DOI: https://doi.org/10.53486/dri2024.07
UDC: 004.056.53:349.2-055.2

EMPOWERING WOMEN IN CYBERSECURITY: NAVIGATING CHALLENGES FOR A RESILIENT DIGITAL FUTURE

Alina-Camelia BELCIU (VASILESCU)[5], PhD Student
ORCID number: 0009-0002-0546-6662

Abstract:
In a global context characterized by a fast digital transition and a shortage of technical skills, promoting women in information and communication technology (ICT) and cybersecurity is becoming essential to reduce the workforce gap in the field and also to ensure a resilient and inclusive digital economy. Women, an underutilized source of talent, can bring innovative and various contribution, contributing to address challenges in ICT and cyber security. This article explores the issue of underrepresentation of women in cybersecurity, where they occupy only 25% of the roles available globally, despite recent initiatives aiming to change this status quo. The research methodology is based on a qualitative approach, using documentary analysis of relevant European policies and reports and articles. The research aims to answer the question "How can empowering women in cybersecurity, by overcoming existing barriers and building on European initiatives, contribute to a safer and more resilient digital future?" The study examines the structure and impact of European initiative, alongside with challenges faced by women in accessing and maintaining a career in this field. The results highlight that the European initiatives, such as Women4Cyber and Girls and Women in Digital, play a key role in bridging the gender gap in ICT and cybersecurity. Mentoring and educational programs developed under these initiatives have a positive impact on women's participation in cybersecurity, but barriers related to gender bias and limited access to equal opportunities still exist. The contribution of this study is to highlight the importance of empowering women in cybersecurity and how the obstacles they face can be addressed through dedicated initiatives, essential for creating a supportive environment for women in this critical field. The study focuses on the European initiatives and future research may consider analyzing the initiatives globally. Furthermore, interviews with women cybersecurity experts may be conducted, thus providing deeper insight into the global dynamics of gender in cybersecurity.

Key words*: women, cybersecurity, digital resilience, barriers, gender gap, European initiatives*

JEL: J24, J16, I28, O33

1. Introduction

Digital resilience represents a major challenge in the digitalization era, but also a significant opportunity for cybersecurity development. In a dynamic and changing cyber landscape, cybersecurity experts face an unprecedented threat landscape, generating a need to attract and retain talent in the field, more than ever. The cybersecurity talent shortage, especially related to women, represents one of the most important obstacles encountered in strengthening this sector.

Despite some progress registered, women are still underrepresented in essential sectors such as ICT - Information and Communication Technology and cybersecurity. At European and international level this situation is acknowledged and represents one of the main concerns in workforce development strategies. Cybersecurity has been traditionally recognized as a technical domain. Currently it is regarded as encompassing multidisciplinary skills, including technical and non-technical competences, communication abilities, risk management and relevant policies and regulations knowledge.

[5] belciualina21@stud.ase.ro, Bucharest University of Economic Studies, Romania

European and international programs and grant have been initiated to address this gender gap. Through its initiatives, the European Union demonstrates the commitment in reducing gender disparities and providing support to women in developing cyber carriers.

This research's objective is to investigate how empowering women in cybersecurity, by overcoming existing barriers and taking advantage of European initiatives, support a resilient digital future.

2. Methodology

A qualitative approach with a descriptive research design was the researcher's option in order to provide an overview of the representation of women in the cybersecurity field and the barriers encountered in developing a carrier in this sector. The research explores the challenges encountered by women and the initiatives aiming to support the participation of women in cyber field.

Secondary data from policy documents, reports, articles and studies were collected, aligned with documentary research methodology, with the aim of identifying relevant information related to women's participation in the cybersecurity field and current initiatives that support them.

Two key initiatives of the European Commission, namely Women4Cyber and Digital Europe Program (DEP)'s Girls and Women in Digital, were the author's option as case studies for research, for a detailed analysis, including analysis of the structure, objective and results of these initiatives, with the aim of providing an understanding of how these programs contribute to increase women's participation in cyber field and reduce barriers they face.

