STUDY ON WOMEN'S MEANINGFUL PARTICIPATION IN CYBERSECURITY WORKFORCE IN THE PUBLIC SECTOR IN THE WESTERN BALKANS

By Donika Elshani

Edited by Leonora Hasani

2025

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders.

DCAF's Foundation Council members represent over 50 countries and the Canton of Geneva. Active in over 70 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on Twitter @DCAF_Geneva.

DCAF - Geneva Centre for Security Sector Governance
Maison de la Paix
Chemin Eugène-Rigot 2E
1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch

Contributors

Editor: Leonora Hasani
Design & Layout: Elmæ Muslija

Disclaimer

Table of Contents

Introduction

The Western Balkans region is facing an increasing surge in advanced and sophisticated cyberattacks. A particularly notable incident occurred in July 2022 when Albania was targeted by a cyberattack attributed to the Iranian Foreign Ministry. This attack, which drew significant international attention, was believed to be retaliation for Albania's decision to shelter members of the Iranian opposition group Mujahedeen-e-Khalq (MEK).[1]

However, Albania is not alone in its struggles. According to a recent report by the Balkan Investigative Reporting Network (BIRN), Bosnia and Herzegovina, North Macedonia, Kosovo, and Serbia all experienced a significant rise in cyberattacks between 2020 and 2023, particularly phishing and ransomware incidents.[2]

In September 2022, Kosovo's Post-Telecommunication Authority fell victim to a targeted cyberattack that temporarily disabled its internal database and email systems.[3] That same month, a ransomware attack crippled the servers of the Parliament of Bosnia and Herzegovina, rendering its website and computers inaccessible for over two weeks.[4]

Meanwhile, in Montenegro and North Macedonia, various state institutions faced cyberattacks in 2022. Notably, North Macedonia's Ministry of Education was among the targets, while Montenegrin government servers were hit by ransomware attacks.[5][6] Serbia experienced an overwhelming surge in cyber threats, with approximately 40 million cyberattacks on Information and Communication Technology (ICT) systems between 2020 and 2021 alone.[7]

In response to these growing digital threats, governments in the region have taken steps to strengthen national cybersecurity strategies and institutional frameworks. To varying degrees, all Western Balkan countries have adopted laws regulating cybersecurity and information security.

---

1 Ayman Oghanna, "How Albania Became a Target for Cyberattacks," Foreign Policy, (March 25, 2023). https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/

2 Balkan Investigative Reporting Network (BIRN),, "Battle for Balkan Cybersecurity: Threats and Implications of Biometrics and Digital Identity," Balkan Insight, June 30, 2023. https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/

3 Emirjeta Vllahiu, "Kosovo to Establish Agency for Cyber Security Amid Recent Attacks," Balkan Insight, (September 14, 2022). https://balkaninsight.com/2022/09/14/kosovo-to-establish-agency-for-cyber-security-amid-recent-attacks/.

4 Azem Kurtic, "Bosnia Remains Silent on Hacker Attack on Parliament," Balkan Insight, (September 28, 2022). https://balkaninsight.com/2022/09/28/bosnia-remains-silent-on-hacker-attack-on-parliament/.

5 Samir Kajosevic, "Montenegro Still Assessing Damage From Mystery Cyber Attacks," Balkan Insight, (August 29, 2022). https://balkaninsight.com/2022/08/29/montenegro-still-assessing-damage-from-mystery-cyber-attacks/.

6 Sinisa Jakov Marusic, "North Macedonia Ministry Confirms New Hacking Attack," Balkan Insight, (February 7, 2022). https://balkaninsight.com/2022/02/07/north-macedonia-ministry-confirms-new-hacking-attack/.

7 Balkan Investigative Reporting Network (BIRN),, "Battle for Balkan Cybersecurity: Threats and Implications of Biometrics and Digital Identity," Balkan Insight, June 30, 2023. https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/

They have also developed National Cybersecurity Strategies and Action Plans aimed at identifying, assessing, and mitigating cyber risks. Institutional bodies have been established to coordinate efforts with security institutions, sectoral Computer Emergency Response Teams (CERTs), and international authorities to uphold effective cybersecurity safeguards.[8]

However, significant challenges remain in enforcement and the practical implementation of these strategies.[9] The region's technical capacity lags behind, with outdated systems and equipment exacerbating vulnerabilities. Additionally, the lack of collaboration between government organizations and private sector actors hinders the effective execution of cybersecurity frameworks.[10] Compounding these issues is a widespread lack of awareness about cyber risks across various sectors of Western Balkan societies, making it difficult to foster a resilient and security-conscious community.

