise the cybersecurity roles and capabilities covering all aspects of cybersecurity and thus, reducing the exposure that could in turn have a great impact if materialized [1].
			28. Legal - Missing comprehensive cybersecurity officer role description in organization compared to data	positions related to cybersecurity are not following any standards, thus lowering possible involvement of competent CISO [4].
S	18. Social Awareness	Medium	16. Social - Stereotypes and misconceptions of Cybersecurity	One of the problems identified by the [19] national report regarding the safety online, is that there is a great deficiency in awareness and knowledge regarding security [5].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			15. Social - Lack of dedicated curricula and training and no clear identification of skills	Currently in Cyprus, there are only a few programs related to cybersecurity. Although the number is small, since there is no agreed and standardized set of competencies, they exhibit differences. For example, if someone compares the two MScs provided from the European University Cyprus and the UCLan Cyprus, they will discover that only a limited number of courses seem to be common (Compulsory courses: CYS601 Introduction to Cybersecurity, CYS610 Communications and Network Security, CYS620 Cryptography, CYS640 Cybersecurity Policy, Governance, Law and Compliance, CYS650 Cybersecurity Risk Analysis and Management, CYS660 Cybersecurity Architecture and Operations for the first one and Critical Analysis, Ethical Hacking, Digital Forensic Investigation , Information Security Management , Cyber Warfare, Cyber Defense for the second) [6], [7].
			5. Political - Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Within the coalition, three working groups have been formed (education and training, certification and awareness) in order to formulate and implement an Action Plan and a roadmap, with the aim to attract young people into ICT education and increase the supply of ICT practitioners. The Action Plan has been approved by the Council of Ministers on 18 January 2016. The majority of actions to be implemented are related to awareness of various target groups [8].
	16. Stereotypes and misconceptions of Cybersecurity	Medium	13. Social - Gender balance	Misconceptions of cybersecurity, lead to low involvement of prospects into this field, and moreover minor involvement of women into cybersecurity [9].
			27. Legal - Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	positions related to cybersecurity are not following any standards, thus lowering possible involvement of prospects in this area [1].
			Social - Cybersecurity training for lower ages - secondary education curriculum	Cybersecurity and related definitions should be introduced into secondary education, thus allowing students to be aware of cybersecurity from their early stages, and secondly to allow them to be acquainted with this field and possibly engage professionally in their later career [3].
	17. Social impact	High	18. Social - Social Awareness	lack of social awareness on cybersecurity has an impact on society [3]

- CYBERSECURITY SKILLS ALLIANCE
ION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			21. Technological - Digitalization of Society	As digitalization of society is increasing, cyber threats are surging. A cyberattack has wide impact, probably also social impact [10].
			5. Political - Greater attention to policies dedicated to raise awareness of cybersecurity career paths	lack of social awareness on cybersecurity has an impact on society [1], [3].
			Social - Cybersecurity training for lower ages - secondary education curriculum	Society will be benefited if cybersecurity education is introduced from secondary education. The soonest people are engaged into cybersecurity, the more benefit will be returned back to the society [11].
T	23. Generalization of cyber attack	Medium	23. Technological - Generalization of cyber attack	Improper classification of attacks due to lack of thorough understanding could lead to risk omissions of and risk priorities, leading to economic impacts as soon as the overlooked risks are materialized [1].
			27. Legal - Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	Generalization of cyber attacks leads to roles and skill sets (one fits all) which in can result in having the wrong people for the job and inherently overlook certain risks [1].
			3. Political - Vulnerabilities of the training systems / Skills shortage	Not matured enough and vulnerable training systems once more lead to lack of expertise and thus, the generalization of all types of attacks and the incompetency to classify and mitigate relevant risk to the various types of these attacks [12].
L	27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	Medium	15. Social - Lack of dedicated curricula and training and no clear identification of skills	Currently in Cyprus, there are only a few programs related to cybersecurity. Although the number is small, since there is no agreed and standardized set of competencies, they exhibit differences. For example, if someone compares the two MScs provided from the European University Cyprus and the UCLan Cyprus, they will discover that only a limited number of courses seem to be common (Compulsory courses: CYS601 Introduction to Cybersecurity, CYS610 Communications and Network Security, CYS620 Cryptography, CYS640 Cybersecurity Policy, Governance, Law and Compliance, CYS650 Cybersecurity Risk Analysis and Management, CYS660 Cybersecurity Architecture and Operations for the first one and Critical

				Analysis, Ethical Hacking, Digital Forensic Investigation , Information Security Management , Cyber Warfare, Cyber Defense for the second) [6], [13].
			28. Legal - Missing comprehensive cybersecurity officer role description in organization compared to data	The national authority for the human resources development of Cyprus conducts surveys and studies based on a standardized set of occupations. Unfortunately occupations regarding information security or cybersecurity are missing. The closest is the one of the IT manager of technician. Since this information is being drawn from the ISCO-08 categories, the relevant studies cannot be implemented in Cyprus, leading to a gap in information [14], [15].
			24. Legal - European Certification lack	The findings of the survey also showed that ICT professionals do not have adequate development in terms of acquiring professional ICT qualifications. ICT companies that participated in the survey identified a lack of necessary skills for the integration of graduates into the Labour market, such as the use of English, effective communication, technical presentations, ability to communicate effectively with customers, ability to find solutions to real problems of companies, ability to contribute to the development of innovative ideas, and ability to manage real risks and crises. The increase in total (employment) demand (including both expansion and replacement demand) in this occupational group is expected to be around 3% per year until 2024 according to the latest set of the HRDA forecasts [16].
	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	Medium	18. Social - Social Awareness	lack of social awareness on data privacy has an impact on society [3].
			3. Political - Vulnerabilities of the training systems / Skills shortage	Explicit training/skill sets covering all aspects (cybersecurity and legal issues) results to inadequate knowledge and expertise. This may lead omissions of risks to which organizations are exposed to and severe impacts [1].
E	30. Covid-19 pandemic crisis	High	11. Economic - Economic costs of incompatible training platforms and cyber ranges	COVID-19 brought forth the need for cybersecurity education from a distance - but also at the level provided (effectiveness). To achieve this level of quality practical remote sessions should be implemented. The Cypriot action plan for digital skills identifies the need to link theory to practice as an important factor.

- CYBERSECURITY SKILLS ALLIANCE
ION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				Practical (cyber range) platforms are expensive directly and indirectly. (Directly through acquisition and installation, indirectly because they require an investment of time of competent people in order to be customized to the needs and for scenarios to be created. The lack of financial ability and time (urgency) led to poor implementation of the practical parts of education and training
			9. Economic - The economic impact of National economic resources	Cyprus was on a solid growth path before the global outbreak of COVID-19. The pandemic and the confinement measures that followed have dramatically changed the picture. In the first quarter of 2020, economic growth slowed down considerably, 0.8% (year-on-year), reflecting a significant fall in external demand for goods and tourism. Economic sentiment and expectations in services are at a historic low, despite a slight improvement in June [17].
			10. Economic - Licensing costs and different licensing models of software used in cybersecurity education	COVID-19 brought forth the need for cybersecurity education from a distance - but also at the level provided (effectiveness). To achieve this level of quality practical remote sessions should be implemented. The cypriot action plan for digital skills identifies the need to link theory to practice as an important factor. Practical (cyber range) platforms are expensive directly and indirectly. (Directly through acquisition and installation, indirectly because they require an investment of time of competent people in order to be customized to the needs and for scenarios to be created. The lack of financial ability and time (urgency) led to poor implementation of the practical parts of education and training [18].
	31. Connected devices controlling environmentally sensitive productions	High	23. Technological - Generalization of cyber attack	Incompetence's may lead to misclassification of attacks where in cases of critical to the environment sectors can result to irrecoverable accidents like oil spills threatening marine ecosystem [1].
			21. Technological - Digitalization of Society	IoT devices and the expertise as to the exposure of these devices is the most important element of securing them and the environments they control. The lack of standards, knowledge, credentials on

REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				testing and certifying such products may lead to vulnerable devices leading high risk exposures [10].
			22. Technological - Emerging Technologies	IoT devices and the expertise as to the exposure of these devices is the most important element of securing them and the environments they control. The lack of standards, knowledge, credentials on testing and certifying such products may lead to vulnerable devices leading high risk exposures [1].

[1] National Strategy (par 3.10) Training, National Strategy (par 3.9), National Strategy (par 3.7) Business Capability Awareness, cyberethics. Url. cybersafety.cy

[2] Cybersecurity Strategy of the Republic par 3.11 of Cyprus Network and Information Security and Protection of Critical Information Infrastructures https://ocecpr.ee.cy/sites/default/files/ec_doc_stratigikikevernoasfalias_en_31-5-2013_ce.pdf

[3] CYBERSECURITY CAPACITY REVIEW, Republic of Cyprus, December 2017, D3.3 https://ocecpr.ee.cy/sites/default/files/cmm_cyprus_report_2017_final.pdf

[4] National Strategy (par 3.7) Business Capability. Url. cybersafety.cy

[5] General Report_Final_2sep16a_noAnnexes.pdf (esafecyprus.ac.cy)

[6] https://euc.ac.cy/el/programs/master-cybersecurity/#program-page-tabs|2

[7] https://www.uclancyprus.ac.cy/postgraduate-course/msc-cybersecurity#tab_b/

[8] www.digitaljobs.cyprus-digitalchampion.gov.cy/el/file/V87uJE4hd0ahGYAsl9Rd6A==/ (cyprus-digitalchampion.gov.cy)

[9] https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)651042

[10] Building National Capabilities. European Project with all stakeholders for building capabilities. Awareness is part of the funded project. National Strategy (par 3.7) Business Capability

[11] National Strategy (par 3.9) Awareness (cyberethics. cybersafety.cy)

[12] National Strategy (par 3.10) Training

[13] https://www.uclancyprus.ac.cy/postgraduate-course/msc-cybersecurity#tab_b/, https://www.cyberwiser.eu/cyprus-cy

[14] Αρχή Ανάπτυξης Ανθρώπινου Δυναμικού Κύπρου (anad.org.cy) http://www.digitaljobs.cyprus-digitalchampion.gov.cy/el/file/V87uJE4hd0ahGYAsl9Rd6A==/

[15] http://www.hrdauth.org.cy/images/media/assetfile/133.pdf

[16] Cyprus: Mismatch priority occupations | Skills Panorama (europa.eu)

[17] https://ec.europa.eu/economy_finance/forecasts/2020/summer/ecfin_forecast_summer_2020_cy_en.pdf

[18] https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf

[19] https://www.esafecyprus.ac.cy/udata/contents/files/Eggrafa/General%20Report_Final_2sep16a_noAnnexes.pdf

Table 14. Cyprus.

