REWIRE
CYBERSECURITY SKILLS ALLIANCE

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

REWIRE - Cybersecurity Skills Alliance

A New Vision for Europe

R5.4.1 Policy Recommendations

Title	R5.4.1 Policy Recommendations
Document description	2nd Policy Brief within R5.4.1
Nature	Public
Task	T5.4 Policy Recommendations
Status	Final
WP	WP5
Lead Partner	EfVET
Partners Involved	All
Date	20/10/2022

Revision history	Authors	Delivery date	Summary of changes and comments
Version 0.1	Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET)	01/07/2022	Initial structure of the Policy Brief and table of contents for partners' comments
Version 0.2	Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET), Petr Dzurenda (BUT), Manos Athanatos (TUC), Petros Portokalakis (TUC), Yianna Danidou (EUC), Remi Badonnel (UL-Telecom Nancy), Julia Sanchez (URL), Fotini Georga (HLSA), Giulia Meschino (EVTA), Apostolos Karras (Apiroplus), Regina Valutytė (MRU)	02/09/2022	Collection of inputs and contributions from REWIRE partners
Version 0.3	Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET)	20/09/2022	Draft for review from partners

Version 0.4	Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET), György Dán (KTH), Apostolos Karras (Apiroplus), Fotini Georga (HLSA)	05/10/2022	First complete draft after partners' feedback and comments
QA Review	Daiva Banaitè (EKT), Donata Judickaite (NRD CS)	13/10/2022	Quality Assurance Review
Final Version 1	Ainhoa Segurola Uli (EfVET), Valentina Chanina (EfVET)	20/10/2022	Final version after QA review

Disclaimer:

CONTENTS

CYBERSECURITY IS A CAREER OPTION

Addressing the lack of attractiveness of cybersecurity as a career path

Summary

The efforts made by the EU to make cybersecurity education attractive and a priority in the agenda are still not enough. Not only the numbers of cybersecurity students are low, but also there is a big skills gap between education and the industry. The REWIRE Cybersecurity Skills Strategy has identified the rebranding and promotion of cybersecurity as one of the most important priorities, based on a series of needs to be addressed. This Policy Brief analyses the lack of training courses on cybersecurity, as well as the unattractiveness of the field as a career option for students. Based on these factors, a series of policy guidelines and recommendations are suggested, such as the importance of raising awareness on cybersecurity among the general population or including cybersecurity in the academic curricula from early stages.

Key Points

- There is an existing inability to attract students into cybersecurity studies and also to produce skilled and prepared graduates
- Cybersecurity needs to be rebranded and promoted
- It is essential to raise awareness on cybersecurity and include it in the curricula at early stages
- Every person should have at least fundamental knowledge of cybersecurity

1. INTRODUCTION

Cybersecurity has been gaining importance in recent years and much work has been done to improve it, but much more remains to be done in the field.

Despite the efforts made by the European Union to increase the interest in cybersecurity education and skills and to make it a priority of the EU cybersecurity strategy [1], “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" [2].

Individuals over 18 years old have different ways to access cybersecurity education and training, such as Higher Education Academic Programs – examples can be found in ENISA's Cybersecurity Higher Education Database (CyberHEAD) platform [3] –, Professional Trainings, like the ones found in the CONCORDIA courses map 2.0 [4], or even self-taught through online courses.

For children and students under 18, however, the situation is different due to the lack of education resources in this area. For citizens in general, the resources are limited as well, and they are mostly focused on cyber safety.

It is at this point crucial to clarify the basic concepts concerning Cybersecurity Education. Cybersecurity [5] is the preservation of confidentiality, integrity, and availability of information in the cyberspace. In broad terms, cybersecurity education is envisaged to provide individuals information, knowledge, and skills to protect their information and that of their companies against the threats in cyberspace.

This means that a term that is related and falls within the cybersecurity domain is cyber safety or online safety, which refers to "protection of people, especially self" [6]. Cybersecurity education should, without doubt, encompass both subjects.

This Policy Brief will focus on how to improve the attractiveness of cybersecurity as a career.

2. THE REWIRE STRATEGY

2.1. Strategic Priorities

The REWIRE Cybersecurity Skills Strategy [7] determined three main priorities for the development of cybersecurity skills: transforming and repositioning (rebranding) cybersecurity; fostering integration of cybersecurity with business strategy; and improving cybersecurity skills development to be better structured and to be simplified.