Another defining characteristic of the cybersecurity field is its gender imbalance. Globally, women comprise less than 24% of the cybersecurity workforce, and only 1% hold top executive positions.[11] In the Western Balkans, female representation in ICT sectors, technology startups, and high-level managerial roles remains low.[12] According to the Western Balkans Digital Society Index, women account for just 19% of ICT specialists in the region, highlighting a significant gender disparity.[13] The highest concentration of women in the workforce is found in traditionally female-dominated fields such as teaching and nursing, where they play a crucial role in public education and healthcare.[14] This trend reflects persistent gender disparities in Science, Technology, Engineering, and Mathematics (STEM) education.[15] University enrolment data from 2017 to 2023 reveals a stark imbalance in female participation in ICT studies, largely due to limited early exposure to the field.[16]

---

8 Irina Rizmal, "Legal and policy frameworks in Western Balkan economies on PPPs in cybersecurity" Geneva Center for Security Sector Governance (DCAF), 2023.

9 INSTRUMENT FOR PRE-ACCESSION ASSISTANCE (IPA II) 2014-2020. https://neighbourhood-enlargement.ec.europa.eu/document/download/1fb8ced5-0608-4083-a2cf-39d87426e302_en

10 Ornela Sollaku, "AI for Good Governance and Cybersecurity in the Western Balkans: Opportunities and Challenges" DCAF, 2023. https://www.dcaf.ch/sites/default/files/imce/ECA/OrnelaSollaku_Young-faces2023.pdf

11 CyberSN, "Improving Female Representation in Cybersecurity" https://cybersn.com/improving-female-representation-in-cybersecurity/#:~:text=The%20State%20of%20Women%20in,under%2030s%20category%20are%20women

12 Jenny Drezin, "Digitally empowered Generation Equality: Women, girls and ICT in the context of COVID-19 in selected Western Balkan and Eastern Partnership countries" International Telecommunication Union and UN Women, 2021. https://eca.unwomen.org/en/digital-library/publications/2021/3/digitally-empowered-generation-equality-women-girls-and-ict-in-the-context-of-covid-19

13 Vesna Tintor, Nikola Jovanovic, Veronica Bocarova and Mihailo Bugarski, "WESTERN BALKANS DIGITAL ECONOMY SOCIETY INDEX 2022" Regional Cooperation Council, (December, 2022). https://www.balkaninnovation.com/docs/38/western-balkans-digital-economy-society-index-wb-desi-2022-report.

14 Ibid.

15 Mexhid Ferati, Venera Demukaj, Erdelina Kurti, Christina Mortberg, Kamal Shahrabi and Mihone Kerolli Mustafa, "Gender Stereotypes and Women Participation in STEM Fields in the Western Balkans: A Scoping Review" Richtmann Publishing, (March, 2023). https://doi.org/10.36941/ajis-2023-0044.

16 Elva Leka, Luis Lamani and Enkeleda Hoxha, "Equity in Bytes: An In-Depth Analysis of Gender Disparities in the ICT Sector Across Albania and Western Balkans Countries - Insights, Challenges, and Strategies for Promoting Inclusion and Empowerment" TEM Journal, May 2024. https://www.temjournal.com/content/132/TEMJournalMay2024_1580_1588.pdf

Promoting gender equality in the ICT sector, particularly within cybersecurity, is essential for driving innovation, accelerating technological advancement, and fostering economic growth.[17] More importantly, including women in cybersecurity is critical because they, along with other marginalized groups, are disproportionately affected by cyberattacks. Cyber violence has a particularly severe impact on women and girls, leading to psychological harm and discouraging their participation in political and social life. In the Western Balkans, digital technologies, including social media platforms, have created new avenues for abuse in a region where gender-based violence remains a serious concern.[18] Cyberbullying, revenge porn, and digital harassment are among the growing threats. A recent case that sent shockwaves across the region involved "Albkings," a notorious Telegram group with over 100,000 members from Kosovo, Albania, and North Macedonia. Members of this group shared personal information of women and girls without their consent, including minors, highlighting the urgent need for stronger protections against cyber violence.[19]

Methodology

This report examines women's participation in the cybersecurity workforce within the public sector of the Western Balkans. Its primary objective is to identify barriers and challenges that women may face before, during, and after entering cybersecurity roles. Additionally, it provides concrete policy recommendations for public policymakers to foster greater inclusion and meaningful participation of women in cybersecurity roles.

For this study, the Geneva Centre for Security Sector Governance (DCAF) designed two questionnaires to assess women's participation in the cybersecurity workforce across the Western Balkans. One questionnaire was distributed to individual women working in cybersecurity within the public sector, aiming to identify and assess the challenges and opportunities they encounter. The participants were selected based on their involvement in past DCAF activities. This questionnaire focused on participants' professional profiles, including their sector, position level, role, and career longevity.

The second questionnaire was sent to representatives of Women4Cyber (W4C) operating in Western Balkan countries. Women4Cyber is a non-profit European foundation dedicated to promoting, encouraging, and supporting women's participation in cybersecurity. This questionnaire sought insights into W4C's experience in supporting women in the field, whether similar studies had been conducted, if they maintained relevant databases, and how country-specific public policies might have influenced women's participation in cybersecurity.