ANNEX 3. Czech Republic

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	1. Lack of relevant european regulatory frameworks	Medium	24. Legal - European Certification lack	Possible ways how to think on certification not only of the devices and services, but also people based on skills framework [1].
			27. Legal - Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	Partly described and defined in the article. One of the goals of the project described in the article is to create the Czech framework in connection to EU pilots [2].
			15. Social - Lack of dedicated curricula and training and no clear identification of skills	Partly described and defined in the article. One of the goals of the project described in the article is to create the Czech framework in connection to EU pilots [2].
	3. Vulnerabilities of the training systems / Skills shortage	Medium	8. Economic - Economic impact of inadequate (national) cybersecurity capabilities	Especially smaller organizations are often not aware of attacks and their impacts on the business because lack of skills [3].
			13. Social - Gender balance	Cybersecurity is still considered as mostly man domain of IT. Not well covered by national references, bud European reference is available [4].
			14. Social - Diversified workforce	The need for education and methodological and supportive approach described in the article stated as a source [2].
E	No identified aspects for Economic Factor			
S	15. Lack of dedicated curricula and training and no clear identification of skills	High	7. Economic - Economic incentives to enroll or upgrade cybersecurity education programs	The lack of curricula and training is not supporting the economic growth and importance of this is seen in the sector. General problem of lack of experts in this field is stressed out [5].
			8. Economic - Economic impact of inadequate (national) cybersecurity capabilities	By education it is needed to support the expertise in this field, because the capacities are insufficient [5].
			8. Economic - Economic impact of inadequate (national) cybersecurity capabilities	Generally mentioned the need of education and positive impacts due to the lack of capacities [6].
T	19. Cyber Ranges	Medium	10. Economic - Licensing costs and different licensing models of software used in cybersecurity education	Open-source solutions are still very rare and high costs of commercial cyber ranges limit their usage for cyber security education [7].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			11. Economic - Economic costs of incompatible training platforms and cyber ranges	Missing open formats limit interoperability, restrict cooperation on training materials and raise costs of cybersecurity education [7].
			20. Technological - Availability of Tools	Selection of quality tools is limited. Commercially available cyber ranges and other tools are hard to reach for smaller organizations [7].
	20. Availability of Tools	Medium	12. Economic - Effects of digital economy on skills demand	Availability of tools for education increases the value of professionals on the market [8].
			10. Economic - Licensing costs and different licensing models of software used in cybersecurity education	High costs of tools limit their usage for cyber security education. Open-source solutions are still very rare [7].
			11. Economic - Economic costs of incompatible training platforms and cyber ranges	Tools are very firmly connected with cyber ranges and lack open approach for data and configuration exchange [7].
	22. Emerging Technologies	Medium	15. Social - Lack of dedicated curricula and training and no clear identification of skills	Lack of training limits professionals in defending critical information infrastructure of the state [8].
			10. Economic - Licensing costs and different licensing models of software used in cybersecurity education	Licenses of software or hardware components are often too high for education purposes [7].
			20. Technological - Availability of Tools	Tools for efficient education of cybersecurity related to technologies like IoT, smart grids, blockchain etc. are needed [7].
	21. Digitalization of Society	Medium	18. Social - Social Awareness	Despite slowly growing awareness about cyber security citizens are not able to grasp severity of some attacks [9].
			3. Political - Vulnerabilities of the training systems / Skills shortage	Education and training are barely keeping pace with new cyber attacks [5].
			30. Environmental - Covid-19 pandemic crisis	During pandemic crisis number of attack on hospitals increased dramatically [10].
L	24. European Certification lack	Medium	2. Political - Lack of coordination	Generally stressed out that in whole field the coordination and support of the field is highly needed [11].
			20. Technological - Availability of Tools	Only partly explained general need of certification with certification specifics to the intelligence [12].
			4. Political - Political ambition to create	A general requirement to grasp this problematics with regard to the construction of related capacities [13].

- CYBERSECURITY SKILLS ALLIANCE
ION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			cooperation frameworks	
	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	Medium	9. Economic - The economic impact of National economic resources	Actual situation connected with data leaks connected with the personal data of the vaccinated Czech inhabitants [14].
			1. Political - Lack of relevant european regulatory frameworks	Uncertainty with cross-border data transfer with US (so called privacy shield) [15].
			2. Political - Lack of coordination	Different types of enforcement mechanisms and fines under GDPR (possible lack of coordination in the approach to the GDPR) [16].
	27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	High	6. Economic - The economic impact of the European cybersecurity educational ecosystem	The methodology and deeper description of the roles in cybersecurity should lead to better understanding of the needs thus to support whole field [17].
			2. Political - Lack of coordination	Standardization and its importance however has to be reflected and supported throughout the field [17].
			14. Social - Diversified workforce	To build on insufficient capacities, it is necessary to understand the potential of different roles played in cybersecurity [17].
E	No identified aspects for Environmental Factor			

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) connected with describing certification of the people: Jakub Vostoupal. The Cybersecurity Qualifications as the Prerequisite for the Cybersecurity Certifications of Persons. Will be published soon Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2021

[2] Jan Hajný, František Kasl, Pavel Loutocký, Miroslav Mareš, Tomáš Pitner. PROGRESS TOWARDS CZECH NATIONAL CYBERSECURITY QUALIFICATIONS FRAMEWORK. Will be published soon Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2021

[3] https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2015-2020.pdf

[4] https://www.concordia-h2020.eu/wp-content/uploads/2019/09/WomenInCyberMANIFESTO.pdf

[5] National cybersecurity strategy 2020 - 2025, https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

[6] Annual Report of the Security Information Service for 2019, https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf

[7] ČEGAN Jakub. Cyber Range as a Tool For Cyber Security Education. In: IS2 - INFORMATION SECURITY SUMMIT. Praha: Tate International s.r.o., 2020, s. 16-21. ISBN 978-80-86813-33-2.

[8] Mentioned by security director of National Agency for Communication and Information Technologies in an article about cybersecurity trainings https://csirt.muni.cz/about-us/news/muni-a-nakit-pripravily-kurzy-kyberbezpecnosti-pro-it-profesionaly

[9] https://cbaonline.cz/kyberbezpecnost-a-index-bezpecnosti-2019

[10] https://www.nukib.cz/download/uredni_deska/Varovani_NUKIB_2020-04-16.pdf

[11] Basic information on certification, EU cyber security certification, https://nukib.cz/cs/kyberneticka-bezpecnost/vyzkum/eu-certifikace-kyberneticke-bezpecnosti/

[12] Annual Report of the Security Information Service for 2019, https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2019-vz-cz.pdf

[13] Mentioned https://nukib.cz/cs/kyberneticka-bezpecnost/vyzkum/eu-certifikace-kyberneticke-bezpecnosti/ or at the conferences and meetings mentioned also here: https://nukib.cz/en/cyber-security/research-nukib/eu-certification-of-cybersecurity/

[14] https://www.uoou.cz/vyjadreni-uradu-k-nbsp-nahodilym-unikum-informaci-o-nbsp-ockovanych-osobach/d-47751

[15] http://curia.europa.eu/juris/document/document.jsf?docid=228677&text=&dir=&doclang=CS&part=1&occ=first&mode=lst&pageIndex=0&cid=6171606

[16] https://www.enforcementtracker.com/

[17] Jan Hajný, František Kasl, Pavel Loutocký, Miroslav Mareš, Tomáš Pitner. PROGRESS TOWARDS CZECH NATIONAL CYBERSECURITY QUALIFICATIONS FRAMEWORK. Will be published soon Jusletter IT. Die Zeitschrift für IT und Recht. Bern: Weblaw, 2021

Table 15. Czech Republic.

ANNEX 4. France

Factor group	Aspect name	Importance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	2. Lack of coordination	High	15. Social - Lack of dedicated curricula and training and no clear identification of skills	ANSSI is also involved in the elaboration of cyber skill framework/curriculum : ANSSI, SecNumedu: Label for Initial Cybersecurity Trainings in Higher Education [1].
			18. Social - Social Awareness	ANSSI is also contributing to cybersecurity awareness activities [2].
E	12. Effects of digital economy on skills demand	High	21. Technological - Digitalization of Society	The main demand for skills is related to artificial intelligence, big data and machine learning, which are proposing salaries higher than the average and are more attractive particularly for students that have a mathematical background [3], [4].
	7. Economic incentives to enroll or upgrade cybersecurity education programs	High	12. Economic - Effects of digital economy on skills demand	Jobs in AI, machine learning and big data are more attractive, hence depleting the number of students entering cybersecurity curricula. In France, the total M2 training programmes only operate at 70% capacity, according to ANSSI (private data) [6].
S	18. Social Awareness	High	26. Legal - Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	National Assistance System for Victims of Cybermalveillance, Digital Risk Awareness Kit [7].
			7. Economic - Economic incentives to enroll or upgrade cybersecurity education programs	Cybersecurity awareness is improving and protective measures are increasing, but they still do so at a slow pace due to a lack of incentive [11].
			15. Social - Lack of dedicated curricula and training and no clear identification of skills	Cybersecurity Awareness for Computer Science Curriculums [8].
	15. Lack of dedicated curricula and training and no clear identification of skills	High	21. Technological	Study program needs to be improved and needs to be involved in reinforcement and development of digital security issues [9].
	13. Gender balance	Medium	15. Social - Lack of dedicated curricula and training and no	Gender balance in cybersecurity studies [10].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			clear identification of skills	
T	21. Digitalization of Society	High	12. Economic - Effects of digital economy on skills demand	Cybersecurity often lacks incentive and academics are often underrepresented in national or industrial advisory committees [11].
L	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	Medium	25. Legal - Legal framework unification lack	harmonized rules are needed in personal data protection [5].
			1. Political - Lack of relevant European regulatory frameworks	"understanding the underlying ecosystem is essential since it often determines the practices in terms of personal data collection and processing. A sustainable ecosystem respectful of European regulation in terms of data protection is needed" [11].
E	No identified aspects for Environmental Factor.			

[1] ANSSI, Centre de Formation à la Sécurité des Systèmes d'Information / Information Systems Security Training Center, https://www.ssi.gouv.fr/uploads/2014/10/anssi-cfssi-plaquette.pdf, 2020

[2] Michel Van Den Berghe, Cyber Campus: Unite and Promote the Cybersecurity Ecosystem, https://www.ssi.gouv.fr/uploads/2019/10/campuscyber-rapport.pdf, 2020.

