REWIRE
CYBERSECURITY SKILLS ALLIANCE

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

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R.5.4.1 Policy Recommendations

Cyber Equality Now: Tackling Gender Disparities in the European Cybersecurity Landscape

Title	R5.4.1 Policy Recommendations
Document description	The present deliverable consists of a policy brief that delves into the underrepresentation of women in the cybersecurity sector, examining the barriers hindering their entry and advancement. It outlines solutions to encourage women's participation in cybersecurity and advance gender equality. Through the provision of insights, data, and actionable recommendations, the brief aims to inspire collective action among stakeholders to actively contribute to narrowing the gender gap and nurturing diversity and inclusivity in cybersecurity.
Nature	Public
Task	T.5.4 Policy recommendations – 4th Policy Brief within R5.4.1
Status	Final
WP	WP5
Lead Partner	EVTA
Partners Involved	All
Date	25/10/2023

Disclaimer:

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

EXECUTIVE SUMMARY

The rising threats of cybersecurity breaches, coupled with shortage of skilled cybersecurity professionals is a pressing concern in our increasingly digitalized society. A potential remedy for this shortage is to actively engage and encourage greater participation of women and gender-diverse individuals in the cybersecurity field. The REWIRE Pestle Analysis highlighted the importance of addressing gender disparities within the cybersecurity sector as a means to mitigate the growing skills shortage and enhance the protection of European digital society, economy and democracy. Based on the literature review, this policy brief explores why women are disproportionally represented in cybersecurity. It identifies barriers deterring them from pursuing a cyber career and provides solutions for encouraging women's participation in cybersecurity and advancing gender equality in the sector. It also highlights the ongoing initiatives within the cybersecurity industry that are designed to promote gender inclusivity. Its actionable recommendations point towards the importance of incorporating a gender perspective in cybersecurity education and workplace practices. They encompass actions to effectively address gender disparities, ranging from educational reforms and recruitment practices to creating gender-inclusive work environments and policy-making processes. By offering insights, data, and practical steps, this brief seeks to inspire collective action among stakeholders to actively contribute to closing the gender gap and promoting diversity and inclusivity within the industry.

Highlights

- Gender norms and stereotypes represent significant barriers to realizing gender equality in cybersecurity industry.
- Disparities in representation, promotion and compensation make retaining women a challenge for the cybersecurity sector.
- The underrepresentation of women in the cybersecurity sector significantly contributes to the skills shortage in the industry and sustains an imbalanced workforce that lacks the varied viewpoints and necessary skills to effectively address the ever-evolving landscape of cyber threats.
- There is need to address societal norms, cultural conventions and institutional policies that uphold gender prejudices and obstacles that hinder women's engagement in cybersecurity field.
- Gender equality within cybersecurity is critical not only for addressing the talent shortages of cybersecurity professionals but also for enforcing human rights and fostering a safer online environment for everyone.

1. INTRODUCTION

The importance of cybersecurity has been increasing rapidly in the past few years; all the while threats are constantly evolving. At the same time, the labour market does not have enough skilled cybersecurity professionals to meet industrial needs. The 2022 (ISC^2) cybersecurity workforce study estimated that there is a shortage of 260 000 cybersecurity professionals in Europe, a 57 % increase over 2021. While the underrepresentation of women in the cybersecurity sector has been widely noted , there are no sufficient data available about the gender composition of the EU's cybersecurity workforce, women's experiences or the professional role profiles they are filling. The underlying causes for low level of participation of women in the sector are complex and reflect how structural barriers prevent women's participation and progression in the cybersecurity field. Structural discrimination, wage inequalities, harmful gender stereotypes, and gender bias in organizational decision-making and practices are only some of the main factors that drive women away from pursuing cybersecurity careers.

In an era marked by the proliferation and variety of cyberattacks, it becomes crucial to reconsider social and cultural barriers preventing women from getting involved in cybersecurity jobs. The advantages brought by a diverse workforce, encompassing a broader array of skillsets, unique perspectives, varied lived experiences, enhanced innovative thinking and effective problem solving, constitute an opportunity that the cybersecurity industry shall capitalize on. The approaches to attain gender equality are not straightforward. Elevating women's involvement in the field requires comprehensive strategy among key actors due to the complexity and interconnected nature of the challenges involved.

Achieving gender equality in cybersecurity is not a task that can be effectively tackled in isolation; rather it requires a collective approach involving governments, academic institutions, the private sector, non-profit organizations, professional and trade associations. This is crucial because gender inequalities are deeply intertwined with cultural norms, biases, and systemic barriers. This policy brief calls attention to the prevailing gender disparities in the cybersecurity sector. It emphasizes the importance of addressing these disparities and provides insights into the root causes and potential solutions. The document seeks to serve as a comprehensive resource that informs and motivates stakeholders to take concerted steps towards achieving gender equality in the cybersecurity industry. By fostering inclusivity and diversity, the industry can tap into a wider pool of talent and perspectives, ultimately bolstering its ability to combat evolving cyber threats.