The first major assumption of the author is that women are still underrepresented in the cybersecurity workforce, limiting the diversity of perspective and innovative solutions, essential for addressing complex digital security challenges. A second assumption clarified during the research considered that women in cybersecurity face a range of systemic barriers that discourage them to enter or remain in this field. The third assumption of the research is considering that various European initiatives consisting in targeted programs to reduce the gender gap are essential in increasing the participation of girls and women in cybersecurity and ICT fields.

3. Results and discussions

According to ISC2 (2023), the global cybersecurity workforce increased with 8.7% last year and reached 5.4 million professionals (Figure 1). Considering the context of increasingly complex cyber threats and demand for cyber skills and solutions, this growth reflects a response to this situation. However, despite this growing, the gap between the need and their availability of cybersecurity specialists has continued to grow significantly. In 2023, the global deficit increased with 12.6% compared to the previous year and reached almost 4 million professionals. Europe is also facing significant challenges, with a shortage of around 348,000 experts.

This trend reflects a significant major problem for organizational security at global level, as skills gap mean that many organizations cannot effectively secure their systems against cyber threats. As cyberattacks become more sophisticated, the difference between the demand and the offer of specialists could influence the vulnerability of digital infrastructure at global level. Therefore, initiatives to attract more professionals in this field, education and training are essential, with a special focus on diversified workforce by promoting women's participation in cyber.

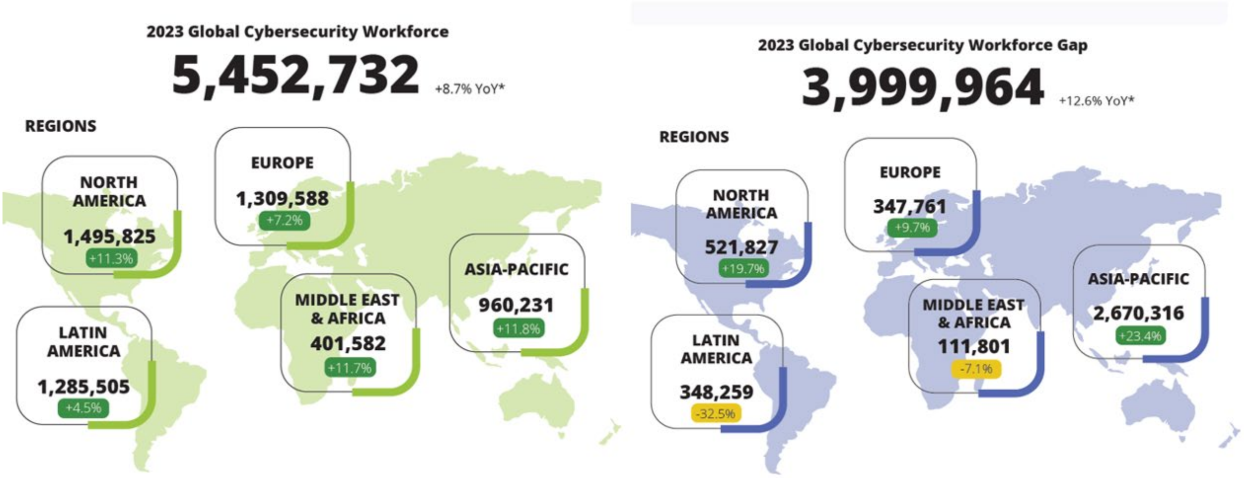

Figure 1. The cybersecurity workforce and gap

Source: https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

3.1. Women representation in the cybersecurity workforce

In 2022, women represented approximately a quarter of global cybersecurity roles, which represents a significant increase compared to 20% in 2019 and only 10% in 2013 (Cybersecurity Ventures, 2022). This evolution reflects the recent efforts to attract more women in this critical sector. However, the percentage of women remains relatively low compared to men, indicating continuous barriers to women's access and entering and advancement in cyber careers. Forecast is optimistic. It is projected that women will occupy 30% of cybersecurity jobs by 2025, and this percentage will increase to 35% by 2031, as shown in Figure 2. This potential growth could be attributed to the continuous effort to address the gender gap and to initiatives dedicated to education and training in STEM and cybersecurity. It will bring more perspectives and innovation, contributing also to digital resilience, through a stronger team in the face of complex challenges of the modern digital landscape.