[3] French government statistics (2019): https://dares.travail-emploi.gouv.fr/publications/les-tensions-sur-le-marche-du-travail-en-2019

[4] https://www.reussirmavie.net/Metiers-de-la-big-data-l-avenir-est-dans-les-donnees_a2107.html

[5] CNIL, Guides and Recommendations on Data Protection, https://www.cnil.fr/fr/mediatheque, 2021

[6] ANSSI, SecNumAcademie, https://secnumacademie.gouv.fr/, 2017

[7] National Assistance System for Victims of Cybermalveillance, Digital Risk Awareness Kit: https://www.cybermalveillance.gouv.fr/medias/2019/02/kit_complet_de_sensibilisation.pdf, 2019.

[8] ANSSI, CyberEdu: Cybersecurity Awareness for Computer Science Curriculums, http://www.cyberedu.fr/, 2016

[9] ANSSI, SecNumedu: Label for Initial Cybersecurity Tranings in Higher Education, https://www.ssi.gouv.fr/entreprise/formations/secnumedu/, 2017

[10] CEFCYS, Cercle des Femmes de la Cyber-Sécurité / Women4Cyber France, Guide of Professions, Trainings and Opportunities in Cybersecurity, https://cefcysblog.wordpress.com/publications/, 2020.

[11] INRIA, White Book on Cyber-Security: Current Challenges and Inria's Research Directions, https://files.inria.fr/dircom/extranet/LB_cybersecurity_WEB.pdf, 2019

Table 16. France.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

ANNEX 5. Lithuania

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	No identified aspects for Political Factor.			
E	9. The economic impact of National economic resources	High	4. Political - Political ambition to create cooperation frameworks	Recommendations: Promote the establishment of a market for cyber-insurance and encourage information-sharing among participants of the market [1].
S	18. Social Awareness	High	2. Political - Lack of coordination	Programs and materials are available to train and improve cybersecurity practices from the private sector and government agencies to raise awareness in schools, universities and among clients. However, it often stays on an institutional level and is not coordinated nationally [1], [2], [3], [4].
			4. Political - Political ambition to create cooperation frameworks	Recommendations: Routinize cross-sectorial cooperation and information sharing among private and public sector organizations on cybersecurity risks and good practice [1], [2], [3], [4].
			25. Legal - Legal framework unification lack	Executives are aware of general cybersecurity issues, but not how these issues and threats might affect their organization necessarily. Executives of particular sectors, such as finance, telecommunications, Internet providers and cloud operators are aware of cybersecurity risks and how the organization deals with cybersecurity issues, but not of the strategic implications. However, there are no requirements for CEOs to receive certain trainings [1], [2], [3], [4].
			27. Legal - Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	
	15. Lack of dedicated curricula and training and no clear identification of skills	High	6. Economic - The economic impact of the European cybersecurity educational ecosystem	Some educational courses exist in cybersecurity-related fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet offered in Lithuania. It was noted during the consultations that the demand for cybersecurity education is evidenced through course enrolment and feedback within Universities [2], [3], [5].
			7. Economic - Economic incentives to enroll or upgrade cybersecurity education programs	Expert educators are limited, some Universities have introduced a scheme of "industry professors", inviting experts from industry to teach specific topics [2], [3], [5].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			12. Economic - Effects of digital economy on skills demand	Research and development is an important consideration in cybersecurity education [2], [3], [5].
T	No identified aspects for Technological Factor.			
L	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	High	18. Social - Social Awareness	Discussions regarding the protection of personal information and about the balance between security and privacy are discussed in the media, but this has not resulted in concrete actions or policies that reach beyond the EU regulation. Recommendations: Promote the understanding of protection of personal information online among users and promote the development of their skills to manage their privacy online. Recommendations: Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making [1].
			15. Social - Lack of dedicated curricula and training and no clear identification of skills	Review participants also agreed that skills do often not exist and services to protect themselves are neither offered nor known [1].
			6. Economic - The economic impact of the European cybersecurity educational ecosystem	
			7. Economic - Economic incentives to enroll or upgrade cybersecurity education programs	
	24. European Certification lack	High	2. Political - Lack of coordination	The Government promotes relevant standards in software development, but there is no widespread use of these standards yet. There are sector-specific requirements, but no policy or regulation for secure software development exists yet [1].
			4. Political - Political ambition to create cooperation frameworks	
E	No identified aspects for Environmental Factor.			

[1] https://www.nrdcs.lt/file/repository/resources/Lithuania_Report_10_8_2017_FINAL.pdf;
[2] http://www.lka.lt/download/49256/3%20journal%20of%20security%20and%20sustainability%20issues%20nr6_3_3.pdf;
[3] https://www.vkontrole.lt/aktualija.aspx?id=21679 (State control: cybersecurity in the public sector is ensured on average,
[4] https://www.vkontrole.lt/failas.aspx?id=3504);
[5] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Lithuania

Table 17. Lithuania.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

ANNEX 6. Greece

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	2. Lack of coordination	Medium	1. Lack of relevant european regulatory frameworks	Greek NCSA cooperates with its EU and international counterparts. At EU level, as Critical Infrastructures are becoming more vulnerable to cyber-attacks, their protection becomes a significant issue for Countries. Over the past few years, the European Union (EU) has proposed a wide range of measures to enhance the protection of its citizens and businesses against cyber-attacks and to equip Europe with the tools necessary to deal with ever-changing cyber threats. In addition to the Directive concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) of July 2016, the European Commission adopted a cybersecurity package in September 2017 with proposals to further strengthen EU's resilience and response to cyber-attacks, along with the Cybersecurity Blueprint to respond effectively to large scale cybersecurity incidents. These initiatives were recently strengthened by the Cybersecurity Act [1].
			3. Vulnerabilities of the training systems / Skills shortage	Greece supports the transfer of know-how and expertise among countries for a more effective cybersecurity strategy. The Greek NCSA has participated in several educational, awareness and research activities, e.g., being one of the first National Authorities that participated in the consortium of CONCORDIA, one of the four pilots (the other three are ECHO, SPARTA and CyberSec4Europe) which addressed the Horizon 2020 Cybersecurity call "Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap" [1].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			21. Digitalization of Society	In order to safeguard common interests, cyber-diplomacy has been developed promoting responsible cyber behavior at state level. At the same time, cross-border dependencies impose international cooperation aimed at achieving a common high level of security. In this context, Greece should maintain and enhance its presence and participation in international cooperation for [20].
	3. Vulnerabilities of the training systems / Skills shortage	Medium	5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Capacity building, systematic and ongoing training, as well as raising and maintaining a high level of awareness of all participants in the National Cybersecurity Ecosystem, are key elements in ensuring vigilance against threats and effective response to security incidents. The development of an education plan compatible and harmonized with the needs of the Ecosystem is crucial for the successful outcome of the actions of this strategic goal. The plan should set specific goals for educating and informing the various stakeholders and outline the roadmap for achieving them [24].
			4. Political ambition to create cooperation frameworks	One important action for ensuring cybersecurity is the enhancement of digital skills and the development of a strong public and private security culture, exploiting the potential of the academic community and public and private sector actors [24, 25]. Continuous adaptation of the national institutional framework to the new technological requirements, always in line with the European regulations on data protection and security will help Greece fight cyber crime. The 2020-2025 National Cybersecurity Strategy places particular emphasis on the preparation of future executives in the field of cyber security, for which support is required from the institutions of higher and higher education [24].
			6. The economic impact of the European cybersecurity educational ecosystem	Investing in innovation, research and development on security issues through the promotion of public-private partnerships aiming at cooperation and the mutual exchange of know-how is also an important step towards a safe and secure cyber space. This initiative includes the exploitation of all available financial tools and the design of new specialized development programs to enhance security and privacy [24,25].

- CYBERSECURITY SKILLS ALLIANCE
SION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			16. Stereotypes and misconceptions of Cybersecurity	Creating appropriate incentives for the younger generations to come into direct contact with cybersecurity and to be able to choose it as a subject of study or specialization. The ultimate goal is to establish a cyber-hygiene framework and to create a positive culture towards cybersecurity [24].
E	8. Economic impact of inadequate (national) cybersecurity capabilities	High	9. The economic impact of National economic resources	Cyberattacks and cybercrime victimization are mainly on the high end of the scale in growing and stabilizing economies such as Greece where cybercriminals target the loopholes existing in an expanding economy [5, 6]. Cyber crime has especially escalated following the understaffing of government agencies mandates with cyber security, their lack of equipment that could match that used by the perpetrators [7].
			18. Social Awareness	Individuals and organizations experience attacks, most of them do not even notice and, therefore, no report of the attacks are made like in the case of Greece [5].
			30. Covid-19 pandemic crisis	The COVID-19 pandemic changed the business landscape for almost every organization, forcing them to abandon their business and strategic plans and to quickly implement secure mass connectivity on a massive scale for their human resources. Digital security teams and technicians also had to deal with growing threats to their cloud systems as hackers sought to take advantage of the pandemic: 71% of digital security professionals reported an increase in cyber threats from the beginning of quarantine. One of the few predictable things about cyber security is that hackers will always try to take advantage of events or changes - such as COVID-19 or the advent of 5G - for their own benefit. In order to stay protected, organizations and businesses must prevent and not leave systems unprotected or unattended, because they risk becoming the next victim of sophisticated and targeted attacks. Malware attacks have returned dynamically to the Greek landscape, with the top 3 being: Emoted which had an impact in the country in September 2020 of 26.84% while last October had doubled to 47.84%, Agenesia in which in September had a percentage of 12.78%, while in October it recorded a slight decrease to 9.88% and finally Tricot where last September it had a percentage of 4.79% and in October 6.79% recording an increase " [5,6,7].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