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. CURRENT LANDSCAPE OF GENDER DISPARITIES IN CYBERSECURITY

Despite the growing demand for cybersecurity professionals, women remain vastly underrepresented in the field of cybersecurity. There are significantly lower proportions of females in the EU's cybersecurity workforce than in the total labour force. Recent research carried out by ENISA (Nurse et al, 2021) indicates that only 20 % of students enrolled in cybersecurity-related programs in Europe in 2020 were women. Still, science, technology, engineering and mathematics (STEM) professions are persistently dominated by men, with women constituting only around 35 % of higher graduates in STEM-related disciplines (European Commission, 2022) and the gap increases for doctoral and full professorship positions. The increased importance of the ICT sector and rapid growth in ICT positions, especially during the pandemic years seem to have affected positively mainly men. According to the She Figures study (European Commission, 2021), women represent only 20% of ICT graduates and only 17 % hold tech sector jobs. When looking at the share among ICT specialists in 2021, only around 19 % of all ICT specialists in Europe were women. Data obtained from LinkedIn reveal that the gender gap in the cybersecurity workforce is also considerable. This gender imbalance is mostly pronounced in Poland, where only 13 % of the cybersecurity workforce comprises women, while Italy has the lowest disparity, with women constituting 25 % of the cyber workforce (Microsoft Corporate, 2022). The gender gaps in salaries and upper-level positions are remarkably high, as more than half of the cybersecurity positions held by women worldwide are entry-level and non-managerial (Reed et al., 2017).

Globally, men are four times more likely to be in executive positions in the cybersecurity industry and nine times more likely to occupy be in managerial positions (Ibid, p.7). The $(ISC)^2$ 2019 Cybersecurity Workforce Study has found a significant gender pay gap of approximately 21%, showcasing that women earn around one-fifth less than men in the cybersecurity field. This was again confirmed in the 2020 Cybersecurity Workforce Study, which showed that women of all experience levels receive notably lower compensation compared to their male colleagues on a global scale. Furthermore, women working within the cybersecurity sector encounter systemic bias, on-the-job discrimination, occupational segregation and wage inequality (Reed et al., 2017 & ISC^2, 2022). These might deter many young women from pursuing careers in cybersecurity and contribute to the phenomenon known as the leaky pipeline.

This underrepresentation is particularly pronounced in leadership roles and technical positions, areas that play a pivotal role in shaping the industry trajectory. The higher cybersecurity positions are less diverse in terms of representation of women and minoritized groups (ISC^2, 2022). Concerning education, globally, women enter the cybersecurity profession with higher education levels than men. Nevertheless, most of the Higher Education Institutions (HEIs) cybersecurity-related programs in Europe have significantly low levels of gender diversity (Nurse et al, 2021), with fewer female student graduates amounting to 18 % of the overall population in 2020. The gender dimension of the cybersecurity skills gap in Europe remains insufficiently explored by available research. Additionally, there is little

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

information about the representation of gender minorities in the EU's cybersecurity student population and workforce.

Current research and the EU's policy framework adopt a binary understanding of gender identity, calling for more studies to understand the experience of gender-diverse people in cybersecurity. Gender disparities are also manifested in the design and enactment of cybersecurity policies, with women and gender minorities being poorly represented in policy formulation process and norm-making (Millar et al., 2021). As highlighted by the United Nations, there is an increasing need to strengthen women's leadership and meaningful participation in cyber-related legislation, cyber diplomacy and governance bodies of cybersecurity decision-making organizations. Moreover, a growing body of research has demonstrated how gender-blind conceptualization of technical and policy aspects of cybersecurity exacerbate gender inequalities. For instance, the study of Slupska (2019) shows how masculine biases inform cybersecurity technology design, uncovering a tendency for smart home threat analyses to overlook gendered technology-facilitated security issues like intimate-partner violence. Feminist studies (Millar et al., 2021) consistently highlight that technologies developed without considering the needs and perspectives of women inadvertently perpetuate biases and discrimination. Additionally, male bias persists in the community of editors who manage scientific journals and conferences in the computer sciences, leading to unequal visibility and participation of women in cybersecurity research and careers (Bıçakcı & Evren, 2022).

The consequences of these disparities are far-reaching. According to Harvard Business Review (2013), diversity can unlock innovation and drives market growth. More specifically, companies characterized by inherent and acquired diversity, referred as 2-D diversity, tend to outshine their counterparts in terms of innovation and performance. Employees at these companies are 45% more inclined to report that their firm's market share grew over the previous year and 70% likelier to report that the firm captured a new market (Hewlett, Marshall & Sherbin, 2013). Hence, a lack of diversity within the cybersecurity sector limits the range of perspectives and approaches when addressing complex cybersecurity challenges. It also hampers innovation and problem-solving, which are essential in a field that constantly battles evolving threats. Without a diverse perspective, the industry is prone to overlooking certain risks or fail to anticipate new attack vectors, resulting in reduced overall cyber resilience. Also, the existing gender disparities in cybersecurity lead to substantial underutilization of talent and missed economic potential.