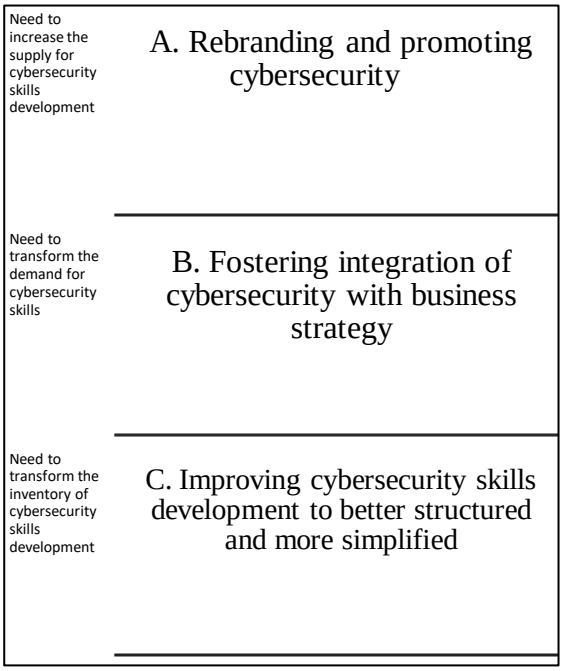

Figure 1. Priorities of the REWIRE Strategy.

Throughout this Policy Brief, we will focus our attention on the first of the abovementioned priorities – rebranding and promoting cybersecurity – driven by the lack of candidates for cybersecurity training, which leads to shortages and gaps in cybersecurity skills development.

The shortage of qualified cybersecurity professionals can only be addressed through an increase of the intake in the pipeline of individuals with the appropriate

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

skills to tackle emerging cyber security threats. Accordingly, the aim is to change the perception of cybersecurity as a field and as a career path, thus expanding cyber security horizontally.

The principal focus of repositioning cybersecurity is making it open and accessible rather than a closed area of high-level professionals only.

2.2. Strategic Needs

Rebranding and promoting cybersecurity are based on the strategic need of increasing the supply for cybersecurity skills development, composed of different factors:

- *Stereotypes and misconceptions of cybersecurity.* The Political, Economic, Social, Technological, Legal, and Environmental (PESTLE) analysis conducted by the REWIRE project has shown that cybersecurity education is often viewed as an add-on to computer science, the critical importance of its interdisciplinary nature is not realized by population in general [8]. The attitude that cybersecurity topics are mainly for experts after a relatively long career in the field prevails [2].
  This might prevent attempts to consider cybersecurity as a possible career path in life (for individuals starting their professional careers from scratch or for existing professionals).
  Persistent stereotypes about the cybersecurity sector being better suited for men stimulates the underrepresentation of women in cybersecurity [2]. A lack of diversity impacts the cybersecurity sector, since diversity fosters talent, representation, and fairness [2].
- *Limited visibility and public awareness of cybersecurity.* Almost everybody has heard of cybersecurity, however, the attitude and behaviour of persons do not reflect a high level of awareness [9]. An increased level of digitalisation of society increases the cybersecurity risks [2].
  The cybercrime victim-pool has in particular augmented due to home-based working [10]. Sophisticated actors and organized crime make use of disinformation techniques to distort public opinion [2]. This creates the need for universal cybersecurity education for the general public, not limited to expert education.
- *Poor awareness of cybersecurity as a career option*. Cybersecurity awareness campaigns are undoubtedly useful, however, cybersecurity as a life career path is not widely promoted [11]. Indeed, awareness campaigns still do not cover enough all relevant target groups in the society, including parents and teachers, who influence greatly the choice of a career paths at an early stage. The general need of cybersecurity campaigns targeted at wider audiences of the public is quite apparent.

3. LACK OF TRAINING RESOURCES

In the PESTLE Analysis [2], 31 aspects affecting cybersecurity education were

identified and defined. Moreover, a social network analysis approach was employed for the visualization of connections among aspects. This helped to reveal which aspects are connected across categories and to describe how they are mutually dependent.

Based on the analysis, four broader areas were found:

1. *Failure of stakeholders to cooperate*,
2. *Lack of a skills framework*,
3. *Lack of training resources*,
4. *Low level of societal interest in cybersecurity*.