S	18. Social Awareness	High	5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Phishing, which involves the capturing of an individual's financial information with the intent of manipulating their financial and online banking data illegally [11,12] and is used to divert the traffic of a legitimate website to another used by cybercriminals [13] key logging as well as the use of Facebook and other social networking platforms in Greece in 2011 has to be the most common form of illegal activity perpetrated by cybercriminals [14].
			17. Social impact	Online child exploitation, which represents a constantly growing phenomenon on an international basis. This results from the lack of focus by the government to improve the social sectors. As such, research proposes that the detection of the cybercrimes that focus on children, when done early enough, could promote the decline in their prevalence [15].
			16. Stereotypes and misconceptions of Cybersecurity	The successful implementation of the National Cyber Security Strategy also depends on the creation of a positive security culture at the national level. Constantly informing the general population is one of the most critical success factors of the Strategy [18].
T	22. Emerging Technologies	High	21. Digitalization of Society	Cybercrime in Greece has risen following the adoption of new technologies, especially in the social networking arena, the banking and finance sectors, and the broadband technologies as have other European nations [14]. Technological upgrades increase the vulnerabilities to attacks and exploitations by cybercriminals [19]. Presently, the National Strategy [20] emphasizes the need to understand technological developments especially with regard to 5G networks, artificial intelligence and IoT. These technologies require the adoption of cyber security principles by design and by default, in order to ensure the protection of both infrastructure and data and compliance with existing laws and regulations (such as EU - Greek Law 4624/20198, NIS Directive - Greek Law 4577/201810, ePrivacy, etc.).
			4. Political ambition to create cooperation frameworks	Coordinated national action is necessary to prevent, respond to and recover from threats in order to secure network infrastructures and reduce incidents. Government agencies, stakeholders from private sector, academics, regional and international organizations could be more aware of potential threats and take steps toward remedy if collaborate among them.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				Effective incident management requires funding, human resources, technological capability, training, government and private sector collaborations, and legal requirements. The development of organizational structures at the national and regional level and the promotion of communications, information sharing and the recognition of digital credentials across different nations are actions that are essential to be made [21,22].
			24. European Certification lack	Development of enhanced security requirements (horizontal and sectoral) taking into account international and European standards and certification frameworks [22].
	19. Cyber Ranges	High	3. Vulnerabilities of the training systems / Skills shortage	Cyber range platforms create the appropriate environment for the technical training of the executives, ensuring their constant vigilance against cyber threats that may endanger their business operation and provision of services [26].
			2. Lack of coordination	Cybersecurity exercises will be carried out in cooperation with national and European bodies. Greece will take an active part in exercises such as Cyber Europe organized by ENISA or Locked Shields organized by NATO [26].
			11. Economic costs of incompatible training platforms and cyber ranges	Cyber ranges enhance the exchange of information and knowledge, the cooperation between the participating bodies while at the same time, strengthen the culture of cooperation for the increase of the level of Cybersecurity in the country [28].
L	25. Legal framework unification lack	High	8. Economic impact of inadequate (national) cybersecurity capabilities	The escalation of cybercrime activities, in European countries; specifically, Greece, is aided by the lack of rigid and concrete laws governing the detection and prosecution of cybercrimes [8].
			4. Political ambition to create cooperation frameworks	International security, following the governance of cyberspace, is impacted adversely by the unchecked sovereign power of states as they are placed at the forefront in the development and opportunities exploited by cybercriminals [5].
			17. Social impact	Regardless of the availability of laws and regulations governing the safe use of the Internet by children in different countries, there still exists a gap in the level of education and awareness of children about online safety [9,10].
	27. Need for standardization of cybersecurity	High	2. Lack of coordination	The ENISA report on Cybersecurity Skills Development in the EU has already pointed out the need for a standardized approach

- CYBERSECURITY SKILLS ALLIANCE
SION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	roles definition and cybersecurity skills across the EU			regarding skills definition and a concrete plan for cybersecurity career management. Already some organizations (and local governments) have implemented some actions but coordination is needed to have a sustainable result. (The reason why we are linking the ENISA study is because Greece in not within the countries where specific developments on the subject are mentioned - unlike e.g. France showing a lack of specific framework). Moreover the need and importance for cooperation is also included in the basic principles behind the Greek National Cybersecurity strategy [31].
			3. Vulnerabilities of the training systems / Skills shortage	There is a skills shortage in Greece regarding digital skills including ones related to cybersecurity. There are several studies showing this deficiency including the DESI index. This gap in knowledge and skills related to cybersecurity has been identified in the National cybersecurity strategy. The strategy contains specific actions to bridge the gap also for young graduates. (Action 5.B.3.) [32].
			1. Lack of relevant european regulatory frameworks	The ENISA report on Cybersecurity Skills Development in the EU has already pointed out the need for a standardized approach regarding skills definition and a concrete plan for cybersecurity career management. Already some organizations (and local governments) have implemented some actions but coordination is needed to have a sustainable result. (The reason why we are linking the ENISA study is because Greece in not within the countries where specific developments on the subject are mentioned - unlike e.g. France showing a lack of specific framework) [31].
	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	Medium	18. Social Awareness	The ENISA report on Cybersecurity Skills Development in the EU has already pointed out the need for a standardized approach regarding skills definition and a concrete plan for cybersecurity career management. Already some organizations (and local governments) have implemented some actions but coordination is needed to have a sustainable result. (The reason why we are linking the ENISA study is because Greece in not within the countries where specific developments on the subject are mentioned - unlike e.g. France showing a lack of specific framework). This gap in knowledge and skills related to cybersecurity has been identified in the National cybersecurity strategy. The strategy contains specific actions to bridge

REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				the gap also for young graduates. (Action 5.Γ.1.) [33].
			5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	The national cybersecurity strategy for greece, contains within the strategic sectors for the review of the strategy (amongst others) the security and protection of privacy with an emphasis on the coordination to the personal data protection framework and the education and awareness. Page 17 of the strategy document [33].
			7. Economic incentives to enroll or upgrade cybersecurity education	The national cybersecurity strategy for Greece, contains within the strategic sectors for the review of the strategy (amongst others) the security and protection of privacy with an emphasis on the coordination to the personal data protection framework and the education and awareness. Page 17 of the strategy document [33].
E	30. Covid-19 pandemic crisis	High	10. Licensing costs and different licensing models of software used in cybersecurity education	The COVID-19 pandemic changed the business landscape for almost every organization, forcing them to abandon their business and strategic plans and to quickly implement secure mass connectivity on a massive scale for their human resources. Digital security teams and technicians also had to deal with growing threats to their cloud systems as hackers sought to take advantage of the pandemic: 71% of digital security professionals reported an increase in cyber threats from the beginning of quarantine. One of the few predictable things about cyber security is that hackers will always try to take advantage of events or changes - such as COVID-19 or the advent of 5G - for their own benefit. In order to stay protected, organizations and businesses must prevent and not leave systems unprotected or unattended, because they risk becoming the next victim of sophisticated and targeted attacks [29].
			15. Lack of dedicated curricula and training and no clear identification of skills	8. Update the European Digital Competence Framework32 with a view to including AI and data-related skills. Support the development of AI learning resources for schools, VET organizations, and other training providers. Raise awareness on the opportunities and challenges of AI for education and training. 9. Develop a European Digital Skills Certificate (EDSC) that may be recognized and accepted by governments, employers and other stakeholders across Europe. This would allow Europeans to indicate their level of digital competences, corresponding to the

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				Digital Competence Framework proficiency levels [30].
			12. Effects of digital economy on skills demand	The COVID-19 pandemic changed the business landscape for almost every organization, forcing them to abandon their business and strategic plans and to quickly implement secure mass connectivity on a massive scale for their human resources. Digital security teams and technicians also had to deal with growing threats to their cloud systems as hackers sought to take advantage of the pandemic: 71% of digital security professionals reported an increase in cyber threats from the beginning of quarantine. One of the few predictable things about cyber security is that hackers will always try to take advantage of events or changes - such as COVID-19 or the advent of 5G - for their own benefit. In order to stay protected, organizations and businesses must prevent and not leave systems unprotected or unattended, because they risk becoming the next victim of sophisticated and targeted attacks. Moreover, The COVID-19 crisis, which has heavily impacted education and training, has accelerated the change and provided a learning experience. According to the consultation, the COVID-19 crisis has led to the widespread use of digital learning practices in education and training across the EU. However, respondents from several Member States said that the difficult circumstances of the pandemic meant that this happened hastily and often in an unplanned manner. Measures put in place by Member States and institutions to ensure continuity of education ranged from televised lessons to online learning management systems to training using simulations. Approaches varied between and within countries, but also across levels and sectors of education and training. This reflected differing levels of digital maturity in different parts of the system. The main areas of concern for respondents were how to ensure access, equity and inclusion. They were worried about the emergence of digital divides. (we could not locate a national reference but the European is especially to the point) [30].
[1] Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinoudakis, C., Ioannidis, S. (2020) Cybersecurity in the Era of Digital Transformation: The case of Greece. IEEE international Conference on Internet of Things and Intelligent Applications (ITIA2020) , Zhenjiang, China, 27-29 November, 2020.				

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

[2] Felson, M. and Cohen, L.E., (1980) Human ecology and crime: A routine activity approach. Human Ecology, 8(4), pp.389-406.

[3] Harichandran, V.S., Breitinger, F., Baggili, I. and Marrington, A., (2016) Cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. Computers & Security, 57, pp.1-13.

[4] Papathanasiou, A., Papanikolaou, A., Vlachos, V., Chaikalis, K., Dimou, M., Karadimou, M. and Katsoula, V. (2013) Legal and social aspects of cybercrime in Greece. In International Conference on e-Democracy (pp. 153-164). Springer, Cham. Pease, K. (2001) Crime

[5] Fidler, D.P., Pregent, R. and Vandurme, A., (2013) NATO, Cyber defense, and international law. . John's J. Int'l & Comp. L., 4, p.1.

[6] Recommendations of the National Cyber Security Authority to companies for effective protection against cyber attacks (in Greek).

[7] Article in the financial newspaper Naftemporiki, available (in Greek) at: https://www.naftemporiki.gr/story/1658840/perissoteres-kubernoepitheseis-sxetikes-me-tin-covid-19-anamenontai-to-2021

[8] Rughiniş, C. and Rughiniş, R. (2014) Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. computers & security, 43, pp.111-125.

[9] Davies, L., (2004) The difference between child abuse and child protection could be you: Creating a community network of protective adults. Child Abuse Review, 13, 426- 432.
[10] Kierkegaard, S. (2008) Cybering, online grooming and ageplay. Computer Law & Security Review, 24(1), pp.41-55.

[11] Pratt, T.C., Holtfreter, K. and Reisig, M.D. (2010) Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency, 47(3), pp.267-296.

[12] Gupta, B.B., Tewari, A., Jain, A.K. and Agrawal, D.P. (2017) Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), pp.3629-3654.

[13] Obied, A. and Alhajj, R. (2009) Fraudulent and malicious sites on the web. Applied intelligence, 30(2), pp.112-120.

[14] Papanikolaou, A., Vlachos, V., Papathanasiou, A., Chaikalis, K., Dimou, M. and Karadimou, M. (2014a) A survey of cyber crime in Greece. Telfor Journal, 6(2), pp.86-91.