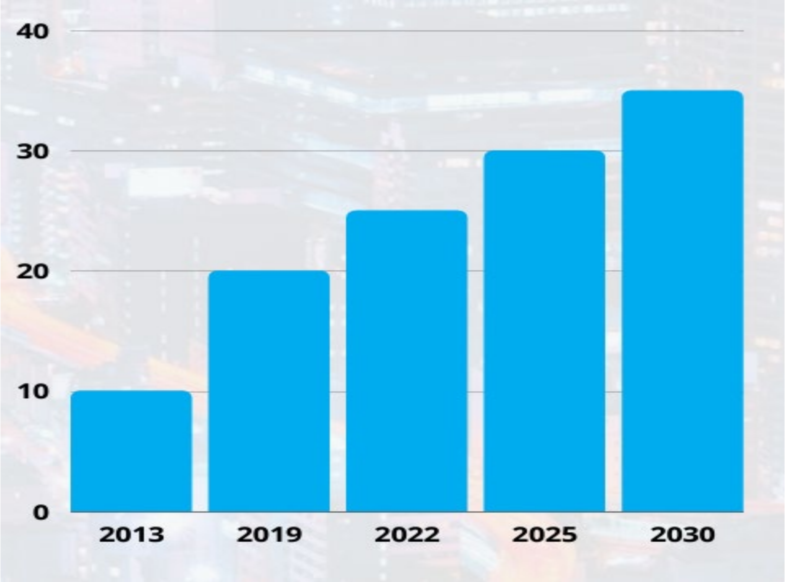

Figure 2. Representation of women in cybersecurity roles (%)

Source: https://cybersecurityventures.com

3.2. Key barriers to gender equality in cybersecurity

In cybersecurity field, women face a series of significant barriers that limit their participation in the field, and also their opportunities for carrier advancement. These obstacles, of a cultural, social and organizational nature, contribute to maintaining an underrepresentation of women in this critical sector, which requires advanced technical competences alongside with multidisciplinary abilities. (Women4Cyber Foundation, 2023)

The lack of confidence in their technical skills represents a major barrier for women which want to pursue a cyber carrier. Moreover, there is a false perception that this domain is strictly technical one and that women are less capable to perform advanced technical activities. This perception discourages women to develop the necessary skills to enter and advance in cyber field.

Many women are not fully aware of the diversified career opportunities available in the cybersecurity field that exceed traditional technical roles. The cyber field also offers various opportunities for specialists in law, risk management, and communication. The lack of visibility of these cyber career opportunities also contribute to the women's underrepresentation in this sector.

The cybersecurity is often perceived as a domain dominated by men, which discourage women to get involved. As a result, the gender stereotypes and less inclusive workplace perpetuate and women are not included and appreciated at the same level as their male colleagues.

The gender stereotypes and bias present in the cyber work environment also play an important role in discouraging women to pursue a career in the field. Women may often be perceived as less capable of performing technical roles, and their ideas and contributions may often be undervalued or ignored. These attitudes, along with the lack of equal opportunities for advancement, contribute to maintaining a gender imbalance.

Women in cybersecurity often face a lack of successful mentors and role models to guide them in their careers. Mentors play an important role in the development of professional careers, and their absence may cause less opportunities for advancement. Thus, mentoring programs are considered essential to improve participation and retention of women in this field.