3. THE ROOTS OF GENDER DISPARITIES IN THE CYBERSECURITY SECTOR

The gender disparities within the cybersecurity domain are not isolated occurrences; rather they are the result of a complex interplay of socio-cultural and structural factors that have shaped the landscape of the industry. The reviewed literature reveals several root causes that contribute to the underrepresentation of women in cybersecurity. These root causes manifest at various stages of education, career progression, and workplace environments, perpetuating a cycle of gender imbalance.

Despite the context-specific nature of gender disparities, it is commonly argued that one of the main causes of cyber inequalities are prevailing gender norms and stereotypical beliefs that prevent women from accessing cybersecurity education and jobs. For instance, the widely shared perception of cybersecurity as a highly technical and male-dominated area disincentivizes women from entering the field. Research (Makarova et al., 2013 & Sultan et al, 2018) suggests that girls are discouraged from pursuing technology-related subjects from an early age due to social expectations. Dominant socio-cultural conceptions that construct technology and security as inherently masculine domains result in a low number of women in the cybersecurity workforce. The common social misperception that cybersecurity entails merely technical qualifications influences interests, beliefs, attitudes, and decisions. Misconceptions and stereotypes drive women away from the industry, though the reality is that cyber work is not only about technology but it also is equally about the impact on people (Gracia & Weingarten 2015). Gender stereotypes are often reinforced by media and education establishments, which gender cybersecurity as inherently masculine and detrimental to women, instilling a sense of non-belongingness in the industry (Lihammer & Hagman, 2021). The media portrayals of hackers and cybersecurity experts as male geniuses or lone wolves reinforce the stereotype that cybersecurity is a male-dominated field, making it difficult for women to envision themselves in such roles.

Other reasons attributed to gender asymmetry in cybersecurity include unequal access to digital technologies, limited familial and school encouragement to enter the cybersecurity industry, individual and family level financial constraints and low perceived level of self-efficacy to accomplish a task. Social environments influence women's personal beliefs and perceptions concerning cybersecurity leading to lower perceived levels of self-efficacy, which results in them not selecting the cybersecurity sector as a career (Zacharias et al., 2020). Past studies have revealed how parent's gender prejudices influence children's perception of their own skills, impairing self-efficacy in STEM among girls (Wang & Degol, 2017). Without a doubt, internalized gender roles shape self-efficacy perceptions, leading girls to believe that they are unsuited for cybersecurity professions. Research conducted in the UK indicates that women require more encouragement than men do to enter the cybersecurity industry (Peacock & Irons, 2017). Disparities in confidence and self-efficacy significantly impact women's access to the cybersecurity field.

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

Another cause contributing to gender discrepancies in cybersecurity is the lack of positive female role models and representation. Cybersecurity and ICT education continue to be dominated by male teachers despite efforts to strengthen women's and girls' participation in technology related studies and careers. Without role models, women are likely to dismiss cybersecurity as a career option. Also, the absence of relatable figures in leadership positions hinders young women's ability to envision themselves in the field. The (ISC^2) Cybersecurity Workforce Study (2022) found that the underrepresentation of women and individuals from minority ethnic groups in leadership roles within the cybersecurity sector leads to a perception among these groups that the industry is unwelcoming to them. Numerous studies (Cobb, 2018; Pinchot et al., 2020) underline the positive impact of role models on women as they help dismantling negative gender stereotypes and making the cybersecurity field more appealing to women.

Also, lack of encouragement within school, and lack of appropriate career education are barriers that impact women's aspirations in cybersecurity (Peacock & Irons, 2017). Schools are part of larger socio-cultural contexts. In an environment where traditional gender roles are reinforced, girls might not receive the encouragement needed to break free from these norms and explore fields like cybersecurity. Late exposure to cybersecurity also limits women's career opportunities in the field. Without early exposure, girls might not even be aware of the field's potential, leading to a lack of motivation to pursue cybersecurity-related educational paths.

The professional culture of exclusion in cybersecurity industries; a lack of policies in place to ensure an appropriate work–life balance, the use of gendered language in job postings that discourage women from applying, lack of support networks, and biased recruiting process that favour male candidates over equally qualified women candidates cause significant gender disparities in the sector. The 2022 Global Information Security Workforce Survey conducted by ISC [2] also pointed out that 30% of women and 18% of non-White employees worldwide experienced workplace discrimination. Most of the survey respondents argued that they cannot be authentic and freely express their identity at work. The main forms of discrimination experienced by women in cybersecurity globally include unexplained denial or delay in career advancement, tokenism, unconscious and overt discrimination based on gender identity and ethnicity (ISC^2, 2022). Incidents of sexual harassment have been reported in STEM education sites, including in schools, universities and workplaces, which further exclude girls and women from the field (European Parliament, 2021). Due to stereotyping, poor work-life balance, and organizational constraints, the cybersecurity industry continues to have difficulty recruiting and retaining women.