The scope of this document will only consider the "lack of training resources", which encompasses the following aspects:

1. *Economic incentives for cybersecurity programs* (Economics aspect): a drop in interest has been reported for those courses that are considered academically challenging, such as engineering and computer science [12]. This has impacted cybersecurity education. It is therefore important to incentivize the enrollment of practitioners in cybersecurity programs.
2. *Licensing costs of cybersecurity education software* (Economics aspect): cybersecurity education often relies on the use of (online) platforms with licensing costs. However, these training providers often seek to maximize profitability aggravating the lack of skilled workforce by providing a financial barrier to entry [13].
3. *Economic costs of incompatible training platforms and cyber ranges* (Economics aspect): Online training platforms and cyber ranges are not designed to easily exchange exercises and scenarios [14]. Multiple teams invest in the development of scenarios that are equivalent but doing so is inefficient. There is a need for standardization and making interchangeable scenarios.
4. *Effects of digital economy on skills demand* (Economics aspect): The digital economy represents 22.5% of the world economy (2020) [15]. Cybersecurity is foundational to the digital economy and the shortage of skilled professionals will limit economic growth.
5. *Cyber ranges* (Technological aspect): Cyber ranges are important means of training groups of security professionals in the areas of ethical hacking and threat identification and response [16].
6. *Availability of tools* (Technological aspect): Hardware and software tools are essential for providing hands-on experience about the configuration and the potential vulnerabilities of software systems [17].
7. *Emerging technologies* (Technological aspect): there is a number of emerging technologies that have the potential to change the way computers and networks are operated and would require a redesign of current security curricula. Examples include quantum computing, machine learning, and cyber-physical systems.
8. *COVID-19 pandemic crisis* (Environmental aspect): due to the COVID-19 pandemic, quarantines

increased the necessity for IT and cybersecurity education to move online [18].

This group consists of 4 Economical, 2 Technological, and 1 Environmental aspects of the referred PESTLE analysis. It is important to notice that cybersecurity is the practice of protecting technology and therefore people in cyberspace. Trainings run on IT environments and the economy relies on IT developments. Accordingly, this can explain the main presence of economic and technological aspects in this group.

3.1. Consequences

Several consequences could be identified:

- A lack of incentives for cybersecurity programs can bring a public spending reduction on education. For instance, in Greece, 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.
- The licensing costs of cybersecurity education software platforms increase the training costs. In fact, 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.
- The incompatibility of training platforms and cyber ranges affects education providers investing in a training platform or cyber range disallowing an easy switch to a different solution provider. Moreover, they produce a duplicate effort of different education providers in developing new scenarios and training exercises that are the same. This duplicated effort could be easily eliminated if the scenarios were standardized and exchangeable.
- The lack of state-of-the-art cyber ranges makes it difficult to provide hands-on experience during education. Moreover, limited levels of automation in cyber ranges make education and training human labor intensive and hence expensive.
- The availability of tools, e.g., Virtual Labs, and sandbox environments, designed for the educational curriculum can help in achieving the learning objectives more efficiently than textbook-only education. Common virtualized training platforms would enable sharing of best experiences among education providers.
- The emergence of new technologies will increase the demand for the "Availability of Tools" aspect, as new hardware and software tools will be needed for state-of-the-art education. For instance, the emergence of economically feasible quantum computing would have a disruptive effect on software systems and would require the re-education of professionals.
- Cybersecurity education has moved mainly to online education due to the COVID-19 pandemic. This made it difficult to teach cybersecurity in topics that require the physical presence of students at school (e.g., topics related to

securing hardware devices). Moreover, the pandemic crisis increased the dependency on IT (especially remote and cloud services and tools) and thus their exposure to cyber-related threats.

4. THE MISCONCEPTIONS OF CYBERSECURITY AS A CAREER OPTION

Cybersecurity is overall a complex domain – including its educational aspect. In 2020, ENISA published a report named "Cybersecurity Skills Development in the EU", which focused on "the status of the cybersecurity education system and the inability to attract more students to study cybersecurity and to produce graduates with the right cybersecurity knowledge and skills" [19].

In a recent study by the Global Forum on Cyber Expertise (GFCE) [20], "within international and multi-national contexts, there is provision of cyber security education (through programmes, guidelines, and initiatives) within a pre-university context, notably within a European and European Union context. Although pre-university education is a priority (in the case of the ITU), the education available seems to have more of an online safety education focus, therefore being less complete for covering the wider range of cybersecurity topics".