[15] Floros, G.D., Siomos, K.E., Fisoun, V., Dafouli, E. and Geroukalis, D. (2013) Adolescent online cyberbullying in Greece: The impact of parental online security practices, bonding, and online impulsiveness. Journal of School Health, 83(6), pp.445-453.

[16] Livingstone, S. and Smith, P.K. (2014) Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. Journal of child psychology and psychiatry, 55(6), pp.635-654.

[17] Fragkou, A. (2018) Greek Primary Educators' Perceptions of Strategies for Mitigating Cyber Child Exploitation. (Doctoral dissertation, Walden University).

[18] National Cybersecurity Authority (2020) National Cybersecurity Strategy 2020-2025, available at https://mindigital.gr/kyvernoasfaleia (in Greek), pg. 66.

[19] Theocharidou, M. and Gritzalis, D.(2009) Situational Crime Preventionand Insider Threat: Countermeasures and Ethical Considerations. In Proc. of the 8th International Computer Ethics Conference (pp. 808-820).

[20] National Cybersecurity Authority (2020) National Cybersecurity Strategy 2020-2025, available at https://mindigital.gr/kyvernoasfaleia (in Greek), pp. 43-45.

[21] Kitsios, F., Kamariotou, M., Fouliras, P. and Mavridis, I. (2018). National Cybersecurity Strategy: A Conceptual Framework for Greece, Proceedings of the11th International Conference for Entrepreneurship, Innovation and Regional Development (ICEIRD 2018), Doha, Qatar, pp. 99-105. Available at: https://www.iceird.eu/2018/wp-content/uploads/2018/12/ICEIRD2018_ProceedingsBook-Preview.pdf

[22] National Cybersecurity Authority (2020) National Cybersecurity Strategy 2020-2025, available at https://mindigital.gr/kyvernoasfaleia (in Greek), pg. 49.

[23] National Cybersecurity Authority (2020) National Cybersecurity Strategy 2020-2025, available at https://mindigital.gr/kyvernoasfaleia (in Greek), pp. 63-66.

[24] Maglaras L., G. Drivas, K. Noou & S. Rallis (2018) NIS directive: The case of Greece, EAI, 4:14

[25] Drivas G., L. Maglaras, H. Janicke and S. Ioannidis, "Assessing Cyber Security Threats and Risks in the Public Sector of Greece," Journal of Information Warfare, vol. 19, no. 1, 2020.

[26] National Cybersecurity Authority (2020) National Cybersecurity Strategy 2020-2025, available at https://mindigital.gr/kyvernoasfaleia (in Greek), pg. 62.

[27] National Cybersecurity Authority (2020) National Cybersecurity Strategy 2020-2025, available at https://mindigital.gr/kyvernoasfaleia (in Greek), pg. 63.

[28] National Cybersecurity Authority (2020) National Cybersecurity Strategy 2020-2025, available at https://mindigital.gr/kyvernoasfaleia (in Greek), pg. 61.

[29] Article in the financial newspaper Naftemporiki, available (in Greek) at: https://www.naftemporiki.gr/story/1658840/perissoteres-kubernoepitheseis-sxetikes-me-tin-covid-19-anamenontai-to-2021

[30] Brussels, 30.9.2020 COM(2020) 624 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Digital Education Action Plan 2021-2027 Resetting education and training for the digital age https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-624-F1-EN-MAIN-PART-1.PDF

[31] Cybersecurity Skills Development in the EU — ENISA (europa.eu)

[32] https://www.nationalcoalition.gov.gr/wp-content/uploads/2019/06/NC-Action-Plan-2019-FINAL.pdf, https://ec.europa.eu/digital-single-market/en/scoreboard/greece, https://mindigital.gr/wp-content/uploads/2020/12/%CE%95%CE%B8%CE%BD%CE%B9%CE%BA%CE%B7%CC%81-%CE%A3%CF%84%CF%81%CE%B1%CF%84%CE%B7%CE%B3%CE%B9%CE%BA%CE%B7%CC%81-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%B1%CC%81%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf

[33] Microsoft Word - ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ_6.12.2020.docx (mindigital.gr)

Table 18. Greece.

ANNEX 7. Hungary

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	2. Lack of coordination	Medium	4. Political ambition to create cooperation frameworks	[1]
	3. Vulnerabilities of the training systems / Skills shortage	Medium	13. Gender balance	Lack of women in cybersecurity specialization causes less specialists [2].
			14. Diversified workforce	Lack of minorities in cybersecurity specialization causes less specialists [3].
E	6. The economic impact of the European cybersecurity educational ecosystem	Medium	4. Political ambition to create cooperation frameworks	The lack of political willingness causes alck of of Universities teaching cyber security [4].
S	13. Gender balance	Low	16. Stereotypes and misconceptions of Cybersecurity	*Szekeres, Valéria, Erzsébet Takács, and Lilla Vicsek. "" Úristen! Te, lányként?!": a nemek kultúrája egy felsőoktatási intézmény műszaki karain: a hallgatónők szemszögéből." Társadalmi Nemek Tudománya Interdiszciplináris eFolyóirat 3.1 (2013): 125-144, http://tntefjournal.hu/vol3/iss1/szekeres_takacs_vicsek.pdf*
	18. Social Awareness	Medium	16. Stereotypes and misconceptions of Cybersecurity	Less people is atracted by engineering studies because of misconceptions [5].
T	19. Cyber Ranges	Medium	7. Economic incentives to enroll or upgrade cybersecurity education programs	Lack of economic incentives creates funding problems for new cyber ranges [6].
	20. Availability of Tools	High	7. Economic incentives to enroll or upgrade cybersecurity education programs	Lack of economic incentives creates funding problems for new tools and [6].
	21. Digitalization of Society	High	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	The digitalization of society without proper personal data protection mechanism endanger the citizens [7].
L	26. Personal data protection lack, knowledge gap of legal requirements concerning	Low	18. Social Awareness	Despite GDPR and other regulations the masses are not interested in privacy protection [8].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	matters closely related to cybersecurity			
E	30. Covid-19 pandemic crisis	Medium	18. Social Awareness	During the pandemic no real social awareness was given to security and privacy in spite of the heavy usage of telecommunication [9].

[1] Magyarország Nemzeti Kiberbiztonsági Stratégiája, National cybersecurity strategy of Hungary, 2013, http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845

[2] https://www.witsec.hu/hu

[3] FARKASMARIETTA, Cigány gyermekek útja a felsőoktatásig, az értelmiségivé válásig; SZVERLESZANDRAFelsőoktatás Magyarországon –Romák/cigányok a magyar felsőoktatásban; 2017, https://core.ac.uk/download/pdf/158266295.pdf

[4] Bányász Péter, A kiberbiztonsági képzés aktuális helyzete és fejlesztési lehetőségei a magyar felsőoktatásban, kiemelt tekintettel a Nemzeti Közszolgálati Egyetemre- Egy kutatás bemutatása, 2019, https://www.researchgate.net/publication/330716278_A_kiberbiztonsagi_kepzes_aktualis_helyzete_es_fejlesztesi_lehetosegei_a_magyar_felsooktatasban_kiemelt_tekintettel_a_Nemzeti_Kozszolgalati_Egyetemre-_Egy_kutatas_bemutatasa

[5] Devrenkár István, Csökkent a bejutási küszöb az informatikai szakokra. Gyorselemzés, 2020, https://bitport.hu/csokkent-a-bejutasi-kuszob-az-informatikai-szakokra-gyorselemzes

[6] Kovács László, Kiberbiztonság és -stratégia, 2018, http://kovacsx.hu/download/books/KovacsLaszlo_A_kiberbiztonsag_es_strategia.pdf

[7] Kovács Róbert, Az okos városkártyák, mint általános helyi azonosító eszközök személyiségi jogi és jogbiztonsági aspektusai, 2020, https://ajk.kre.hu/images/doc6/PR/A_digitalizacio_hatasa_az_egyes_jogteruleteken.pdf

[8] Társaság a szabadságjogokért, Milyen az adatvédelem helyzete ma Magyarországon?, 2017, https://www.liberties.eu/hu/stories/az-adatvedelem-helyzete-magyarorszagon/12909

[9] ESET, A koronavírus járvány okozta tömeges home office 5 legfontosabb kiberbiztonsági tanulsága, 2020, https://www.eset.com/hu/hirek/covid-19-legfontosabb-kiberbiztonsagi-tanulsaga-2020/

Table 19. Hungary.

ANNEX 8. Portugal

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	3. Vulnerabilities of the training systems / Skills shortage	High	5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	The national cybersecurity strategy has 6 actions. Action 2 is devoted to "Prevention, education and awareness". In this scope it addresses the issue of promoting careers in Cybersecurity within organizations and among students at all education levels [1].
			6. The economic impact of the European cybersecurity educational ecosystem	The national cybersecurity strategy has 6 actions. Action 2 is devoted to "Prevention, education and awareness". In this scope it addresses the issue of the failure to produce candidates by promoting Cybersecurity among students at all education levels [1].
	4. Political ambition to create cooperation frameworks	Medium	6. The economic impact of the European cybersecurity educational ecosystem	The goal of this initiative is to engage young students in the cybersecurity field and address the skills gap [2,3].
E	8. Economic impact of inadequate (national) cybersecurity capabilities	Low	2. Lack of coordination	[4].
S	13. Gender balance	Medium	16. Stereotypes and misconceptions of Cybersecurity	Addresses the possible effects of "Less interest in cybersecurity studies." [4,5,6,7].
	15. Lack of dedicated curricula and training and no clear identification of skills	Medium	16. Stereotypes and misconceptions of Cybersecurity	Addresses the possible effects of "Less interest in cybersecurity studies." [4,5,6,7].
	17. Social impact	Low	21. Digitalization of Society	[8,9].
			23. Generalization of cyber attack	[8,9].
	18. Social Awareness	Low	5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	This is one of the vectors of the National Cybersecurity strategy [1].
			21. Digitalization of Society	Everyone has multiple devices connected to the internet. And more often than not, users share devices for both personal and business use. In order to preserve security of organizations, basic security awareness is needed to separate the two environments. This addresses the possible effects of "Digitalization creates a need for universal