---

17 Ibid

18 European Institute for Gender Equality, "Cyber violence against women and girls," (2017). https://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls.pdf

19 Donika Elshani and Diona Budima, " Misogyny in the Albanian Manosphere" The Case of 'Albkings'," (2024). https://balkaninsight.com/wp-content/uploads/2024/06/THECASE-OF-ALBKINGS.pdf

Both questionnaires explored women's experiences as they enter and progress in the workforce. The first set of questions examined employment criteria and their impact on women's participation, including barriers to entry, existing measures to encourage candidacy (such as targeted campaigns), recruitment or advancement quotas, and gender-equal selection processes. The second set of questions focused on women's experiences during their careers, including fair treatment, the impact of preconceived attitudes, and other obstacles to career progression in cybersecurity.

This study presents a qualitative analysis of the data collected from both questionnaires. The findings are organized around key themes that emerged from participants' responses, outlining the main challenges and opportunities for women in the cybersecurity public sector. Special attention is given to comparing responses across different Western Balkan countries to highlight potential country-specific trends.

Additionally, by drawing on selected best practices from European countries that have successfully implemented policies to enhance women's participation in the cybersecurity workforce—such as the UK, Netherlands, Germany, Sweden, and France—this report aims to provide actionable recommendations tailored to the region's specific challenges and institutional frameworks.

The findings of this report are not exhaustive, as the study's participant pool is limited. As a result, while the findings offer a general first impression, they do not allow for a more in-depth analysis of differences and similarities between Western Balkan countries or variations in experiences within individual countries. Additionally, participants varied in the length and detail of their responses, further limiting the depth of analysis. To build on these insights, further research is needed to explore the emerging themes in greater detail. This could include expanding the participant pool, conducting individual interviews to allow for more in-depth responses, and organizing focus groups with target audiences.

Key findings and analysis

The respondents of the first survey conducted for this study are women working in the cybersecurity workforce within the public sector across various Western Balkan economies, including Montenegro, Kosovo, Serbia, and Albania. Their positions range from intermediate staff to executive and first-level management roles. Their experience in cybersecurity varies from a few months to 14 years.

Their responsibilities span a wide range of functions, including implementing preventive measures, assessing vulnerabilities to enhance security, engaging in strategic planning and project management, and overseeing governance and compliance within their institutions.

Specific roles mentioned include **Head of International Projects Coordination and Strategic Development, Specialist in Governance and Compliance, and IT Security Administrator**.

The respondents of the second survey represent various **Women4Cyber** chapters operating in the Western Balkans, including **Bosnia and Herzegovina, Kosovo, Montenegro, and Serbia**. Their responses regarding the existence of databases for women in the cybersecurity workforce vary:

- **Women4Cyber Bosnia and Herzegovina** maintains a list of women in cybersecurity, but it is not publicly accessible.
- **Women4Cyber Kosovo** has established a database, but it remains private due to the sensitive nature of the information.
- **Women4Cyber Montenegro** currently lacks an official national database.
- **Women4Cyber Serbia** has a database, but it is not publicly available due to Serbia's **Data Privacy Law.**

These responses highlight ongoing challenges related to the transparency and accessibility of information on women in cybersecurity across the region.
In the following section, the main survey findings will be organized into thematic areas based on responses from women in cybersecurity positions within public institutions in the Western Balkans, as well as insights from **Women4Cyber (W4C) regional representatives.**

3.1. Measures that ensure a fair recruitment process

In both questionnaires and across Western Balkan (WB) countries, respondents indicated that legal frameworks in their respective countries do not impose formal barriers to women's involvement in the public sector. However, while general gender equality policies exist, they lack the specificity and enforcement needed to significantly increase women's participation in technical fields such as cybersecurity.
Respondents highlighted the absence of targeted policies or initiatives to support recruitment, retention, and advancement. Specifically, recruitment processes lack gender quotas, and gender-balanced selection panels are not consistently applied across public institutions, contributing to persistent gender disparities in hiring and promotion. In **Bosnia and Herzegovina**, for example, the **Law on Gender Equality**—while designed to prevent gender-based discrimination—also restricts targeted recruitment campaigns for women, potentially limiting proactive measures to boost female participation. Across all Western Balkan countries, the reliance on general gender equality laws without targeted initiatives or quotas has resulted in limited systemic support for women in cybersecurity.

Notably, while responses from the **Women4Cyber (W4C)** questionnaire indicate consistent similarities across WB countries, responses from the **individual questionnaire** reveal a divide in perceptions regarding the challenges women face in cybersecurity. While most respondents believe recruitment processes are formally equal, opinions vary on what the real challenges are. Some argue that the absence of formal recruitment barriers ensures fairness, while others recognize that **formal measures alone do not necessarily translate into equality in practice**. These respondents emphasize the need for **proactive measures to address unconscious biases and structural barriers**.