ENISA's report mentioned above states that "education tends to focus on the reasons, the theory and the mechanisms behind the material", which leads to unqualified students in the eyes of the industry, due to a lack of hands-on experience [21].

Current material and activities designed for children are based on videos, books, activities on paper and a lot of theory. The above may be one of the reasons why surveys and reports indicate "a perceived general lack of interest and awareness among children in developing cyber skills and of cybersecurity as a potential career path" [6].

The difference between the effort and the resources invested in cyber safety, compared to the rest of the cybersecurity domain, could lead to the misconception that cybersecurity is just about keeping yourself safe while browsing, playing or otherwise interacting online and not as cybersecurity being a valid career choice.

5. POLICY GUIDELINES

The end goal is to ensure the understanding of cybersecurity as a comprehensive domain and a valid career choice for everyone. To achieve that goal, policies should be directed at different areas, such as improving or adding training resources or introducing cybersecurity at early stages of the education curriculum.

Resources should be introduced in realistic, practical, and suitable ways according to different ages, and focused on various threats (including the different exploitation and attack paths and methods and ways to protect against them).

Getting familiar with the cybersecurity field is one of the ways that could be useful to make cybersecurity field attractive to students. However, it is not the only one. To increase interest in cybersecurity, it is also important to raise awareness, and to

organize contests and competitions in cybersecurity.

As described before, the perception of cybersecurity work is often based on media stereotypes, misconception of the area as fully technological, and is lacking diversity [22]. Rebranding cybersecurity as an industry with a wealth of opportunities available to those willing to take the leap and thus fixing cybersecurity reputation is needed [23].

In summary, rebranding cybersecurity requires:

- Reviewing the current perception of cybersecurity;
- Collecting best practices of repositioning efforts of cybersecurity;
- Modifying the rebranding of cybersecurity concept at EU/regional level.

Having said that, we will now briefly present some policy options or actions to that could be further developed or taken as example to tackle the lack of training resources and make cybersecurity more attractive to students.

6. POLICY OPTIONS

Increase public awareness [24] Raising awareness on cybersecurity among citizens and students in general has been recognized as essential throughout the years. In fact, the largest number of initiatives collected in the first analysis carried out for the REWIRE Fiche I were precisely categorised as awareness-raising campaigns – 21,60% –, and awareness tools were also frequently found (See Table 1) [25].

Row Labels	Count of Activity or Action or Entity Present
Awareness campaigns	21,60%
Education, Training & Awareness Prioritization	17,90%
HE Courses	14,81%
Awareness Tools	13,58%
Establishment of a Cybersecurity Organization	7,41%
Dedicated training programs	6,79%
Bug Bounty Program	4,94%
Reporting illegal content tool	3,09%
Guide for Businesses	1,85%
Establishment of a Cybersecurity Awareness Portal	1,85%
Cybersecurity Awareness Portal	1,23%
Partnership between Academic World - Public Authorities - Private Sector	1,23%
Awareness app	1,23%
Teach the teachers	1,23%
Cybersecurity Exercises Tool	0,62%
Establishment of a Cybersecurity Awareness Center	0,62%
Grand Total	100,00%

Table 1. Percentage per category of the REWIRE Fiche I

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

Such activities will help to develop fundamental cybersecurity knowledge at all age levels, thus not only directly addressing cybersecurity skills capacity building, but also boosting visibility of cybersecurity as a career, which will result in increasing number of candidates for specialized cybersecurity training.

Introduce cybersecurity in early stages Dedicated efforts to promote cybersecurity for youngsters considering taking up new path in life and other target groups, that shape the choices of the youngsters. Early adoption of introduction to cybersecurity creates awareness of such career path even as just as a hypothetical one.

Students, starting from early ages, should be encouraged to engage in activities related to cybersecurity. They should be allowed to explore cybersecurity and take part in activities or events that would ignite their imagination and willingness to explore the field.

In addition, providing basic education on cybersecurity from early stages at primary school level could increase attractiveness and could improve skills in the field, as well as showing the students the importance of cybersecurity in a world dominated by digitization.