Cybersecurity workplaces operate on the assumption that most workers are men; hence, practices associated with masculinity are more valued than those perceived as essentially feminine (Millar et al., 2021). The male-dominated work environment can also impede the capacity of women to bring about any change. For instance they may lack the authority and influence to shape organizational policies and practices. Gendered assumptions often influence hiring, retention, and opportunities for career promotion. Additionally, the use of non-inclusive language in hiring practices and at work negatively impacts the cybersecurity organization's ability to attract and retain talent. The gendered language used in job postings

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

influence how women and men perceive their suitability for the role. Many studies (Gaucher & Friesen, 2011; D'Hondt, 2016) indicate that cybersecurity job descriptions with male-coded words that emphasize competitiveness, assertiveness or self-reliance may discourage women from applying for those positions. Similarly, as noted by REWIRE partners, often cybersecurity job descriptions demand a broad spectrum of skills, some of which may not be directly related to the roles being advertised. Female applicants tend to abstain from applying unless they possess mastery in most of these skills, while men apply even if they only have proficiency in a few. Additionally, research (Malan et al., 2018) targeting cybersecurity university programs has also found that terminology and branding materials used to describe cybersecurity courses, majors, and scholarships make a difference in women's and girls' perception about them belonging within the cyberspace sector. Militaristic language of cybersecurity (e.g., cyberwar or cyber kill chain) and vocabulary used to describe the industry alienate women considering entering the field (D'Hondt , 2016).

The absence of strong support networks and mentorship opportunities for women in cybersecurity contributes to their isolation in the field. Limited networks hinder women's access to valuable opportunities for skills development and advancement. Additionally, inflexible working practices, such as the shift requirements of Security Operation Centres (SOCs) and some cybersecurity certification programs that demand long hours of engagement, are impractical work models for women who often bear the burden of care. It is well documented that care responsibilities have a disproportionate impact on women's careers compared to men in the sector, as women generally have longer career breaks due to caring for children and family members. Gender biases also contribute to the unbalanced gender composition of the cybersecurity workforce and maintain male-dominated workplace culture.

Diversity and inclusion prove to have a positive impact on workplace culture and play an essential role in addressing gender disparities. The Cybersecurity Workforce study (2022) revealed that organizations that have implemented diversity and inclusion initiatives are starting to overcome workforce shortages. Only 19% of the organizations that have enacted DEI experienced significant shortages in their cybersecurity personnel, in contrast to the 34% of those that have not implemented such initiatives and have no intentions of doing so (ISC^2, 2022). The study also indicated that large corporations are increasingly acknowledging the improved performance of diverse teams when it comes to detecting and neutralizing threats. The introduction of diverse perspectives in cybersecurity can contribute to problem-solving innovativeness and strengthen the collective security labour market. Research (Hewlett et al., 2013; Rock & Grant, 2016) has shown that the greater the diversity of the cybersecurity workforce, the more effectively the sector will be able to manage cyber threats and respond to the industry's needs. Companies with high gender diversity are better able to access the best skills and are more likely to be profitable. Nevertheless, addressing the root causes of gender disparities within the cybersecurity sector involves not only transforming work cultures, industry norms and practices but also requires concerted efforts from educational institutions, policymakers and industry associations. By dismantling these barriers and cultivating an environment that promotes diversity, inclusivity, and equal opportunity, the cybersecurity industry can transcend its historical disparities and tap into the full potential of a diverse workforce, ensuring a safer and more innovative digital world for everyone.

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

4. EU POLICY ACTIONS FOR GENDER BALANCE IN CYBERSPACE

EU has taken a range of policy actions and initiatives to encourage gender balance and inclusivity in the digital sphere, though only a few of them are specific to the cybersecurity sector. The European Commission has set strategic actions to increase women's participation in the digital sector, merely focusing on the promotion of digital skills and education. The "Women in Digital" strategy and WeGate work towards improving gender balance in the sector by targeting three main areas of action: upgrading the digital skills of women, challenging digital gender stereotypes and advocating for more women entrepreneurs. The EU's Women in Digital strategy stresses the importance of fostering collaboration between public institutions, sectorial enterprises, and education institutions to effectively tackle gender inequalities in the digital domain. The Women in Digital Scoreboard was introduced to assess the performance of Member States in areas such as digital skills and employment. Nevertheless, the scoreboard does not include the cybersecurity-specific indicators on gender.

The European Digital Women Diversity Charter is one of the initiatives launched in 2021 aiming to reduce gender disparities in IT and tech roles. The initiative provides certification to companies, organizations or education establishments for undertaking actions and policies to increase gender diversity in IT roles. By joining this initiative, applicants receive practical guidance on how to support women working in technology roles. A renewed policy initiative called the Digital Education Action Plan 2021-2027 foresees gender-sensitive actions aiming at encouraging women's participation in STEM study fields and careers, including as entrepreneurs. The policy document puts emphasis on the need to make ICT curricula and careers more attractive to women and girls and provide them with training in digital business skills during their secondary schools.

In a similar vein, the 2021 EU Parliament resolution on Closing the digital gender gap: women's participation in the digital economy outlines that targeted interventions are needed in early primary schools to fight harmful gender stereotypes and sustain girls' interest in the digital field. Also, it underlines the importance of ensuring gender mainstreaming in digital education at all levels, calling for the inclusion of gender components in all STEM and ICT-related curricula, educational materials, and teaching practices to encourage girls to take up ICT subjects in schools.