The absence of targeted initiatives to support women in cybersecurity is a recurring theme, with only a few institutions taking concrete steps to address gender disparities. This highlights the broader need for policies and programs that actively promote gender equality in **cybersecurity recruitment, retention, and career advancement.**

3.2. Workplace culture and lack of supportive networks

The main workplace challenges reported across the Western Balkans include a **male-dominated work culture, career advancement barriers, and the lack of support systems**. Patriarchal norms and the perception of cybersecurity as a male-dominated field make it difficult for women to access the same opportunities as men, particularly in terms of **salary and promotions**. Women in leadership roles often struggle to assert their authority, as they are frequently **undermined by male colleagues**. Additionally, they are held to **higher standards**, with respondents noting that women in leadership positions are expected to always perform flawlessly, as their mistakes are judged more harshly than those of their male counterparts. Meanwhile, men often benefit from more relaxed and informal work relationships, which can lead to favoritism in promotions and career opportunities.

Furthermore, women face difficulties finding **inclusive environments and structured support networks**, such as mentorship programs, access to key projects, and training opportunities. Without these support systems, they often struggle to build the **professional connections and visibility** needed to advance in their careers. The absence of an inclusive workplace culture and robust support mechanisms **hinders their ability to thrive and reach their full potential** in the field.

3.3. Cultural norms fueled by gender-based stereotypes and assumptions about work-life balance

According to survey respondents, **traditional gender roles and societal expectations** significantly influence perceptions of women's capabilities in technical fields such as cybersecurity.

The main barriers to women's participation and advancement in the Western Balkans include **stereotypes about technical competence, a male-dominated workplace culture, and entrenched gender norms**.

Technical professions are often regarded as **"masculine"**, fostering the belief that women are less skilled or competent—especially in cybersecurity analysis, cyber engineering, and threat intelligence, which are traditionally seen as male-dominated fields.[20] This perception discourages women from entering the sector and can **undermine their confidence**, leading them to question their own competence. Over time, this can result in a **lower sense of self-efficacy** among women in cybersecurity.

Additionally, respondents highlighted workplace culture as a barrier, with women often **marginalized or underrepresented** in key projects and leadership positions, limiting their career advancement. The **deep-rooted patriarchal culture** and resistance to gender equality among decision-makers—who are predominantly male—further hinder women's progress in the cybersecurity sector across the Western Balkans.

Closely linked to these cultural norms are **assumptions about work-life balance and women's availability** for cybersecurity roles. There is a widespread belief that cybersecurity positions—often demanding long hours and a high level of commitment—are **less suitable for women**, who are expected to juggle work with family responsibilities. This leads to the assumption that women are **less committed to their careers**, as they are presumed to prioritize family obligations over professional aspirations.

Respondents also noted that many workplaces **lack flexible work policies**, such as remote work options, flexible hours, and adequate parental leave—all of which are essential for balancing professional and personal responsibilities.

Family constraints can significantly impact women's ability to pursue cybersecurity careers, though the extent varies based on individual circumstances and available support systems. However, some respondents observed a **positive trend among younger generations**, who appear l**ess constrained by traditional gender roles**. These younger women are more proactive in seeking out **support networks and flexible work arrangements**, enabling them to better balance professional and family responsibilities. As a result, they are increasingly able **to pursue cybersecurity careers without being held back by outdated societal expectations**, signaling a potential shift in the industry's landscape.

---

20 Meraiah Foley and Sulagna Basu, "Decoding the gendered imaginary of cybersecurity careers: a social shaping of technology perspective" Information, Communication & Society, (August 17, 2024). https://www.tandfonline.com/doi/full/10.1080/1369118X.2024.2391818#d1e260

3.4. Lack of female role models/mentors in leadership positions

When asked about women's participation in the cybersecurity field, most respondents acknowledged a positive upward trend in women's engagement across both the private and public sectors, despite the challenges previously discussed. They noted a growing awareness of diversity's importance and a stronger commitment to fostering inclusive environments within organizations. However, a significant gap remains: women in the cybersecurity workforce in the Western Balkans are rarely found in managerial, high-level, or executive positions. This disparity is evident among the respondents themselves—of the women currently working in cybersecurity roles within public institutions in the region, only one reported holding an executive management position. The underrepresentation of women in leadership roles can largely be attributed to the lack of role models and mentors within the cybersecurity sector. Few senior women hold prominent cybersecurity positions, limiting opportunities for younger professionals to receive guidance and see examples of success. Unfortunately, this issue extends beyond cybersecurity. A regional comparative report on women's employment in the Western Balkans, using 2020 data, shows that managerial positions constitute the smallest occupational category for women across the region. In Albania, only 1.1% of women are employed in managerial roles, while in Kosovo, this figure rises to just 6.3%. In North Macedonia, women occupy about one in five managerial positions, and in Bosnia and Herzegovina, they hold approximately one in four.[21]

3.5. Prospects for the future

The W4C questionnaire also allowed respondents to reflect on whether they have observed recent improvements in cyber career opportunities for women in the public sector and how these changes might relate to country-specific policies. Responses from country representatives highlight varied experiences and progress across the region.