The organizational culture and work environment in the cybersecurity field can often be unfriendly to women. They often face exclusion from informal networks, which are dominated by men, and could feel additional pressure to prove that they are as competent as their male colleagues. The workplace environment may also be characterized by the lack of flexible working policies, to ensure the balance between the professional and personal life.

Salary disparities between men and women represent an additional barrier to gender equality in cybersecurity. Women, even those who occupy similar positions with their male colleagues, are often paid less. This not only discourages them from entering the field, but also contributes to a higher rate of abandoning cybersecurity careers.

In addition to these obstacles, the lack of strong inclusion and diversity policies in many organizations that are active in the cybersecurity field must be highlighted. Existing initiatives are often insufficient to fully counteract the cumulative effects of these barriers and create a truly inclusive working environment.

According to Bagchi-Sen et al. (2010), the barriers that women face in advancing within cybersecurity are multi-dimensional, encompassing social, institutional, and personal challenges. Social factors include work-family conflict, the influence of informal networks, and societal expectations placed on women, which often pressure them to balance domestic responsibilities with demanding cybersecurity roles. Institutional barriers consist of the lack of female role models and mentors, occupational cultures that are not always welcoming to women, and the demographic makeup of cybersecurity teams, which are predominantly male. The authors highlight that, while IT and cybersecurity share similar barriers, the personal factors—such as specialized cybersecurity skills, work experience, knowledge in the field —differentiate cybersecurity professionals from IT roles. (Figure 3). These personal factors are crucial for career success in cybersecurity, further emphasizing the importance of providing women with opportunities for skill development and mentorship to overcome these challenges.

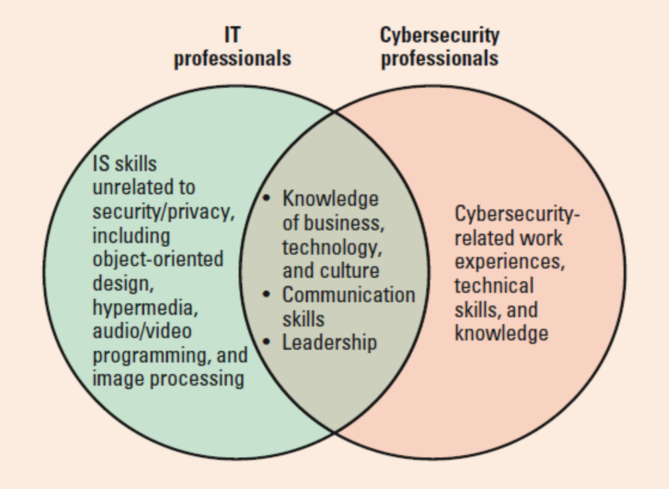
IT professionals
Cybersecurity professionals
IS skills unrelated to security/privacy, including object-oriented design, hypermedia, audio/video programming, and image processing
• Knowledge of business, technology, and culture
• Communication skills
• Leadership
Cybersecurity-related work experiences, technical skills, and knowledge

Figure 3. Barriers encountered by women in IT and women in cybersecurity

Source:
https://www.researchgate.net/publication/224110561_Women_in_Cybersecurity_A_Study_of_Career_Advancement

Giboney et al. (2023) recognize also that barriers to women's participation in cybersecurity are diverse and persistent, involving social, institutional, and personal challenges. Research reveals that social barriers include a lack of career awareness, misconceptions about cybersecurity being a male-dominated field, and fears of harassment. Institutional barriers are equally significant, such as the absence of role models, lack of mentorship, and workplace cultures that may not be inclusive of women. Additionally, personal barriers like inadequate skills, lack of knowledge in cybersecurity, and work experience in the field, further hinder women's ability to enter and progress in this field. These barriers are perceived differently depending on the career stage of the individual. Young women, in particular, express uncertainty about career paths and limited exposure to cybersecurity roles, while adult women, especially those early or mid-career, are more likely to report being underestimated or harassed in a male-dominated profession. Addressing these obstacles through improved awareness campaigns, mentorship programs, and more inclusive workplace policies is essential for creating a supportive environment for women in cybersecurity.