Additionally, the recent initiative launched by the European Commission to close the cybersecurity skills shortage pays moderate attention to the gender dimension of the skills gap. The third pillar of the EU Cybersecurity Skills Academy asks for increased commitment from stakeholders in increasing the diversity of persons with cybersecurity skills, notably the share of women. While the European Union is making considerable strides in fostering digital inclusivity, a dedicated focus on gender equality within cybersecurity remains crucial. It is imperative that efforts to bridge gender disparities encompass specific and targeted policy

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

actions tailored to the cybersecurity sector in order to address the significant gender inequalities in this field. In doing so, the EU can not only tackle the underrepresentation of women but also enrich the industry with diverse expertise, ultimately enhancing the security and resilience of digital space.

5. A SNAPSHOT OF EXISTING CYBERSECURITY GENDER - RESPONSIVE INITIATIVES

Despite persisting gender imbalances in cybersecurity, numerous initiatives have been undertaken by public, private and non-profit sectors across Europe to improve gender diversity in the cybersecurity industry. One important initiative launched in 2019 at the EU level by the European Cyber Security Organization was the Women4Cyber, which works towards a more gender-inclusive cybersecurity sector through the promotion, encouragement and support of women's involvement in the field. To date, the foundation has established 19 National Chapters to support women and gender diversity in cybersecurity at a national level.

Cercle des Femmes de la CyberSécurité is a French initiative also dedicated to women in the cybersecurity industry. It provides education, training and mentorship programs and educates recruiters on the cybersecurity gender gap. Initiatives like Seidea adopt an intersectional approach in addressing cyber gender inequalities by providing training and education programs to upskill young black and ethnic minority women who are disproportionally underrepresented in the field. For instance, the Seidea Cyber Bootcamp program diversifies the cybersecurity industry by empowering women minorities with cybersecurity skills and knowledge.

Cybersecurity companies have started paying attention to gender disparities by undertaking targeted actions to attract and retain girls and women in the cyber domain. Microsoft launched a partnership with Women in Cybersecurity to expand their student chapters in 12 European countries. This partnership seeks to unite local communities of aspiring and thriving women cybersecurity professionals across the globe to encourage collaboration, networking, mentoring and the creation of professional development programs. CTF Tech opened its Girl's Cyber Academy to empower girls who are interested in entering in the cyber domain. The academy proved to be effective in improving the cybersecurity skills of girls and increasing their number as participants in the annual Cyber Battle competition of Estonia. Another leading tech service company, Accenture, works towards advancing gender equality by providing flexible work arrangements and tailored training programs. The Women Only Coaching and Mentoring Programs have been running for several years, providing opportunities for professional and personal development of women. There is growing body of literature (Rowland et al., 2018) that indicates that initiatives like mentoring help in changing the perceptions of women about cybersecurity and ensure retainment of female talent in tech industry.

In an attempt to remedy the unbalanced gender composition of the cybersecurity workforce, Orange Cyberdefence launched the #NoBiasInCyber Campaign which sought to break down barriers in cybersecurity by addressing gender stereotypes and promoting female role models to allow women to thrive in these jobs. This campaign underlined the importance of recognizing and deconstructing gender stereotypes from a very early age and to encourage student aspirations regardless of gender or social background.

There are several projects funded by the European Union that seek to close the cybersecurity gender and diversity gap through carrying out research and awareness-raising activities. SPARTA project has conducted the Women in SPARTA campaign to raise awareness of gender stereotypes in the cyber domain and build a strong community among women by presenting their achievements. Furthermore, the Concordia grant has established specific objectives to address cybersecurity gender disparities across different areas, including education and entrepreneurship. A series of diversity and cybersecurity webinars has been organized to provide insights into challenges women face in starting a cyber career. Similarly, the REWIRE project seeks to foster gender balance by raising awareness of the need for a gender-balanced and diverse workforce and setting gender-sensitive targets for all training-related activities.

Additionally, through this policy brief, REWIRE aims to enhance the understanding of cybersecurity stakeholders of the factors that support and prevent women from joining and staying in the industry as well as incentivize relevant stakeholders to undertake gender responsive measures and practices in the field. Last but not least, national projects like INDUCE investigate broader access and expansion of cyber exercises to new target groups by adopting a diversity approach. Through the development of diverse-sensitive cyber scenarios and competence-building actions, in the long term, this intervention is expected to contribute to the empowerment of diverse target groups to act in digital society.

From the establishment of a non-profit European private foundation that supports participation of women in cybersecurity, to industry campaigns that tackle gender stereotypes, these efforts reflect a collective commitment to reshaping the narrative of the industry, underscoring the value of inclusivity and innovation. As we navigate the complex digital landscape, the imperative to persist and expand these efforts remains resolute. The importance of continued commitment, not only at the European level but also within the individual Member States, cannot be overstated .

6. RECOMMENDATIONS FOR CLOSING GENDER DISPARITIES IN THE CYBERSECURITY SECTOR

This section presents a set of targeted recommendations aimed at various key stakeholders in the effort to address gender disparities within the cybersecurity sector. These recommendations offer actionable guidance for educational institutions, cybersecurity associations and policymakers, outlining specific strategies to foster gender inclusivity and diversity within the industry.