In Kosovo and Montenegro, notable advancements have been reported, with initiatives like Women4Cyber playing a crucial role in raising awareness and providing mentorship, training, and networking opportunities for women in cybersecurity. In Kosovo, public policies promoting gender equality and inclusivity have supported this progress, though their direct impact on cybersecurity careers is still emerging. Similarly, in Montenegro, increased advocacy for gender equality—through initiatives such as Women4Cyber Montenegro and the CyberEqUal Together project—has expanded opportunities for women. However, Montenegro's representative stresses that while progress has been made, stronger public policies are needed to ensure sustainable improvements.

---

21 Esmeralda Shehaj, "Regional Comparative Report on Women's Employment in Western Balkans," Regional Cooperation Council, (May, 2022). https://www.esap.online/docs/188/rcc-esap-2-regional-comparative-report-on-womens-employment-in-western-balkans

In contrast, Serbia's representative reports no significant advancements, noting that although women are present in the public sector, none hold leadership positions. Bosnia and Herzegovina's representative is similarly pessimistic, citing a shortage of cybersecurity specialists and emphasizing the need to leverage favorable social policies and a secure work environment to attract women to the field.

European best practices and public policies on women's inclusion in the cybersecurity workforce

Recognizing the importance of women in cybersecurity and the benefits of advancing gender equality in the sector, many European countries have adopted targeted policies and initiatives to increase women's participation in the workforce. These efforts include inclusive recruitment and training programs, flexible work arrangements, public-private partnerships, and mentorship initiatives. The following section provides an overview of case studies from across Europe that can serve as models for adoption in the Western Balkans.

Most European countries have introduced regulations and policies to promote gender representation in government agencies and public institutions. These measures include gender equality laws and strategies aimed at increasing women's leadership roles in both public and private sectors. For example, France's Law on Gender Equality mandates that public sector organizations, including cybersecurity agencies like the National Cybersecurity Agency of France (ANSSI), ensure at least 40% of senior and executive positions are held by women.[22] Additionally, various European countries have enacted work-life balance policies, such as flexible work arrangements and generous parental leave, to help retain women in the workforce. Sweden stands out in this regard, offering up to 480 days of paid parental leave—shared between both parents—with 80% salary coverage for the first 390 days, along with flexible working hours and remote work options.[23]

While these institutional developments are significant, they are not specifically targeted at the cybersecurity sector. Therefore, it is crucial to examine examples of initiatives directly promoting gender inclusion in the cybersecurity workforce. Some of the most effective efforts focus on attracting young women to cybersecurity early on. A prime example is the UK's National Cyber Security Centre's **CyberFirst** initiative, which provides scholarships, training, and internships to equip young women with the skills and knowledge needed for cybersecurity careers.[24]

22 https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/510024/IPOL_IDA(2015)510024_EN.pdf

23 https://www.forsakringskassan.se/english/parents/when-the-child-is-born/parental-benefit?utm_source=chatgpt.com

24 https://www.ncsc.gov.uk/cyberfirst/overview

Another successful approach has been forging partnerships with non-governmental organizations to support women's inclusion in cybersecurity. **Women4Cyber** and **Women in CyberSecurity (WiCyS)** are two leading global organizations dedicated to increasing women's participation in the field.[25][26] The **WiCyS UK affiliate**, for instance, collaborates with the UK government, private sector leaders, and universities to create pathways for women through educational initiatives, mentorship programs, and job placements. Similarly, the **Women in Cybersecurity Community Association** in the Netherlands works with businesses, the Dutch government, and universities to offer educational opportunities for aspiring female cybersecurity professionals.

Policy recommendations for enhancing women's inclusion in the cybersecurity workforce in the Western Balkans

Although the underrepresentation of women in cybersecurity is a global issue, it is particularly pronounced in the Western Balkans due to deep-rooted patriarchal norms and resistance to gender equality among predominantly male decision-makers. As previously noted, the male-dominated workplace culture fosters prejudice and informal barriers that significantly impact how women enter and advance in the field. While these challenges make structural change difficult, governments in the Western Balkans can implement targeted actions to gradually shift prevailing gender norms and dismantle gender-based stereotypes in technical sectors.

Harmonisation of legislation with the EU Work-Life Balance Directive

To ensure the meaningful participation of women in the workforce—including the cybersecurity sector—Western Balkan countries must implement family-friendly and gender-responsive policies. These should promote work-life balance, support shared caregiving responsibilities, provide adequate parental leave, and create inclusive workplace environments that accommodate the needs of working parents, especially mothers.