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

				security education for the masses, not only expert education." [1].
			30. Covid-19 pandemic crisis	Many organizations had to adapt their infrastructure to work remotely, which increased the attack surface of organizations. This addresses the possible effects of "The pandemic crisis increased the dependency on IT" [1].
T	19. Cyber Ranges	High	10. Licensing costs and different licensing models of software used in cybersecurity education	The solution at Técnico-Lisboa and CyberSecurity Challenge PT, relies solely on open-source technologies as a constraint identified as "Reluctance to incorporate COTS" [2,12].
			11. Economic costs of incompatible training platforms and cyber ranges	Difficulty in sharing of Scenarios due to non-uniform development. Addresses the possible effect "Duplicated effort" [2,12].
			20. Availability of Tools	Universities tend to develop their own learning environments to teach their courses [2,12].
	22. Emerging Technologies	Medium	7. Economic incentives to enroll or upgrade cybersecurity education programs	Funding of a doctoral program in an emergent research filed that may have significant impact in Cybersecurity (Quantum Computation) [13].
L	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	Low	21. Digitalization of Society	[14,15].
E	No identified aspects for Environmental Factor			

[1] National Cybersecurity Strategy - https://dre.pt/home/-/dre/122498962/details/maximized

[2] CyberSecurity Challenge PT - https://cybersecuritychallenge.pt/

[3] CyberSecurity Challenge PT - https://www.cncs.gov.pt/cyber-challenge/

[4] Relatório CiberSegurança em Portugal - Sociedade 2020 - https://www.cncs.gov.pt/content/files/relatorio_sociedade2020__observatoriocibersegurança_cncs.pdf (pages 99-110)

[5] Total students registered in the national higher education system by gender - https://www.pordata.pt/Portugal/Alunos+matriculados+no+ensino+superior+total+e+por+sexo-1048

[6] Percentage of students that are women among all students of a given subject - https://www.pordata.pt/Portugal/Alunos+do+sexo+feminino+em+percentagem+dos+matriculados+no+ensino+superior+total+e+por+%c3%a1rea+de+educa%c3%a7%c3%a3o+e+forma%c3%a7%c3%a3o+-1051-8512

[7] Total students registered in the national higher education system by subject - https://www.pordata.pt/Portugal/Alunos+matriculados+no+ensino+superior+total+e+por+%c3%a1rea+de+educa%c3%a7%c3%a3o+e+forma%c3%a7%c3%a3o-1026-8239

[8] Cidadão Ciberinformado - https://www.nau.edu.pt/curso/cidadao-ciberinformado/

[9] Consumidor Ciberseguro - https://www.nau.edu.pt/curso/consumidor-ciberseguro/

[10] Cidadão Ciberseguro - https://www.cncs.gov.pt/recursos/cidadao-ciberseguro/

[11] Curso Geral de Cibersegurança - https://www.cncs.gov.pt/atividades/curso-geral-de-ciberseguranca/

[12] https://scoreboard.ssof.rnl.tecnico.ulisboa.pt/

[13] Doctoral Programme in the Physics and Mathematics of Information (DP-PMI) at Instituto Superior Técnico (IST) - http://www.dp-pmi.org/structure.html

[14] Regulamento Geral de Protecção de Dados - https://dre.pt/pesquisa/-/search/123815982/details/maximized

[15] MSc in Information Security and Cyberspace Law - https://fenix.tecnico.ulisboa.pt/cursos/msidc

Table 20. Portugal.

Aspect name	Notes
3. Vulnerabilities of the training systems / Skills shortage	The national cybersecurity strategy has 6 actions. Action 2 is devoted to "Prevention, education and awareness" and aims at capacity development among organizations, professors, students at all education levels, and to promote general digital literacy among all citizens.
4. Political ambition to create cooperation frameworks	CyberSecurity Challenge PT is a joint initiative of the Portuguese National CyberSecurity Center (CNCS), Instituto Superior Técnico-Universidade de Lisboa (IST), Universidade do Porto (2 universities), and AP2SI (an association of cybersecurity professionals), that aims at selecting the top-10 Portuguese students that will each year represent Portugal in the European CyberSecurity Challenge organized by ENISA.
8. Economic impact of inadequate (national) cybersecurity capabilities	The data from [4] reveals that there are 636 students registered in CyberSecurity Courses at the BSc, MSc, or PhD level in Portugal out of the 34.5k registered in the areas of Sciences, Mathematics and Informatics (data from 2020), and 75 new graduates (data from 2020). This partially matches the possible effects of "(governments wanting to) know how many students enroll each year, how many graduates a course produces and possibly the types of jobs end up securing after obtaining the degree"
13. Gender balance	Gender Balance is an issue at the admission for Cybersecurity courses. Although [4] refers that there was an increase of 25% of new students in cybersecurity related courses (data of 2020 compared to 2019) only 10% of all registered students were women. [5] reports that 54% of the approximate 397k students in PT national higher education system are women, whereas [6] reports that women represent 43% among all students of Sciences, Mathematics and Informatics. Cybersecurity falls short of that number with just 10%.
15. Lack of dedicated curricula and training and no clear identification of skills	The data from [4] reveals that there are 636 students registered in CyberSecurity Courses at the BSc, MSc, or PhD level in Portugal out of the 34.5k registered in the areas of Sciences, Mathematics and Informatics [7] (data from 2020), and 75 new graduates (data from 2020). This matches

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	the identified possible effects of "Lack of applicants for cybersecurity degrees" and "Shortage of qualified cybersecurity professionals (quantitative issue)"
17. Social impact	The Portuguese CyberSecurity Center has developed several mini-courses to create awareness among citizens: fake news [8], and secure and safe online shopping [9] are among the actions developed to raise awareness among citizens.
18. Social Awareness	The Portuguese CyberSecurity Center has developed several mini-courses to create awareness among citizens: general practices [10], and generic organizational security [11] are among the actions developed to raise awareness among organizations and citizens.
19. Cyber Ranges	Due to the high-costs of training platforms, universities usually rely on open-source solutions. Although the platforms are usually free, the scenarios have to be developed by the users. At Técnico-Lisboa, we develop new content as part of our Software Security course [12], containerized in Docker containers, that we intend to open source and share with the academic community. Similarly for the CyberSecurity Challenge PT [2]
22. Emerging Technologies	A 2.2MEuro grant was put forward by the PT Science Foundation (FCT) to sponsor the Doctoral Program in the Physics and Mathematics of Information: Foundations of Future Information Technologies. The goal was to provide training in information sciences and technologies, and in particular new enabling technologies such as Quantum Computation, and Quantum Cryptography. The grant started in 2014 and aimed at funding 40 PhD students until 2022.
26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	The approved EU regulation GDPR [14] led to the creation of several professional courses to train the future DPOs. This also led to the creation of some cybersecurity courses that bridge the gap between Technological, Organizational, and Legal subjects such as the MSc in Information Security and Cyberspace Law jointly developed by Técnico-Lisboa, Law School of ULisboa, and the Naval School [15]

Table 21. Portugal Notes.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

ANNEX 9. Serbia

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	2. Lack of coordination	Medium	25. Legal framework unification lack	There is lack of systematic approach to different mechanisms - education, research, standardization etc [1,2].
			3. Vulnerabilities of the training systems / Skills shortage	[1,2].
	3. Vulnerabilities of the training systems / Skills shortage	High	5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Additional efforts are needed to build an educational system to decrease the skill shortage [1,2,3].
			27. Need for standardization of cybersecurity roles definition and cybersecurity skills across the EU	Clearly defined roles and pay grades can attract talent and reduce shortages [1,2,3].
	5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	Medium	3. Vulnerabilities of the training systems / Skills shortage	Right course development and standardization is needed raise the competitiveness of students graduating at the HEIs in Serbia [3].
			2. Lack of coordination	[3].
	4. Political ambition to create cooperation frameworks	High	2. Lack of coordination	The government needs to coordinate all the efforts especially involving collaboration between different parties. The strategy is the relevant mechanism to nurture this activities, but the real challenge is to execute successfully all the relevant activities [1,2].
			25. Legal framework unification lack	Aligned legal frameworks might foster the creation of cooperation frameworks [1,2].
E	6. The economic impact of the European cybersecurity educational ecosystem	Medium	3. Vulnerabilities of the training systems / Skills shortage	The skill shortage is not officially measured in Serbia, but there is an understanding on all levels that the there is a lack of relevant skill [1,2,3].
			5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	[1,2,3].
	7. Economic incentives to enroll or upgrade cybersecurity education programs	Medium	6. The economic impact of the European cybersecurity educational ecosystem	Without economic support there are no possibilities enhance the education programs. The ISSES project is a result of ERASMUS project funding and the Serbian Cybersecurity Challenge is sponsored by different parties [3,4,5].
			3. Vulnerabilities of the training systems / Skills shortage	The National CERT thanks to the donation of Norway established a national training cyber range [3,4,5].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			10. Licensing costs and different licensing models of software used in cybersecurity education	The licensing costs of high quality platform raise the costs of institutions which plan to introduce cybersecurity education programs [3,4,5].
	10. Licensing costs and different licensing models of software used in cybersecurity education	Medium	7. Economic incentives to enroll or upgrade cybersecurity education programs	Cyber exercise platforms as the most effective mechanisms in cyber education have very high price-tags. Without a donation the Serbian NCERT would not had resources to obtain a cyber range platform [5].
			19. Cyber Ranges	Ranges are not standardized, vendor lock-in is a significant challenge [5].
	12. Effects of digital economy on skills demand	Medium	3. Vulnerabilities of the training systems / Skills shortage	The Serbian Strategy for Development of Information Society focuses on development of digital services and enhancing the digital economy. The development of cybersecurity has to follow the development of the digital economy [1,2,6].
			5. Greater attention to policies dedicated to raise awareness of cybersecurity career paths	[1,2,6].
			21. Digitalization of Society	[1,2,6].
S	18. Social Awareness	High	8. Economic impact of inadequate (national) cybersecurity capabilities	Roundtables/panels should be organized to raise social awareness about the inadequate national cybersecurity capabilities [2].
			21. Digitalization of Society	A digital society has to be aware of the high importance of cybersecurity in its uninterrupted operation [2].
			31. Connected devices controlling environmentally sensitive productions	Lack of proper security controls can lead to environmental disasters or loss of human life [2].
	13. Gender balance	High	3. Vulnerabilities of the training systems / Skills shortage	Properly tackled gender balance in cybersecurity education can lower the skills shortage.
			8. Economic impact of inadequate (national) cybersecurity capabilities	Properly tackled gender balance in cybersecurity education can improve nation cybersecurity capabilities.
			16. Stereotypes and misconceptions of Cybersecurity	Gender balance can be attained if stereotypes and misconceptions about cybersecurity being a purely male and geeky job are erased.
T	19. Cyber Ranges	Medium	7. Economic incentives to enroll or upgrade	Cyber exercise platforms as the most effective mechanisms in cyber education have very high price-tags. Without a

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			cybersecurity education programs	donation the Serbian NCERT would not had resources to obtain a cyber range platform [5].
			20. Availability of Tools	[5].
			3. Vulnerabilities of the training systems / Skills shortage	[5].
	21. Digitalization of Society	Medium	12. Effects of digital economy on skills demand	The Serbian Strategy for Development of Information Society focuses on development of digital services and enhancing the digital economy. The development of cybersecurity has to follow the development of the digial economy [1,2,6].
			3. Vulnerabilities of the training systems / Skills shortage	A digital society is highly susceptible to disruption if it is not properly secured due to skills shortages [1,2,6].
L	24. European Certification lack	Medium	1. Lack of relevant European regulatory frameworks	Common regulatory frameworks would ease the creation of European certifications [2].
			15. Lack of dedicated curricula and training and no clear identification of skills	Certification programs would be aligned with skills needs and act as guidance to education providers towards creating unified curricula and training programs [2].
			7. Economic incentives to enroll or upgrade cybersecurity education programs	Inexpensive European certification programs would act as incentives to enroll in cybersecurity programs. They would act as well-defined milestones in a cybersecurity career [2].
E	No identified aspects for Environmental Factor			

[1] STRATEGY for the Development of Information Security in the Republic of Serbia for the period 2017-2020 (https://mtt.gov.rs/en/download/3/Strategy.pdf).