6.1 For Educational Institutions

- Tackle gender stereotypes that women and girls are not interested in cybersecurity, by taking actions that focus on changing women's perceptions of cybersecurity and its wider ecosystem, including educational staff, family, students, and community members. For instance, reshaping parental attitudes toward female participation in cybersecurity by underlining the advantages of choosing cybersecurity classes can increase familial support and encouragement towards participation of women in the field.
- Ensure mainstreaming of gender perspective in cybersecurity education at all levels, including informal and non-formal education, through highlighting the importance of diversity in cybersecurity, emphasizing that diverse teams are more effective at addressing complex security challenges.
- Ensure gender-inclusive curriculum, learning materials and teaching methods that are free from gender stereotypes and bias. The curriculum should encourage a diverse range of perspectives and experiences in the content to appeal to a broader audience.
- Remove gendered coded words from university programs and course descriptions in order to attract more women. Brand cybersecurity programs in a way that appeals to a broader target group by using gender-responsive language and images. One study (Malan et al., 2018) found that careful use of language and images to highlight the collaborative aspects of a career in the cybersecurity sector has had a positive effect in attracting more women to cybersecurity courses. For instance, emphasizing transferable skills rather than hacking skills and demonstrating how cybersecurity can solve societal problems can enhance the interest of women in cybersecurity programs.
- Encourage positive attitudes towards cybersecurity careers from an early age. Promote cybersecurity awareness among high school girls in order to increase their interest in cybersecurity-related professions before they start high schools. Promote the presence of female role models by inviting women guest speakers to cybersecurity classes or events to share their experiences and insights.
- Forge partnerships with cybersecurity companies and organizations that are committed to diversity and gender inclusion. Collaborate with industry associations on extracurricular initiatives that promote girl's and women's participation in the field. For instance, summer camps and study visits for children and teenagers developed in

partnership with industry organizations are a great opportunity for girls to acquire cybersecurity knowledge and skills.

- Provide career orientation and recruitment initiatives by offering insights into cybersecurity education, inviting girls visiting cybersecurity departments at university campuses and offering free mentorship programs for girls who are interested in cybersecurity field. Informing about the career possibilities and returns of studying cybersecurity can increase girls and women's interests and influence their educational choices. Offer internship and apprenticeship opportunities to female students, allowing them to gain hands-on practical experience.
- Organize promotional events or talks to visualize the contributions and roles of women in cybersecurity. Role models are a source of inspiration as they help girls to see varied pathways into the cybersecurity sector and encourage them to pursue cybersecurity-related studies and careers.
- Implement comprehensive data collection initiative on the representation of women in cybersecurity sector. This data should be used to establish a continuous monitoring mechanism to track progress over time and identify areas within educational programs where improvements are required to encourage greater female participation in the field.

6.2 For Cybersecurity Companies/Associations

- Develop and implement gender-inclusive and diversity policies and programs that target organizational practices and workplace culture. Policies should support the elimination of gender stereotypes and biases and promote work-life balance measures, including flexible working hours and career leave to accommodate the needs of workers with caring responsibilities.
- Equal pay and benefits- Ensure that all cybersecurity industry employees receive equal pay for equal work, regardless of their gender identity, sexual orientation, ethnicity, race, or any other socio-demographic characteristic. Review compensation structures regularly to identify and address gender and any other discriminatory pay disparities.
- Make the recruitment process gender inclusive - Adopt diverse and inclusive recruiting and promotion practices that actively seek out and attract women and other underrepresented cohorts. Ensure job descriptions are free from gender bias and they accurately reflect the core job requirements, eliminating excessively broad skill expectations. Use inclusive language in job listings and emphasize that applicants do not need to meet every listed requirement to apply.
- Set clear goals and targets for gender equality in the organization to deliver meaningful change and tackle existing disparities. For instance, cybersecurity companies could set hiring targets to promote greater gender balance in their workforce, leadership, and board positions among equally qualified candidates.
- Formalize mentorship programs and promote female role models – establish mentorship programs within the company to support the career growth of female

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

employees. Promote the achievements of women in the cybersecurity industry in order to inspire and attract more women to pursue careers in this field. Simultaneously, invest in attraction, retention, and women's career advancement.

- Ensure equal access to training and professional development opportunities - Offer training and professional development opportunities to empower female employees in the cybersecurity industry. This can include technical skills development, leadership training, and opportunities to attend workshops.
- Collaborate with educational institutions and other stakeholders to design and provide initiatives that encourage women and minoritized groups to pursue careers in cybersecurity. Offer in-company internships, apprenticeships, scholarships and support educational programs that promote diversity in the cybersecurity domain.
- Undertake regular diversity and inclusion assessments. Collect and analyse data on gender equality and diversity to understand gender disparities within the organization, measure the effectiveness of gender-responsive initiatives undertaken, and identify areas for improvement.
- Implement diversity training and awareness programs with cybersecurity companies to address inherent biases in the workplace and encourage an inclusive work environment where everybody feels valued and respected.
- Establish safe, easily accessible, and confidential reporting mechanisms to address gender discrimination and harassment in the workplace.
- Publicly commit to promoting gender equality and diversity in the cybersecurity industry. Demonstrating a strong commitment to diversity can attract a more diverse talent pool and show a genuine dedication to creating a more inclusive work environment.