At primary and secondary levels, these strategies could focus on extracurricular activities, summer activities, *tehcnolabs* or similar activities. In Spain, for example, there exist similar initiatives focused on technology, such as TbKids - Emprendimiento tecnológico para niños y jóvenes (*TbKids - technology entrepreneurship for children and young people*) or TECNOLAB., that could be extended to the cybersecurity sector. A good example for how to do so is CyberSprinters (UK) or SPOOFY, a game that teaches children about the dangers of the Internet, behaving online and other topics related to smart devices.

An important aspect of this policy recommendation is to enhance and strengthen initiatives based on learning-by-doing, as the most effective way to engage young people.

At higher level education, workshops could be the best option for example for high school students. Such workshops could be given by university professors or cybersecurity professionals. Moreover, including a strong orientation service for students' future career at school would help them have a better understanding of the options available in cybersecurity.

Hold contests or competitions on cybersecurity Having children or students participating in competitions, games or events about cybersecurity not only would increase their knowledge in the field, but also make them more attracted to it. Events of such nature could be organised at national, regional, EU or international levels.

Several countries hold national cybersecurity competitions already, such as the United Kingdom's CyberCenturion. This is a free to enter cybersecurity competition where teams participate in a series of three online rounds in pursuit of a place in the National Finals, attempting to discover all the security vulnerabilities within various operating systems.

At European level, for example, there is the European Cyber Security Challenge [26]. These kind of events and challenges let students discover and learn new skills in the cybersecurity domain, as well as having

fun and exchanging ideas. However, they are intended to students between 15-25 years old, thus, it is necessary to promote similar activities among children at a younger age. For instance, local competitions could be held accompanied with bootcamps that would allow children to participate, learn and compete in an interactive and safe environment.

Other examples of the nature of the competitions or events that could serve to increase the attractiveness of students are:

- Capture the Flag or Cyber War games that integrate both technical (identification of vulnerabilities on computer systems, protection of networked infrastructures) and organisational aspects (crisis management).
- Hackathon events, mixing students and industrial partners on specific topics, such as analysing how and to what extent to apply security recommendations on industrial systems.
- Cyber escape fames, based on common security vulnerabilities.
- Bug bounty programs that may be offered by software editors, developing and encouraging hacking clubs in engineering schools and universities.

Ensure funding for cybersecurity education and training Programs at regional or national level focused on cybersecurity issues should be enhanced by education providers and authorities.

Moreover, it must be ensured that entry possibilities are accessible and individuals taking this step would be supported. Adequate funding for pursuing cybersecurity specialized studies, at least in formal education, including micro credentials, must be ensured.

Promote reskilling, upskilling and self-education on cybersecurity When tackling the workforce gap in cybersecurity, traditional education system is not the only way. Vocational education and training (VET), lifetime learning, and other ways need to be considered as well, and include them in the curricula.

In fact, the 2021 Cybersecurity Workforce Study of (ISC)^2 stated that although having an IT background is yet the most common pathway into cybersecurity, "slightly more than half of cybersecurity professionals got their start outside of IT" [27]. For example, 15% answered that they studied cybersecurity concepts on their own.

Reskilling and upskilling, thus, need to be considered and enhanced. Regarding self-education, it might present some concerns to be addressed as well, such as recognition or certification of the knowledge and skills acquired. Nevertheless, all education possibilities should be considered to enhance access into the cybersecurity sector.

Promote cybersecurity in higher education Revisiting cybersecurity as a discipline for studies and including it in the curricula of all study fields of education will become essential, since fundamental cybersecurity knowledge is increasingly expected from any potential employee.

On the one hand, it contributes to expanding cybersecurity horizontally and increases general cyber safety; on the other hand, it widens life-long-learning opportunities in the field of cybersecurity. Although it can be a small improvement at a time, it has the potential to encourage

people at least to consider cybersecurity as a career. Each discipline has its own specifics; thus, cybersecurity should be adjusted to correspond to most relevant vulnerabilities of a particular discipline and to deal with attack vectors most likely to be used in it.

Promote gender diversity in cybersecurity The under-representation of women in the cybersecurity sector is not an exception; it is something that can also be seen in various STEM sectors. According to Cybersecurity Ventures, "women held 25 percent of cybersecurity jobs globally in 2021" [28]. Thus, this by itself shows the importance of promoting gender diversity and the participation of women in cybersecurity, and in IT or tech overall (where the percentage of working women in the sector is of 24%) [29] even if over the years the numbers have increased.