[2] STRATEGY DRAFT for the Development of Information Society and Information Security in the Republic of Serbia for the period 2021-2026

[3] Information Security Services Education in Serbia – ISSES (https://isses.etf.bg.ac.rs/about/)

[4] Serbian Cybersecurity Challenge (https://isses.etf.bg.ac.rs/events/serbian-cybersecurity-challenge-2020/)

[5] 1.2 Million Euros from the Kingdom of Norway for Strengthening Information Security of the Serbian Government (https://www.norveskazavas.org.rs/en/vtext/za-jacanje-informacione-bezbednosti-vlade-srbije-1-2-miliona-evra-od-kraljevine-norveske)

[6] STRATEGY for Development of Information Society till 2020. (https://mtt.gov.rs/download/3/Strategija_razvoja_informacionog_drustva_2020.pdf)

Table 22. Serbia.

ANNEX 10. Spain

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	1. Lack of relevant european regulatory frameworks	Medium	2. Lack of coordination	There is a lack of coordination that leads to the missing integration of intelligence levels, the technical, for immediate use to improve the protection of computer devices and their systems, and the geopolitical or strategic. This integration, in Spain has not occurred, as stated in [32]
			3. Vulnerabilities of the training systems / Skills shortage	There are not enough training programs and the training systems are not aligned with the National needs in terms of cybersecurity, leading to a lack of professionals, as stated in [33].
			25. Legal framework unification lack	There is a lack of unified legal framework [32,33].
E	No identified aspects for Economic Factor			
S	15. Lack of dedicated curricula and training and no clear identification of skills	Medium	22. Emerging Technologies	Constant technological change and emerging technologies place cybersecurity experts among the most needed profiles in Spain and with the greatest future [26]. Some regions of Spain are betting on creating specific training programs that include the actual needs of companies (skills to be trained) and new trends in cybersecurity [27].
			23. Generalization of cyber attack	Digitization has led to a generalization of cyberattacks, from unsophisticated attacks with great reach, to more elaborate attacks with specific targets. As mentioned in [28], Spain is the third most attractive country for cybercriminals after Germany and the United States of America. This fact fuels the need for cybersecurity experts and therefore quality, updated and available training that meets the lack of experts in the sector.
			16. Stereotypes and misconceptions of Cybersecurity	In many environments, cybersecurity continues to be perceived as an addition to other disciplines such as computer science or telematics. It is important and relevant that a specific curricula exists for training each of the cybersecurity profiles in the professional environment with the necessary skills to cover the increasing demand [29].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	13. Gender balance	High	14. Diversified workforce	As stated in [31], there is a huge need of cybersecurity experts personnel and that lack of trained people can be benefitted from a better gender balance in the sector. The percentage of women who work in cybersecurity is extremely low, standing at 11%, as shown in the report published by Women in Cybersecurity. However, the number of female leaders in the cybersecurity field is increasing, helping to ensure the success of the industry and its organizations. At the XII CCN Incident Response Capacity Conference (CCN-CERT), the ATENEA-Rooted room, created in honor of the security challenges platform of the same name, featured an opening technical module in which they participated some of the best women cybersecurity experts.
T	20. Availability of Tools	Medium	10. Licensing costs and different licensing models of software used in cybersecurity education	The cost of licenses and software for cybersecurity education is very varied and sometimes unaffordable. There are companies that have educational programs for their products with more affordable costs, but others do not make such difference in prices. It is possible to reach agreements for the transfer of equipment, software or tools from some suppliers when they are interested in training students with their products [5]. Better solutions for cybersecurity education are needed, offering free solutions for learning or low-cost solutions, similar to the INCIBE initiative for SMEs, companies and the self-employed [22].
	21. Digitalization of Society	Medium	17. Social impact	The digitization of all areas of society, in terms of work, communication between people and leisure, and including public and private sector, is an aspect that has impacted for a few years on the behavior of the population, their thoughts, daily choices, etc. Now, this digitalization could be one of the drivers for economic recovery and the establishment of a true European single digital market [23]. The most common attacks in the last year (and due to the COVID-19 pandemic) have been ransomware, phishing, information leaks and crypto jacking. This implies a great dependence on digitization with cybersecurity, they have to go hand in hand [24]. It is necessary to adequately train the professionals who must ensure the cybersecurity of the infrastructures of the companies that provide services to society, as well as the citizens who consume those services.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

			18. Social Awareness	The digitization of society is a process that began a few years ago, when technology enabled acceptable connectivity rates for end users, BYOD devices became available, and then Internet-based services proliferated. Currently, immersed in an intensification of this digitization, and even more so after the COVID-19 pandemic [25], the Spanish government confirms that there is not a great awareness of cybersecurity among citizens. A greater digitization gives rise to new threats and in greater numbers, which implies the need for greater cybersecurity awareness by society [24].
	19. Cyber Ranges	Medium	11. Economic costs of incompatible training platforms and cyber ranges	Most of the cyberranges and cyber virtual training environments are directly built and maintained by sector specific enterprises, being very tailored to the needs of that company. Hence, there is a lack of a market of cyberranges that can cover the needs of the enterprises and keep an infrastructure that can be maintained and service several different stakeholders.
			16. Stereotypes and misconceptions of Cybersecurity	There is still a lack of compromise and understanding of Cybersecurity in order to build the necessary infrastructures, such as Cyber Ranges to train cybersecurity personnel and prepared them with real-world environments and scenarios.
	22. Emerging Technologies	Medium	Effects of digital economy on skills demand	The changes on emerging technologies and new trends on managing IT and cybersecurity have a direct impact on the need of trained personnel expert on the new technologies [36].
			26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely related to cybersecurity	Emerging trends such as quantum computing has an impact on cryptography security and the personal data protection. There should be changes on legal requirements aligned to those technology changes in order to keep the same level of the current personal data protection regulation [36].
			7. Economic incentives to enroll or upgrade cybersecurity education programs	The constant rise of new technologies make difficult to the academia to prepare and maintain updated training and education programs. To constantly update and upgrade the training programs, economic incentives should be applied [36].
L	26. Personal data protection lack, knowledge gap of legal requirements concerning matters closely	Medium	16. Social - Stereotypes and misconceptions of Cybersecurity	Cybersecurity training is not only for experts or professionals who want to dedicate themselves to this sector [14]. It is important to start training the population from an early age [15] so that they are aware of the dangers and thus make known a discipline that needs to be more integrated with young people so that they choose it as a

- CYBERSECURITY SKILLS ALLIANCE
SION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	related to cybersecurity			future career (incentivize them to be trained as cybersecurity experts to cover the demands of the sector [16]).
			17. Social - Social impact	As explained in [17], ethics in the treatment of personal data collected and how it is protected respecting the GDPR, is important for society. A good application of the legal framework can lead to greater confidence of the population in companies [18]. On the other hand, Spain must improve with respect to the application of the GDPR (the biggest problem for Spanish companies is the lack of a legal basis in data processing), even though it is one of the countries with the greatest maturity in applying this regulation [19].
			18. Social - Social Awareness	In Spain and in other European countries, awareness of employees regarding cybersecurity is necessary for compliance with the GDPR. Each company is responsible for security incidents and can be sanctioned, so this social awareness of cybersecurity is improving at the worker level [20]. The cybersecurity of the systems, tools or procedures used is important, but the awareness of people is also a key factor [21].
	24. European Certification lack	Medium	20. Availability of Tools	There is a lack of tools that are certified against European standards and certifications. Moreover, Spain is specially sensitive to this factor because the cybersecurity infrastructures of the country are smaller compared to other countries [35]. It has given us the ability to be agile in adapting, but there is a need to compare and validate the cyberseucity of IT tools faster and following homogeneous processes that cannot lead to future vulnerabilities
			19. Cyber Ranges	There is a lack of homogeneity of cyberranges because there is a lack of certification schemes that allows cybersecurity personnel to be continuously adapted to the changes of the sector. It is difficult to prepare cyberranges that are aligned to the skills needed to be certified, when there is no homogenous certification at European level [35].
			15. Lack of dedicated curricula and training and no clear identification of skills	The lack of European certification on cybersecurity skills and competences lead to a lack of guidelines to develop a standardized cybersecurity dedicated curricula and training programs [35].

- CYBERSECURITY SKILLS ALLIANCE
SION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

E	30. Covid-19 pandemic crisis	High	15. Lack of dedicated curricula and training and no clear identification of skills	The COVID-19 pandemic has generalized and caused an increase in the use of the Internet to communicate, work [1], buy online [2], etc. This fact has caused an increase in different types of attacks [3], which will cause an increase in cybersecurity in Spain from 2021 [4]. More experts or people trained in cybersecurity will be needed and therefore there will be an increase in training. Currently, this training needs improvements in its curricula, applying methodologies more based on hands-on labs and with an approach to the industry to define the profiles with the necessary skills. Some institutions and universities [5] are already teaching based in this type of activities but it is necessary to continue improving.
			17. Social impact	During the COVID-19 pandemic, misinformation and fake news have had a huge impact on the Spanish population [6]. Social networks and other platforms have been used to collect information about the interests of the population and spread harmful or uncertain messages with the intention of harming the people, political groups and other collectives [7]. To solve this, more education and awareness is required (some advices of the national police department of Spain in [8]).
			18. Social Awareness	The number of attacks has increased during the COVID-19 pandemic [9]. Cyber attacks have targeted people (online fraud, phishing, etc.) [10]. The teleworking platforms used are not safe enough for teleworkers [11] and teleworkers do not have the necessary knowledge about cybersecurity risks [12]. It is necessary to raise awareness and educate the population with good practices and a minimum knowledge of cybersecurity [13] (for its daily operation on the Internet and social networks).