3.3. European context for promoting women in ICT and cyber

In recent decades, the European Union has recognized the essential role of information and communication technology (ICT) in promoting the digital shift across economic and social areas. Between 2013 and 2023, the number of ICT specialists increased by 59.3%, almost six times faster than the total employment growth. (Eurostat, 2024). However, women continue to be underrepresented in this field, representing approximately 1 of 5 graduates and ICT specialists in the EU, with 19.4 % employed as ICT specialists in 2023 against 80.6 % men.

This underrepresentation of women in ICT led European institutions to develop policy and initiatives with the aim of enhancing the participation of women in the sector. In this context, the European Commission (2022) set up an essential framework that establishes ambitious goals for the future of the European digital economy. Among these, one of the main targets is represented by the employment in the European Union of minimum 20 million specialists in ICT field until 2030, with a specific focus on promoting women in this field and also increasing the number of ICT graduates.

The European Commission (2023) highlights the importance of digital skills for a successful digital transformation of Europe and identifies the urgent need to ensure an adequate number of ICT specialists and benefit from women contribution to reduce the talent shortage in the field and build an inclusive digital Europe.

One of the main tools developed to monitor progress in women's inclusion in digital jobs and careers is the Women in Digital (WiD) Scoreboard. WiD scoreboard represents a mechanism to evaluate the performance of Member States regarding the Internet use, user skills, and employment in specialist positions. It offers a detailed overview of the level of integration of women in the digital economy, identifying gaps and areas that need improvement, and additional policies to ensure equal participation.

The "European Union Agency for Network and Information Security (ENISA)" (2019) is taking proactive steps to enhance its digital security capacities, recognizing that protecting its society, economy, and democracy requires strong cybersecurity measures. An integral aspect of achieving this goal is promoting diversity and gender balance within the cybersecurity workforce, which has been identified as a key factor for success. ENISA plays an active role in supporting initiatives that advocate for women in cybersecurity roles in various sectors, including IT security, IoT security, medical, transport, military and defense cybersecurity. ENISA emphasizes its commitment to creating an inclusive environment where women are valued, respected, and given equal opportunities, including equal pay and career development programs. Furthermore, ENISA's efforts aim not only at improving representation, but also at inspiring the next generation of young girls to pursue careers in cybersecurity, thereby changing societal mindsets and raising awareness about the importance of diversity in this growing sector. In this context, ENISA's work contributes to a broader European strategy to close the gender gap in cybersecurity and build a resilient digital future by ensuring that the talent pool is both diverse and inclusive.

Girls and Women in Digital

The initiative "Girls and Women in Digital" and its call for proposal, launched by the European Commission (2024), is part of coordinated efforts to increase girls and women's participation in ICT and cybersecurity. The initiative addresses a general context in which women remain underrepresented in ICT professions, despite the rapid growth of demand in this sector. Although in terms of basic digital skills, women register higher performance, they represent only 19% of specialists. The initiative is managed by the European Commission, Directorate-General for Communication, Networks, Content and Technology (DG CONNECT) and is part of Work program 2023-2024. The structure of this action is concentrated around several key objectives, aimed at supporting the commitment to reach the target of 20 million ICT specialists in the EU until 2030.

The objectives are clear and well defined, aiming not only at increasing the number of women in ICT, but also at building a network of expertise and involving the relevant stakeholders at the European level. Identification of the main obstacles that girls and women face in selecting and maintaining a ICT carrier, promoting actions and initiatives to enhance women's representation in the field and building a network of relevant experts and actors represent the main objectives of the initiative.