6.3 For Governments & Policymakers

- Take concrete policy actions to address the gender gap in cybersecurity, focusing on boosting women and girls' involvement across all education and employment levels, including research, development, and innovation.
- Allocate funding for conducting comprehensive research on gender disparities in cybersecurity, examining participation rates, identifying barriers, and best practices to inform improvements. Utilize the collected data to inform policies, and interventions aimed at addressing gender disparities.
- Encourage the collection of gender-disaggregated data in educational institutions and organizations to track progress towards gender equality within cybersecurity field. At the European level, the creation of cybersecurity-specific indicators on women as part of the Digital Society and Economy Index could help in understanding and addressing gender gaps in the cybersecurity domain.
- Support training programs specifically targeting women in cybersecurity, offering both technical and non-technical skills development opportunities.

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

- Implement policies that integrate cybersecurity skills into the curriculum at all levels of compulsory education.
- Foster multi-stakeholder partnerships between governments, academia, and private sector organisations to facilitate cybersecurity training and skills development initiatives for women and other underrepresented cohorts.
- Provide appropriate funding and resources for initiatives aiming at attracting more girls and women to study and work in cybersecurity.
- Encourage cybersecurity companies to implement meaningful diversity and inclusion initiatives within their organizations, with a focus on cybersecurity roles. For instance, introducing inclusive recruitment practices, such as blind hiring processes and diverse interview panels can mitigate unconscious biases during the hiring process. In certain contexts, the use of diversity quotas and hiring targets can accelerate progress toward gender equality without compromising the principle of merit-based selection. Furthermore, encouraging the adoption of comprehensive parental leave policies and fostering an environment where employees feel supported in taking advantage of these benefits can help parents and caregivers to balance their professional and personal commitments effectively.
- Encourage organizations within the cybersecurity industry to establish diversity and inclusion committees with a specific focus on addressing gender disparities. Their role would involve developing strategies, setting goals and overseeing the implementation of programs designed to attain gender balance.
- Support the establishment of mentorship programs connecting girls and women with experienced female professionals in cybersecurity to provide career guidance.
- Support the creation of a European platform to facilitate knowledge and good practice sharing among cybersecurity stakeholders (e.g., companies, educational institutions, NGOs, and governments) on gender-inclusive initiatives and the promotion of gender diversity in the cybersecurity field.
- Launch national and EU-wide campaigns to challenge persistent gender stereotypes and raise awareness about the existing gender disparities within the cybersecurity sector, highlighting the need for systemic change and encouraging stakeholders to actively participate in a more inclusive industry.
- Ensure gender-balanced representation at the cybersecurity policy level- women must be involved in designing national and European cybersecurity policy. Cybersecurity female leadership should be regarded as a key objective in the offer to gender gap narrowing.

7. CONCLUSIONS

The gender gap within the cybersecurity sector is an undeniable reality, with women being disproportionately underrepresented in technical roles, leadership positions and decision-making spheres. The ramifications of this disparity extend beyond mere statistics; they encompass missed opportunities for innovation, economic growth, and the robust defence of Europe's cyberspace. The poor representation of women in cybersecurity perpetuates a skewed workforce that lacks diverse viewpoints and skills essential for tackling the ever-evolving landscape of cyber threats. Closing the gender gap in cybersecurity is a vital necessity for the industry's advancement and overall European digital security. Addressing the existing disparities would help the public sector and companies tackle the shortage of skilled professionals and increase adaptability to the changing threat landscape.

Achieving gender equality within the cybersecurity sector is more than simply encouraging women to study cybersecurity and setting gender quotas for representational purposes. It is also a matter of equality and responsibility in human rights. It is about understanding and tackling the root causes of gender disparities that discourage women from entering or advancing in cybersecurity industry. Solutions can only start to emerge when there is a situated understanding of the generative mechanisms that form the basis of inequality. Key actors of the cybersecurity sector, such as government, industry associations, education institutions, CSOs, and professional and trade associations, have an important role to play in addressing gender bias and promoting cultural change. This could be done by committing to actioning the recommendations provided in this policy brief, ensuring all aspects of gender disparities are addressed: from deconstructing gender stereotypes and promoting cybersecurity education at an early age, providing mentorships and support for women and underrepresented groups pursuing cybersecurity career, to fostering inclusive workplaces that promote diversity and incorporating gender lens to policymaking processes. By working together, a more holistic and sustainable change can be achieved. Collaborative efforts also promote knowledge-sharing, enabling the sector to develop best practices that truly advance gender equality.

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

8. REFERENCES & FURTHER READING

Bıçakcı, A., Evren, A. (2022). Building a Gender-Balanced Security Culture for Constructive Cyber Security. *International Gender for Excellence Research Conference-Selected Papers and Abstracts*.