[1] El País Economía, "La incidencia del teletrabajo en España pasa del 5% al 34% durante la pandemia", https://cincodias.elpais.com/cincodias/2020/05/05/economia/1588694657_002760.html

[2] Europa Press, "Las compras online aumentan un 15% con la pandemia y los 'millennials' son los que más gastan", https://m.europapress.es/portaltic/sector/noticia-compras-online-aumentan-15-pandemia-millennials-son-mas-gastan-20210209115856.html

[3] COPE, "El CNI detecta un aumento "cuantitativo y cualitativo" de ciberataques durante la pandemia", https://www.cope.es/actualidad/espana/noticias/cni-detecta-aumento-cuantitativo-cualitativo-ciberataques-durante-pandemia-20201130_1022601

[4] Europa Press, "La ciberseguridad crecerá un 8,1% este año en España, superando los 1.324 millones de euros", https://www.europapress.es/economia/noticia-ciberseguridad-crecera-81-ano-espana-superando-1324-millones-euros-20210218163150.html

[5] Sánchez J, Mallorquí A, Briones A, Zaballos A, Corral G, "An Integral Pedagogical Strategy for Teaching and Learning IoT Cybersecurity. Sensors (Basel). 2020 Jul 17;20(14):3970. doi: 10.3390/s20143970

[6] We Live Security by ESET, "Fake news y sus riesgos en tiempos de COVID-19", https://www.welivesecurity.com/la-es/2020/07/02/fake-news-riesgos-covid-19/

[7] Openmind BBVA, "Infodemia: 'fake news' y COVID-19", https://www.bbvaopenmind.com/humanidades/comunicacion/infodemia-fake-news-y-covid-19/

[8] Escuela Andaluza de Salud Pública, "Fake news y bulos contra la seguridad y la salud durante la crisis del coronavirus", https://www.easp.es/web/coronavirusysaludpublica/fake-news-y-bulos-contra-la-seguridad-y-la-salud-durante-la-crisis-del-coronavirus/

[9] Europa Press, "El CNI avisa de más ciberataques en la pandemia: ciberespionaje por la vacuna, desinformación y ataques al teletrabajo", https://www.europapress.es/nacional/noticia-cni-avisa-mas-ciberataques-pandemia-ciberespionaje-vacuna-desinformacion-ataques-teletrabajo-20200917131233.html

[10] Diario ABC, "Los ciberataques más comunes durante la pandemia de coronavirus", https://www.abc.es/tecnologia/redes/abci-ciberataques-mas-comunes-durante-pandemia-coronavirus-202004080154_noticia.html

[11] IT User, "Más allá de Zoom, ¿son seguras plataformas como Webex, Slack o Trello?", https://www.ituser.es/seguridad/2020/04/mas-alla-de-zoom-son-seguras-plataformas-como-webex-slack-o-trello

[12] El Heraldo, "Teletrabajo y digitalización: los retos que la pandemia ha traído a la ciberseguridad", https://www.heraldo.es/branded/teletrabajo-y-digitalizacion-los-retos-que-la-pandemia-ha-traido-a-la-ciberseguridad/?autoref=true

[13] Reflexiones sobre la Sociedad Digital de Fernando Davara, "Teletrabajo en tiempos de pandemia; ciberseguridad de los trabajadores", https://fernandodavara.com/teletrabajo-ciberseguridad-de-los-trabajadores/

[14] Inforges - Seidor, "Educación en Ciberseguridad: ¿Estamos concienciados?", https://www.inforges.es/Blog/iblog/2017/10/24/educacion-en-ciberseguridad-estamos-concienciados

[15] Campus Internacional Ciberseguridad, "EDUCACIÓN EN CIBERSEGURIDAD", https://www.campusciberseguridad.com/blog/item/113-educacion-en-ciberseguridad

[16] El PAIS, "Se necesitan urgentemente expertos en ciberseguridad: ¿qué estudiar para ser uno de ellos?", https://elpais.com/economia/2019/01/14/actualidad/1547486152_048652.html

[17] FABIANO, Nicola; FABIANO, Studio Legale. Ethics and the Protection of Personal Data. paragraph, 2019, vol. 1, p. 3.

[18] SIRT, "Impacto de la GDPR en la ciberseguridad", https://www.sirt.com/2019/06/gdpr-impacto-ciberseguridad/

[19] ComputerWolrd, "España, el país que más multas acumula por incumplimiento de GDPR", https://www.computerworlduniversity.es/ciberseguridad/espana-el-pais-que-mas-multas-acumula-por-incumplimiento-de-gdpr

[20] MTP - Digital Bussiness Assurance, "Concienciar a los empleados, factor clave para el cumplimiento de la GDPR", https://www.mtp.es/blog/seguridad-informatica/concienciar-a-los-empleados-factor-clave-para-el-cumplimiento-de-la-gdpr

[21] Asociación Española para la Calidad (AEC), "La importancia de la concienciación en la seguridad de la información", https://dpd.aec.es/la-importancia-de-la-concienciacion-en-la-seguridad-de-la-informacion/

[22] INCIBE (Instituto Nacional de Ciberseguridad de España), "Herramientas de ciberseguridad", https://www.incibe.es/protege-tu-empresa/herramientas

[23] Confederación Española de Organizaciones Empresariales (CEOE), "Plan Digital 2020: La digitalización de la sociedad española", http://contenidos.ceoe.es/CEOE/var/pool/pdf/publications_docs-file-334-plan-digital-2020-la-digitalizacion-de-la-sociedad-espanola.pdf

[24] El Mundo, "No hay digitalización sin ciberseguridad", https://www.elmundo.es/promociones/actualidad-economica/native/2020/12/21te/index.html

[25] Bussiness Insider, "Por qué todavía hace falta concienciar en ciberseguridad en España", https://www.businessinsider.es/todavia-hace-falta-concienciar-ciberseguridad-espana-795955

[26] UNIR, "Los 10 perfiles emergentes con más futuro", https://www.unir.net/ingenieria/revista/los-10-perfiles-emergentes-con-mas-futuro

[27] NoticiasCyL, "Mejorar la formación en ciberseguridad para dar respuesta a los retos de la digitalización", https://www.noticiascyl.com/t/2638436/leon-sociedad-leon-mejorar-formacion-ciberseguridad-dar-respuesta-retos-digitalizacion

[28] Diario Abierto, "España es el tercer país más atractivo para los ciberdelincuentes", https://www.diarioabierto.es/536683

[29] Computing, "La digitalización 'de emergencia' incrementa la demanda de expertos en ciberseguridad, cloud architects y analytics", https://www.computing.es/seguridad/informes/1118793002501/digitalizacion-de-emergencia-incrementa-demanda-de-expertos-ciberseguridad-cloud-architects-y-analytics.1.html

[31] Conseguir talento en ciberseguridad, el gran reto de las organizaciones https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/7773-conseguir-talento-en-ciberseguridad-el-gran-reto-de-las-organizaciones.html

[32] El Mundo, "Un alto cargo del CNI advierte sobre la falta de expertos en ciberdefensa", https://www.elmundo.es/tecnologia/2017/09/15/59bbc5ba22601dbd638b45bc.html

[33] Business Insider, "España necesita más expertos en ciberseguridad, según alertan la ministra de Defensa y las grandes empresas", https://www.businessinsider.es/espana-necesita-formacion-jovenes-expertos-ciberseguridad-546487

[35] CyberEop, "NUEVOS DESAFÍOS DE CIBERSEGURIDAD PARA 2021", https://www.cybereop.com/blog/nuevos-desafios-ciberseguridad-2021.html

[36] itTrends, "Crecen las iniciativas para la formación en ciberseguridad", https://www.ittrends.es/seguridad/2019/03/crecen-las-iniciativas-para-la-formacion-en-ciberseguridad

Table 23. Spain.

ANNEX 11. Sweden

Factor group	Aspect name	Impor-tance	Linking with other aspect(s)	Justification of linking of aspects and its dependence
P	3. Vulnerabilities of the training systems / Skills shortage	Low	14. Diversified workforce	Skills shortage could negatively affect the diversity of work force [1].
	1. Lack of relevant european regulatory frameworks	Medium	20. Availability of Tools	Lack of standardization makes it difficult to develop tools [4].
E	12. Effects of digital economy on skills demand	High	21. Digitalization of Society	The two are tightly related, as the digitalization of the economy affects the demand for a variety of digital skills, increasing the shortage of personnel [1].
	10. Licensing costs and different licensing models of software used in cybersecurity education	Low	20. Availability of Tools	Availability of tools is tightly linked to their cost [1].
	11. Economic costs of incompatible training platforms and cyber ranges	Medium	19. Cyber Ranges	The ease of developing educational material depends to a large extent on the ability to use cyber ranges. Hence some form of standardization is beneficial [3].
S	13. Gender balance	Low	21. Digitalization of Society	Skills shortage could be addressed by improving gender balance, but digitalization of society may counteract [1].
T	20. Availability of Tools	Medium	23. Generalization of cyber attack	The generalization of cyber attack strategies makes it more challenging to create and maintain an adequate set of tools for training [1].
	22. Emerging Technologies	High	18. Social Awareness	Emerging technologies can redefine the threat landscape, and in lack of social awareness they are significant threat to society [2].
L	24. European Certification lack	Medium	1. Lack of relevant European regulatory frameworks	The two aspects seem to be very much related, they are overlapping [2].
	25. Legal framework unification lack	Medium	1. Lack of relevant European regulatory frameworks	Misalignment in national legislation makes it difficult for companies to operate across borders, which affects the job market [2].
E	No identified aspects for Environmental Factor			

[1] Swedish IT and Telecom industries, "The IT Competence Shortage", 2020 available at https://www.almega.se/app/uploads/sites/2/2020/12/ittelekomforetagen-it-kompetensbristen-2020-eng-online-version.pdf

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

[2] Legislation about critical infrastructure security (https://www.svenskforfattningssamling.se/doc/20181174.html) [3] Swedish national cyber range https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nationell-cyber-range-och-test-webb/ [4] Standardization within information security https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/standardisering-inom-informationssakerhet/

Table 24. Sweden.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union