This is a wide topic that requires even more research, however, misrepresentation of women in cybersecurity is detrimental because, among other reasons, cybersecurity skills and shortage already exist, but the situation worsens if there is no gender balance due to the lack of people joining the field. Therefore, promoting gender diversity and having different perspectives is needed and very valuable.

Just to give few examples, CONCORDIA and Women4Cyber [30] organised a workshop in 2019 to prepare a Manifesto aiming at raising and increasing awareness and promoting positive role models [31].

At an international level, the Tennessee Tech University started WiCyS [32], which has turned into an organization that represents a leading alliance between academia, government, and industry institutions.

7. CONCLUSION

Despite the efforts made by different actors at European and national levels, cybersecurity is somehow still not an option for young people to study. In addition, there is a clear cybersecurity skills gap and shortage around the world.

Up to this point, understanding that every person should have at least fundamental knowledge of cybersecurity is crucial to lessen or ameliorate the situation.

As we have seen, the cybersecurity education opportunities available are lagging or, at least, they do not cover the multiple skills required by industry and focus on a specific aspect of the cybersecurity field. Moreover, these training and studying opportunities are mainly targeted to university students or professionals, leaving out children.

Therefore, some policy options have been exposed in this document, with which we expect to obtain the following results:

- *Rebranding of cybersecurity* as reachable, valuable and attractive career;
- *Making it easier to enter the cybersecurity area for people from unrelated backgrounds*. Perception of accessibility of cybersecurity is expected to be higher;
- *Bringing diversity to cybersecurity, addressing gender gap issues*. In 2018, considering upper secondary and tertiary education, girls and women were still under-represented in this field, accounting for only 17% of all ICT students in the EU [33]. Promoting cybersecurity and motivating girls

and women to join this field is a promising solution to involve more talents and thus fill cybersecurity specialists' gap;

- *Increasing variety of specialists involved in the field of cybersecurity*. Horizontal expansion of cybersecurity, non-related fields specialists' inclusion in cybersecurity expands cybersecurity horizontally and increases general cyber safety.

8. REFERENCES

[1] European Commission (2020). The EU's Cybersecurity Strategy for the Digital Decade. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

[2] REWIRE (2022). WP2 PESTLE Analysis of Cybersecurity Education. https://rewireproject.eu/wp-content/uploads/2022/04/R2.1.1-PESTLE-analysis-results_FINAL-v1.1_compressed.pdf

[3] ENISA. Cybersecurity Higher Education Database (CyberHEAD). https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/

[4] CONCORDIA (2021). CONCORDIA Map 2.0. https://www.concordia-h2020.eu/map-courses-cyber-professionals/

[5] International Organization for Standarization (ISO) (2012). *ISO/IEC 27032:2012 Information Technology – Security Ttechniques – Guidelines for cybersecurity.* https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

[6] Waldock, K. E., Miller, V., Li, S., Franqueira, V. (2022). *Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people.* Global Forum on Cyber Expertise (GFCE) and the University of Kent. https://thegfce.org/wp-content/uploads/2022/08/GFCE-report-20220731.pdf

[7] REWIRE (2022). WP2 Cybersecurity Skills Strategy. https://rewireproject.eu/wp-content/uploads/2022/05/R2.3.1-Cybersecurity-Skills-Strategy_FINAL-v1-compressed.pdf

[8] ECSO, Gaps in European Cyber Education and Professional Training, 2018, Cited by REWIRE, PESTLE […], p. 20. Also, ENISA (2021), *Addressing skills shortage and gap through higher education*. https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education.

[9] de Bruijn, H., Janssen, M.: Building cybersecurity awareness. Government Information Quarterly 34(1), 1–7 (2017), https://doi.org/10.1016/j.giq.2017.02.007, Cited by REWIRE, PESTLE [...].

[10] UNODC Cybercrime and Anti-Money Laundering Section (2020). *Cybercrime and Covid-19: Risks and Responses*. https://www.unodc.org/documents/Advocacy-Section/EN_-_UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf, accessed on 27/03/2022. See also PESTLE analysis, p. 27.

[11] ENISA (2020). Cybersecurity Education. https://www.enisa.europa.eu/topics/cybersecurity-education, Cited by REWIRE, PESTLE analysis results, p.13.