Parental leave policies and the distribution of unpaid labor vary significantly across the Western Balkans, directly affecting gender equality and women's workforce participation. Current labor laws in Kosovo and Albania grant fathers just three days of paid leave following the birth of a child.[27]

Additionally, contract termination due to pregnancy remains a common issue.
According to the Women's Rights Center in Montenegro, prevalent forms of workplace discrimination against women include interview questions about marriage and childbearing plans, as well

25 https://women4cyber.eu/our-goals/

26 https://www.wicys.org/

27 https://kvinnatillkvinna.org/wp-content/uploads/2024/11/The-Kvinna-till-Kvinna-Foundation-Womens-Rights-in-Western-Balkans-2024.pdf

as the dismissal of pregnant employees rather than offering temporary replacements.[28] In North Macedonia and Bosnia and Herzegovina, women are more likely to take career breaks or reduce their working hours to fulfill caregiving responsibilities. Meanwhile, in Serbia, women face multiple disadvantages, including a higher likelihood of lacking pension insurance and an increased risk of poverty.[29]

To enhance women's workforce participation, including in cybersecurity, Western Balkan countries should align their maternity leave legislation with the parental leave provisions of the **EU Work-Life Balance Directive**. This directive aims to create a more equitable environment for caregivers—particularly women—by promoting inclusive and supportive workplace policies across EU countries.

Advancing the inclusion of women and girls in cybersecurity through government-funded scholarship programs

One effective way to encourage women and girls in the Western Balkans to pursue careers in cybersecurity is by offering fully funded educational opportunities in this field. Similar to the **CyberFirst** program in the UK, governments in the region can collaborate with international organizations and donors to establish scholarship programs for women and girls to study cyber-related subjects at universities abroad.

A relevant example from the region is the **Young Cell Scheme**, the EU Postgraduate Scholarship Programme for Kosovo, co-funded by the European Union and the Government of Kosovo. Through this initiative, Kosovar students receive fully funded scholarships to study abroad and are required to return to Kosovo upon graduation to work in the civil service for three consecutive years.[30] Similar programs could be developed across the Western Balkans specifically to support women and girls in IT and cybersecurity. Scholarship recipients could be required to return to their home countries and work in public institutions responsible for cybersecurity policy, digital infrastructure protection, and cybercrime prevention.

In **November 2023**, the **University of Montenegro's Center for Interdisciplinary and Multidisciplinary Studies** received official accreditation for its **Master's program in Cyber Security—**the first of its kind in the region. This program allows both Montenegrin and international students to study cybersecurity at a public university in English.[31] To make the program more appealing to women and girls in the Western Balkans, the University of Montenegro could partner with IT, programming, and computer science departments at other public universities in the region. Potential initiatives could include student exchange programs and regional cybersecurity competitions specifically for female students.

28 https://womensrightscenter.org/wp-content/uploads/2022/04/GBD_in_Labour_in_Montenegro.pdf
29 https://kvinnatillkvinna.org/wp-content/uploads/2024/11/The-Kvinna-till-Kvinna-Foundation-Womens-Rights-in-Western-Balkans-2024.pdf
30 https://ycskosovo.org/index.php/en/about-the-programme/what-is-young-cell-scheme
31 https://akokvo.me/en/accredited-masters-interdisciplinary-study-programme-in-english-cyber-security/?utm_source=chatgpt.com

Fostering institutional partnerships with NGOs that support women's participation in the cybersecurity field

Several NGOs in the region actively contribute to the cybersecurity field, offering expertise, training programs, and capacity-building initiatives for various stakeholders. In the context of women's representation, it is important to highlight the **Women4Cyber (W4C)** chapters established across the Western Balkans, including in **Albania, North Macedonia, Serbia, Kosovo, Montenegro, and Bosnia and Herzegovina**. These sister organizations work to increase the number of women in cybersecurity by raising awareness, providing educational opportunities, facilitating knowledge exchange, and ensuring institutional oversight.[32]

Recently, the **W4C chapter in Kosovo** partnered with the **Cyber Security Challenge Kosova & Albania**, a collaborative event designed to foster regional cybersecurity talent while encouraging girls' participation and promoting gender inclusivity.[33] Additionally, several W4C chapters—including those in **Kosovo**[34], **North Macedonia**[35], **Montenegro**[36], and **Bosnia and Herzegovina**[37]—now offer free training for women and girls in **Governance**, **Risk**, and **Compliance (GRC)**. This initiative aims to equip participants with the skills to integrate GRC responsibilities into their professional roles across the public, private, and civil society sectors.

To enhance women's participation in cybersecurity, **governments in the Western Balkans should adopt a multi-stakeholder approach** when formulating and implementing cybersecurity policies. Organizations like W4C have built extensive networks of professionally trained women and girls in cybersecurity, serving as a valuable talent pool for public institutions and creating a direct recruitment pipeline for women in the sector. By fostering **public-private partnerships** with W4C and similar organizations, governments can leverage their expertise and industry connections to strengthen cybersecurity initiatives. Moreover, these organizations' direct engagement with women in the field provides critical insights into barriers to recruitment, retention, and career advancement—data that should inform the development of **gender-responsive public policies**.