Cobb, M. (2013) "Plugging the cyber security skills gap: The Vital Rola that Women Should Play in Cyber-security ", *Computer Fraud & Security*, (7), 5-10.

De Zan, T., Di Franco. (2019). *Cybersecurity Skills Development in the EU*. European Union Agency for Cybersecurity.

D'Hondt, K. (2016). Women and Public Policy Program. *Harvard Kennedy School*. https://wappp.hks.harvard.edu/files/wappp/files/dhondt_pae.pdf

European Union. (2020). *Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. Official Journal of the European Union.

European Commission. (2023). Digital Skills and Jobs Platform. https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

European Union. (2021). *She Figures 2021 : Gender in Research and Innovation : Statistics and Indicators*. Publications Office of the EU. https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/67d5a207-4da1-11ec-91ac-01aa75ed71a1

European Union. (2023). *Council Recommendation on Improving the Provision of Digital Skills in Education and Training*. Official Journal of the European Union.

European Parliament. (2020). *Report on Closing the Digital Gender Gap: Women's Participation in the Digital Economy.*

Gaucher., G, Friesen, J. (2011). Evidence that Gendered Wording in Job Advertisements Exists and Sustains Gender Inequality. *Journal of Personality and Social Psychology*. Vol. 101, No. 1, 109 –128.

Hewlett, S., Marshall, M., Sherbin.(2013). How Diversity Can Drive Innovation. *Harvard Business Review*.

(ISC)2. (2017). The 2017 Global Information Security Workforce Study: Women in Cybersecurity. *Frost & Sullivan White Paper*.

(ISC)2. (2022). Cybersecurity Workforce Study : A Critical Need for Cybersecurity Professionals Persists Amidst a Year of Cultural and Workplace Evolution.

Jamie, J., Donna, D., Sushma, S., & Karen, K. (2020). Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap. *Information Systems Education Journal,* 18(3), 44.

Kshetri, N., Chhetri, M. (2022). Gender Asymmetry in Cybersecurity: Socioeconomic Causes and Consequences. *University of North Carolina*.

Lihammer, S., Hagman, L. (2021). Investigating Gender Disparity within Cyber Security- Analysis of Possible Factors through a Mixed-Method Qualitative Study and Self-Implemented Testing Program. *KTH Royal Institute of Technology*. Sweden.

Malan, J., Lale-Demoz, E., Rampton., J. (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development. *Department for Digital, Culture, Media and Sport*. United Kingdom.

Makarova, E., Aeschlimann, B., Herzog., W. (2019). The Gender Gap in STEM Fields: The Impact of the Gender Stereotype of Match and Science on Secondary Students' Career Aspirations. *Educational Psychology*, 10 (4).

Microsoft Corporate. (2022). The Urgency of Tacking Europe's Cybersecurity Skills Shortage.

Millar, K., Shires, J., Tropina, T. (2021). Gender Approaches to Cybersecurity: Design, Defence and Response. *United Nations Institute for Disarmament Research*.

Nurse, J., Konstantinos, A., Grammatopoulos, A., Di Franco, F. (2021). Addressing Skills Shortage and Gap through Higher Education. *European Union Agency for Cybersecurity*.

Peacock, D., & Irons, A. (2017). Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science and Technology*, 9, 25–44.

Reed, J., Zhong, Y., Terwoerds, L., and Brocaglia, J. (2017) The 2017 Global Information Security Workforce Study: Women in Cybersecurity.

Resolution 2022/C 67/18 of the European Parliament on Promoting Gender Equality in Science, Technology, Engineering and Mathematics (STEM) Education and Careers. *Official Journal of the European Union*.

Rock., D, Grant, H. (2016). Why Diverse Teams Are Smarter. *Harvard Business Review*.

Rowland, P., Podhradsky, A., Plucker, S. (2018). Cybher: A method for Empowering, Motivating, Educating and Anchoring Girls to a Cybersecurity Career Path. *Hawaii International Conference on System Sciences*.

Slupska, J. (2019). Safe at Home: Towards a Feminist Critique of Cybersecurity. *St Antony's International Review* 15(1), 83-100.

Slupsla, J., Tanczer, L. (2021). "Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things", In J. Bailey, A. Flynn and N. Henry (eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*.

Sultan, U., Axell, C., Hallstrom, J. (2018). Girls' Engagement in Technology Education: A Systematic Review of the Literature. *PATT36 International Conference: Research and Practice in Technology Education: Perspectives on Human Capacity and Development*.

Wang, MT., Degol, J.L. (2017). Gender Gap in Science, Technology, Engineering, and Mathematics (STEM): Current Knowledge, Implications for Practice, Policy, and Future Directions. *Educational Psychology Review* 29, 119–140 (2017).

West, M., Kraut, R., Chew, H. (2019). I'd Blush If I Could: Closing Gender Divides in Digital Skills Through Education. *UNESCO Publication*.

Zacharias, C., Hovardas, T., Xenofonotos, N., Pavlou, I., Irakleous. (2020). Education and Employment of Women in Science, Technology, and the Digital Economy including AI and its influence on Gender Equality. *FEMM Committee, European Parliament*.