The expected results encompass a detailed report that identifies the main obstacles women face in choosing an ICT career and proposes practical and effective measures that contribute to reducing the gender gap in this domain, an analysis of national and regional strategies to implement Women in Digital Declaration, including best practices and challenges encountered, establishing a platform where stakeholders can interact to evaluate progress and discuss new initiatives to promote women.

The impact of these measures is expected to be significant in achieving the EU's goal of reducing the gender gap in ICT and increasing the number of women involved in this sector. By mapping and analyzing best practices, the initiative will contribute to changing the European digital landscape, facilitating a gender convergence that is essential for the digital success of Europe in the next decade.

This initiative represents a major step towards bridging the gender gap in ICT. By identifying barriers, promoting concrete measures, and collaborating across sectors and relevant stakeholders, it will contribute to a more inclusive and equal digital environment. The results of this action will provide the European Union with valuable information on the effective measures needed to change the status quo and help build a more diverse and fair digital future.

ECSO "Women4Cyber" initiative

Initiatives such as "Women4Cyber", launched by the "European Cyber Security Organization (ECSO)" in collaboration with the "European Union Agency for Cybersecurity (ENISA)", aim to enhance the visibility and presence of women in cybersecurity, an essential field in the protection of European digital infrastructure. The Women4Cyber Foundation was created in 2019 as a non-profit foundation based in Europe focused on promoting and supporting the participation of women in the cybersecurity field and its journey is underlined in Figure 4 (Women4Cyber Foundation, 2023).

An essential element of the structure of this initiative is represented by national chapters that have a key role to play in facilitating local and regional collaboration to support the increase in the number of women in cybersecurity. Each national chapter operates as an extension of the main foundation, offering direct support to women established in that country through mentoring, education, and networking.

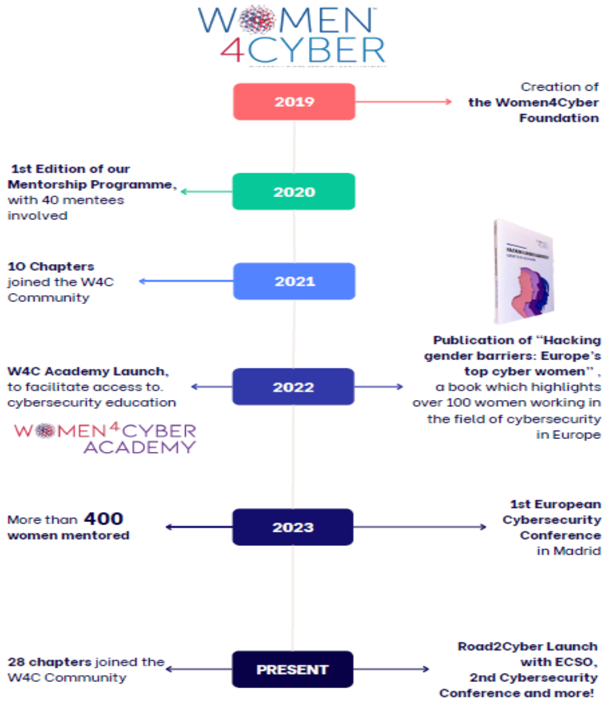
WOMEN 4CYBER
2019
Creation of the Women4Cyber Foundation
2020
1st Edition of our Mentorship Programme, with 40 mentees involved
2021
10 Chapters joined the W4C Community
2022
W4C Academy Launch, to facilitate access to cybersecurity education
WOMEN4CYBER ACADEMY
Publication of "Hacking gender barriers: Europe's top cyber women", a book which highlights over 100 women working in the field of cybersecurity in Europe
2023
More than 400 women mentored
1st European Cybersecurity Conference in Madrid
PRESENT
28 chapters joined the W4C Community
Road2Cyber Launch with ECSO, 2nd Cybersecurity Conference and more!