32 https://women4cyber.eu/#

33 https://www.linkedin.com/company/cybersecuritychallengeal/posts/?feedView=all

34 https://www.linkedin.com/posts/women4cyber-kosovo_our-grc-training-program-launches-last-activity-7293266972388016130-6fEN?utm_source=share&utm_medium=member_desktop&rcm=ACoAACzBIFwB3uZtYcuFYpGkn5GbgT2n8PbwWi4

35 https://www.linkedin.com/posts/women4cyber-north-macedonia_analytics-risk-management-activity-7296066496022118400-adw_?utm_source=share&utm_medium=member_desktop&rcm=ACoAACzBIFwB3uZtYcuFYpGkn5GbgT2n8PbwWi4

36 https://www.linkedin.com/posts/women-4-cyber-montenegro_women4cybermontenegro-cybersecuritytraining-activity-7292104414599782407-zO9U?utm_source=share&utm_medium=member_desktop&rcm=ACoAACzBIFwB3uZtYcuFYpGkn5GbgT2n8PbwWi4

37 https://www.linkedin.com/posts/women4cyber-bosnia-and-herzegovina_cybersigurnost-women4cyberbih-grc-activity-7292538008451350528-2fp0?utm_source=share&utm_medium=member_desktop&rcm=ACoAACzBIFwB3uZtYcuFYpGkn5GbgT2n8PbwWi4

Conclusion and recommendations for new research pathways

This study highlights significant gender disparities and structural barriers that hinder women's participation in the cybersecurity workforce within the **Western Balkans public sector**. Despite legal frameworks nominally promoting gender equality in all these countries, the lack of **targeted recruitment, gender-aware selection processes, and retention policies** leaves systemic inequalities unaddressed, rendering these frameworks ineffective in practice.

Most respondents noted that while they do not face **formal** obstacles, the **male-dominated workplace culture**—reinforced by ingrained patriarchal societal norms—creates **prejudice and informal barriers** that significantly impact women's entry and advancement in the field. Additionally, **limited female representation in leadership roles** exacerbates the issue, as the scarcity of women in senior positions reduces mentorship opportunities for younger professionals, further curbing their career advancement.

However, there are signs of progress. Participants noted a growing awareness of the **importance of gender equality and the need to create more inclusive work environments.**

The findings raise several important questions that warrant further exploration. One critical area concerns **educational initiatives** that can encourage girls to engage in **STEM and ICT fields** from an early age. For example, would making certain **ICT-related subjects, such as coding, mandatory in school curricula** be an effective approach? Kosovo Prime Minister **Albin Kurti's** proposal to **introduce coding classes for students in grades 1 through 9** serves as an interesting case study.[38] How would such an initiative impact **girls' interest and involvement in technology**, and how might similar curriculum changes be adapted and implemented in other Western Balkan countries?

As the region faces **growing cybersecurity threats**, integrating more women into the field will be crucial—particularly in addressing **cyber threats that disproportionately affect women**. Future research with broader participation will be essential to build on these findings and drive meaningful change in the **Western Balkans cybersecurity workforce**. Including the perspectives of **male counterparts** to the women cybersecurity professionals interviewed in this study could provide valuable insights into **workplace dynamics** and highlight areas for improvement in fostering a more supportive environment for women.

38 Telegrafi, "Kurti: From next year, coding will be part of the school curricula of pre-university education", (December, 2023)

Based on this study's findings, several intersectional research pathways should be explored:

- **Intersectional studies** examining how factors such as **ethnicity, socioeconomic status, and geographic location** influence women's participation in cybersecurity.
- **Longitudinal studies** assessing the evolving challenges women face at different **career stages**.
- **Research on the impact of education and training**, particularly **access to STEM education and gender-equality training**.
- **Studies on gender-responsive programs** addressing **misogynistic cyberbullying and harassment**.
- **Analysis of fair recruitment and retention policies** to identify the most effective strategies for increasing women's representation.

Notably, given the significant variations in survey responses—particularly regarding **perceived challenges for women in cybersecurity**—future research should be both c**ross-sectional and longitudinal** to better evaluate the factors shaping these differences in perception. Additionally, **in-depth country-specific studies** are needed to complement the regional overview presented in this paper, providing more tailored insights into **the unique challenges faced by individual countries**.

Bibliography

Balkan Investigative Reporting Network. “Battle for Balkan Cybersecurity: Threats and Implications of Biometrics and Digital Identity.” Balkan Insight, (June 30, 2023). https://balkaninsight.com/2023/06/30/battle-for-balkan-cybersecurity-threats-and-implications-of-biometrics-and-digital-identity/.