[12] European Statistical System (ESS) (2020). https://ec.europa.eu/eurostat/

[13] Ukwandu, E., Ben Farah, M.A., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtazis, C., Bures, M., Andonovic, I., Bellekens, X. (2020). *A Review of Cyber-Ranges and Test-Beds.* https://doi.org/10.3390/s20247148

[14] Urias, V., Stout, W., Van Leeuwen, B., Lin, H. (2018). *Cyberrange infrastructure limitations and needs of tomorrow: A position paper*. International Carnahan Conference on Security Technology (ICCST). IEEE, 1–5.

[15] Abbosh, O. & Bissell, K. (2019). *Securing the Digital Economy*. https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf
[16] ECSO WG5. *Understanding Cyber Ranges: From Hype to Reality.* https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf
[17] 021. Rootme. https://www.root-me.org/
[18] Styles, J. (2020). *The unseen COVID-19 ripple effect: Security misconfiguration risk.* https://www.securityinfowatch.com/covid-19/article/21137323/the-unseen-covid19-ripple-effect-security-misconfiguration-risk
[19] ENISA (2020). *Cybersecurity Skills Development in the EU.* https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[20] Global Forum on Cyber Expertise. https://thegfce.org/
[21] Conklin, W. A., Cline, R. E., Roosa T (2014). *Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors*. 47th Hawaii International Conference on System Sciences, 2014, pp. 2006-2014. Retrieved from https://www.computer.org/csdl/proceedings/hicss/2014/2504/00/2504c006.pdf
[22] ISC2, 'How Views on Cybersecurity Professionals Are Changing and What Hiring Organizations Need to Know. The 2020 (ISC) Cybersecurity Perception Study', 2020, https://www.isc2.org/-/media/ISC2/Research/2020/Perception-Study/2020ISC2CybersecurityPerceptionStudy.ashx?la=en&hash=DC18089BF1D88460E1697A76BBEB5185A504D10C, accessed on 19/03/2022.
[23] Rizkallah, J., 'Rebranding Cybersecurity', Forbes, https://www.forbes.com/sites/forbestechcouncil/2018/06/27/rebranding-cybersecurity/?sh=88e9fb11686e, accessed on 28/03/2022.
[24] ENISA (2021) Raising Awareness of Cybersecurity. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity
[25] REWIRE (2022) WP5 5.3.1 REWIRE Fiche I. https://rewireproject.eu/wp-content/uploads/2022/05/R5.3.1-REWIRE-Fiches-I_FINAL-2.pdf
[26] ENISA. European Cyber Security Challenge. https://ecsc.eu/
[27] ECSO. *Unlocking our potential: Cybersecurity education and workforce needs in Europe*. https://ecs-org.eu/newsroom/unlocking-our-potential-cybersecurity-education-and-workforce-needs-in-europe
[28] Cybersecurity Ventures (2021). *Women In Cybersecurity Resource Center.* Sponsored by Deloitte Cyber. https://cybersecurityventures.com/women-in-cybersecurity/
[29] Cveticanin, N (2022). *Women in Tech Statistics: Girls Get Tech*. https://dataprot.net/statistics/women-in-tech-statistics/#:~:text=Women%20in%20tech%20statistics%20shed,gap%20in%20the%20technology%20business.&text=Only%2024%25%20of%20computing%20jobs,45%25%20higher%20rate%20than%20men.
[30] ECSO. Women4Cyber. https://women4cyber.eu/
[31] CONCORDIA (2019). *Women in Cyber – Manifesto for today.* https://www.concordia-h2020.eu/wp-content/uploads/2019/09/WomenInCyberMANIFESTO.pdf
[32] Tennessee Tech University (2013). WiCyS. https://www.wicys.org/

[33] Eurostat, 'Girls and women among ICT students: what do we know?', https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20200423-1, 2020, accessed on 19/03/2022.

9. LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/ Definition
CyberHEAD	Cybersecurity Higher Education Database
CONCORDIA	Cyber security cOmpeteNCe fOr Research anD InnovAtion
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
GFCE	Global Forum on Cyber Expertise
INCIBE	Instituto Nacional de Ciberseguridad de España (Spanish National Institute of Cybersecurity)
ITU	International Technological University
UK	United Kingdom

Table 2. List of abbreviations and acronyms

10. LIST OF FIGURES

11. LIST OF TABLES