Figure 4. Women4Cyber's journey

Source: [*https://women4cyber.eu*](https://women4cyber.eu)

In 2021, Women4Cyber registered a significant growth of its community, expanding by 10 national chapters, and in 2024 the network reached 28 chapters, including many countries in Europe, thus demonstrating a broad coverage and extended commitment to support women in cybersecurity, as shown in Figure 5. Each national chapter has the objective of promoting the activities of Women4Cyber at the national level and adapting the initiatives to the specific needs and challenges of each region (Women4Cyber Foundation, n.d.).

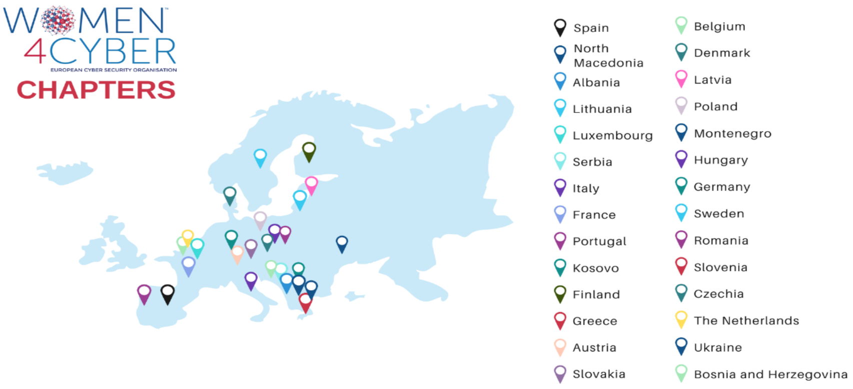

Figure 5. Women4Cyber Chapters

Source: [*https://women4cyber.eu/*](https://women4cyber.eu/)

The main objectives of Women4Cyber are increasing the number of women in cybersecurity, in technical and nontechnical roles, through mentorship and education, establishing a support network at European level, including the national chapters that facilitate collaboration and mutual support among women, and reducing barriers that women encounter in cybersecurity field, including gender stereotypes, lack of success models, and limited access to development opportunities. (Women4Cyber Foundation, n.d.).

According to Women4Cyber Foundation (2023), since its launch, Women4Cyber has achieved important results in terms of increasing women's participation in cybersecurity, namely more than 400 women who benefit from support through the mentoring program launched in 2020, contributing to their career development and professional confidence. Furthermore, the Women4Cyber Academy, launched in 2022, facilitates access to high-quality educational resources in the field, helps to reduce the skill gap among women, and contributes to new generations of women specialists. Moreover, through the additional national chapters included, the support network has expanded, thus consolidating the collaboration between professionals from various countries and cultures. Women4Cyber and ECSO promote a common platform, Road2Cyber, to bridge the cybersecurity talent shortage and increase diversity in the field by optimizing hiring processes, offering specific training suggestions, and actively motivating women to participate in the cybersecurity community.

Women4Cyber and its network of national chapters play a key role in tackling the challenges women face in the field of cybersecurity. To address the lack of confidence and skills, the initiative helps women, through mentoring and educational programs, develop the necessary skills to excel in this technical domain and gain confidence in their abilities. Women4Cyber contributes to change the perception that cybersecurity is a male-dominated domain, offering visibility to successful women and creating support networks that encourage women to pursue a career in the field. The lack of successful mentors and success models is addressed by mentoring programs and publications that provide concrete examples of women who achieved to overcome barriers and excel in this complex domain. (Women4Cyber Foundation, n.d.).

This analysis details the structure, objective, and results of Women4Cyber and highlights the impact of this initiative in increasing women's participation in cybersecurity by overcoming the barriers they face, supporting the third hypothesis.

4. Conclusions

Promoting women in ICT and cybersecurity proves to be essential to reduce the workforce gap in the field and also to ensure a resilient and inclusive digital economy. Women, an underutilized source of talent, can bring innovative and various contribution, contributing to address challenges in ICT and cyber security. Their deeper integration into the digital workforce is a strategic step, recognized at European level. EU policies and dedicated initiatives support active participation of women, tackling the barriers they encounter and providing essential resources for career development in this critical sector.