Drezin, Jenny. “Digitally empowered Generation Equality: Women, girls and ICT in the context of COVID-19 in selected Western Balkan and Eastern Partnership countries.” International Telecommunication Union and UN Women, (2021). https://eca.unwomen.org/sites/default/files/Field%20Office%20ECA/Attachments/Publications/2021/5/Digitally%20empowered%20Generation%20Equality-min.pdf.

Elshani, Donika and Budima, Diona. “Misogyny in the Albanian Manosphere” The Case of ‘Albkings’.” Balkan Investigative Reporting Network (BIRN). (2024). https://balkaninsight.com/wp-content/uploads/2024/06/THECASE-OF-ALBKINGS.pdf.

European Institute for Gender Equality (EIGE). “Cyber violence against women and girls.” (2017). https://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls.pdf.

Ferati, Mexhid, Demukaj, Venera, Kurti, Erdelina, Mörtberg, Christina, Shahrabi, Kamal and Mustafa Kerolli, Mihone. “Gender Stereotypes and Women Participation in STEM Fields in the Western Balkans: A Scoping Review.” Richtmann Publishing 12(2). Doi: https://doi.org/10.36941/ajis-2023-0044.

Foley, Meraiah and Basu, Sulagna. “Decoding the gendered imaginary of cybersecurity careers: a social shaping of technology perspective.” Information, Communication & Society, 1-17. https://www.tandfonline.com/doi/full/10.1080/1369118X.2024.2391818.

Instrument for Pre-Accession Assistance (IPA II) 2014 - 2022. “MULTI-COUNTRY EU support to cybersecurity capacity building in the Western Balkans.” European Commission. https://neighbourhood-enlargement.ec.europa.eu/document/download/1fb8ced5-0608-4083-a2cf-39d87426e302_en.

Jakov Marusic, Sinisa. “North Macedonia Ministry Confirms New Hacking Attack.” Balkan Insight, (February 7, 2022). https://balkaninsight.com/2022/02/07/north-macedonia-ministry-confirms-new-hacking-attack/.

Kajosevic, Samir. “Montenegro Still Assessing Damage From Mystery Cyber Attacks.” Balkan Insight, (August 29, 2022). https://balkaninsight.com/2022/08/29/montenegro-still-assessing-damage-from-mystery-cyber-attacks/.

Kurtic, Azem. “Bosnia Remains Silent on Hacker Attack on Parliament.” Balkan Insight, (September 28, 2022). https://balkaninsight.com/2022/09/28/bosnia-remains-silent-on-hacker-attack-on-parliament/

Leka, Elva, Lamani, Luis, and Hoxha, Enkeleda. “Equity in Bytes: An In-Depth Analysis of Gender Disparities in the ICT Sector Across Albania and Western Balkans Countries - Insights, Challenges, and Strategies for Promoting Inclusion and Empowerment.” TEM Journal 13 (2), 1580-1588. Doi: 10.18421/TEM132-71.

Oghanna, Ayman. “How Albania Became a Target for Cyberattacks.” Foreign Policy, (March 25, 2023). https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/.

Rizmal, Irina. “Legal and policy frameworks in Western Balkan economies on PPPs in cybersecurity.” Geneva Center for Security Governance (DCAF), (2021). https://www.dcaf.ch/sites/default/files/imce/ECA/LegalPolicyFrameworksCS_PPPs_WB_mar2021.pdf.

Shehaj, Esmeralda. “Regional Comparative Report on Women’s Employment in Western Balkans.” Regional Cooperation Council. (May, 2022). https://www.esap.online/docs/188/rcc-esap-2-regional-comparative-report-on-womens-employment-in-western-balkans.

Sollaku, Ornela. “AI for Good Governance and Cybersecurity in the Western Balkans: Opportunities and Challenges.” Geneva Center for Security Governance (DCAF) - Young Faces 2023, (2023). https://www.dcaf.ch/sites/default/files/imce/ECA/OrnelaSollaku_Young-faces2023.pdf.

Telegrafi. “Kurti: From next year, coding will be part of the school curricula of pre-university Education”, (December, 2023). https://telegrafi.com/en/From-next-year%2C-coding-will-be-part-of-the-school-curricula-of-pre-university-education/

Tintor, Vesna, Jovanovic, Nikola, Bocarova, Veronica and Bugarski, Mihailo. “WESTERN BALKANS DIGITAL ECONOMY SOCIETY INDEX - WB DESI 2022 Report.” Regional Cooperation Council. (December, 2022). https://www.balkaninnovation.com/docs/38/western-balkans-digital-economy-society-index-wb-desi-2022-report.

Vllahiu, Emirjeta. “Kosovo to Establish Agency for Cyber Security Amid Recent Attacks.” Balkan Insight, (September 14, 2022). https://balkaninsight.com/2022/09/14/kosovo-to-establish-agency-for-cyber-security-amid-recent-attacks/.

DCAF Geneva Centre for Security Sector Governance

Chemin Eugène-Rigot 2E
P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 22 730 94 00

www.dcaf.ch