Despite recently registered progress, women remain significantly underrepresented in cybersecurity, with 25% of global roles, limiting diversity and innovation in the sector. Traditional barriers continue to represent major obstacles that prevent the potential contribution of women in this field. Perception of cybersecurity as a male dominated field, gender stereotypes, lack of mentors and role models, lack of confidence and skills development need to be underlined. Addressing these obstacles through awareness campaigns, mentorship programs and policies dedicated to inclusive workspaces, is essential to create an environment that support women in cybersecurity field.

European initiatives have an essential role in addressing these challenges. Programs and initiatives such as Women4Cyber and DEP – Girls and Women in Digital offer specific support through mentorship programs, training and professional network, important to enhance women's participation in the field and to create a safe and resilient cyberspace. These initiatives contribute not only to the paradigm shift in the perception related to women's role in cyber field, but also to consolidating an inclusive framework for professional development.

The implication of this research highlights the importance of empowering women in cybersecurity, through addressing the existing barriers and benefiting from the specific European initiatives, thus contributing to a safer and more resilient digital future. These efforts could be expanded by initiating new educational programs starting at secondary school and high school level, thus creating a continuous flow of qualified women for future ICT careers.

Research limitations include the dependency on secondary data and the analysis of specific initiatives, which, while relevant, do not provide a complete overview of the barriers and challenges women face in cybersecurity at global level. Additionally, the research focuses on the European initiatives, which limits the applicability of the conclusions. Future research may consider expanding research globally and conducting interviews with women cybersecurity experts, thus providing deeper insight into the global dynamics of gender in cybersecurity.

Bibliographical references

1. Bagchi-Sen, S., Rao, H. R., Upadhyaya, S., & Sangmi, C. (2010). Women in Cybersecurity: A Study of Career Advancement. *IT Professional*, 12(1), 24-31. https://doi.org/10.1109/MITP.2010.39, https://www.researchgate.net/publication/224110561_Women_in_Cybersecurity_A_Study_of_Career_Advancement
2. Cybersecurity Ventures. (2022). Women in cybersecurity 2022 report. Cybercrime Magazine. Retrieved from https://cybersecurityventures.com
3. European Commission. (2022). Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030. Retrieved from https://eur-lex.europa.eu/eli/dec/2022/2481/oj
4. European Commission. (2023). 2023 Report on the state of the Digital Decade. Retrieved from https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade, https://eur-lex.europa.eu/eli/dec/2022/2481/oj
5. European Commission. (2024). Call for proposal DIGITAL-2024-ADVANCED-SKILLS-06-WOMEN - Girls and Women in Digital. Retrieved from https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2024-advanced-skills-06-women, https://eufundingportal.eu/girls-and-women-in-digital/
6. European Union Agency for Network and Information Security (ENISA). (2019). Women in cybersecurity leaflet. Retrieved from https://www.enisa.europa.eu/news/enisa-news/women-in-cybersecurity-1/view
7. EUROSTAT. (2024). ICT specialists in employment. Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment#ICT_specialists_by_sex
8. Giboney, J. S., Anderson, B. B., Wright, G. A., Oh, S., Taylor, Q., Warren, M., & Johnson, K. (2023). Barriers to a cybersecurity career: Analysis across career stage and gender. *Computers & Security*, 103316. https://doi.org/10.1016/j.cose.2023.103316
9. ISC2. (2023). Cybersecurity workforce study 2023: How the economy, skills gap and artificial intelligence are challenging the global cybersecurity workforce. Retrieved from https://www.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf
10. Women4Cyber Foundation. (2023). Annual report 2023: Building a diverse cybersecurity approach in Europe.
11. Women4Cyber Foundation. (n.d.). Official site. Retrieved from https://women4cyber.eu