DCAF Geneva Centre for Security Sector Governance

DCAF Young Faces 2026

Teo Milanković

Cyber Ambassadors of the Western Balkans: Empowering Youth for Regional Cyber Capacity & Cooperation

By:Teo Milanković

DCAF Young Faces 2026 Participant

Table of Contents

1.0 Abstract

The focus of this policy is the proposal of an effective method that will help combat cybersecurity threats in the Western Balkans. Every day, there are new threats targeting both public institutions and private organizations, and the situation is only getting worse. Recent research data indicate that cyber incidents in the region increased by approximately 40% within a year, while ransomware attacks rose by 200% over two years.[1] These trends not only show the rising frequency of attacks but also the evolution and improvement of the tools used for malicious activities. More than ever the region needs innovative approaches to cybersecurity improvement and general protection overhaul.

Recognizing the potential of young people as the changemakers, the **„Cyber Ambassadors of the Western Balkans“** initiative aims to utilise youth talent to improve regional cyber resilience. Drawing inspiration from the „Young European Ambassadors (YEA) programme“, which engages youth in the Western Balkans to promote EU values and civic activism, this initiative envisions intensive education and practical training for selected youth leaders.[2] Through training, students gain knowledge of cybersecurity threats, international practices and collaborative problem-solving strategies-becoming Cyber Ambassadors.

An important part of this paper is also using the existing regional structures, such as the „Western Balkans Cyber Camp“ that offers hands-on experience in cyber governance. While effective for skills development, these programs alone do not fully integrate youth into decision-making processes. The Cyber Ambassadors model addresses this gap by fostering **active** involvement in policy discussions, collaboration with law enforcement, and, most importantly, outreach to educational institutions. Accomplishing all of the above would establish a long-term support system needed in the Balkans!

The establishment of the **Western Balkans Cyber Capacity Centre (WB3C)** would offer a complementary platform for ongoing training and cross-border cooperation.[3,4] Cyber Ambassadors could use such structures to facilitate regional exchanges of successful practices.[5] This approach mirrors EU and UN frameworks for youth engagement in cybersecurity, demonstrating that structured participation enhances both technical and governance capacity.[6,7]

One of the core components of this initiative is engaging the peer-to-peer education in primary and secondary schools. Cyber Ambassadors (in cooperation with local law enforcement) would deliver seminars and workshops to spread cyber hygiene awareness and safe online practices among all young students. By empowering youth to teach their peers, the program fosters a sustainable culture of cybersecurity awareness!

In addition to all campaigns, ambassadors must participate in cross-national collaboration, connecting with counterparts to share their personally developed strategies and insights. This borderless approach among the WB region reflects the reality that cyber threats do not respect national boundaries. By combining education, engagement, and institutional cooperation, the **Cyber Ambassadors of the Western Balkans** initiative aims to strengthen youth-led capacity building and contribute to a safer, more resilient digital environment.

2.0 Problem Identification

Bosnia and Herzegovina faces a serious and growing cybersecurity problem affecting public institutions, the private sector, and citizens. In recent years, **millions of cyberattacks** have been recorded, clearly showing the intensity and prevalence of threats. For example, the **Cyber Threat Report** shows that **BiH experienced over 9.2 million different cyberattacks during one month of monitoring in 2022**, with DDoS attacks being the most common, targeting critical systems and services[8]. This figure is supported by media reports stating **over 15.4 million cybersecurity threats in BiH by August 2023**, including multi-million attacks on both private and public networks[9].

Beyond the number of incidents, statistics reveal **structural weaknesses** in BiH: the country **lacks a national cybersecurity framework, a national strategy, and a centralized CERT team**, leaving attacks unaddressed at a systemic level[10]. Vulnerabilities also stem from **limited institutional capacity and awareness of cyber risks**, which further hinders the effective protection of infrastructure and citizens' data[11].

The private sector, particularly small and medium-sized enterprises that make up about **97 % of all registered companies**, shows very low digital maturity and advanced security measures. Approximately **90 % of these companies lack adequate systemic cybersecurity approaches, and 70 % do not have robust backup systems**, increasing exposure to attacks and data loss[12].

This combination of **high threat volume, structural gaps in protective measures, and low cybersecurity awareness** makes BiH extremely vulnerable to attacks that could paralyze key government systems, businesses, and critical infrastructure highlighting the urgent need for targeted policies, educational programs, and institutional capacity building.

2.1 How Does This Impact Us?

Cybersecurity problems in Bosnia and Herzegovina affect everyone. They impact institutions, businesses, and citizens. They are not just pure numbers. Millions of attacks happen every month. In one monitored month, there were over 9.2 million attacks in BiH. By some estimates, there were more than circa 15 million threats in a year[13]. These attacks target both government systems and private companies. They make digital services less safe and reduce trust in online platforms[14].

Institutions struggle because the country does not have a full national cybersecurity strategy or a centralized CERT team[15]. This means attacks can disrupt government services, damage data, and slow down public services like e-government or the judicial system[16].

For citizens, the risks are real. Weak cybersecurity exposes people to identity theft, financial fraud, and stolen personal data[17]. Many people do not know how to protect themselves online.

Businesses are also affected. Small and medium enterprises make up almost 97 percent of companies in BiH. Most of them do not have proper cybersecurity plans or backup systems[18]. This leaves them vulnerable to data loss, financial harm, and operational downtime.

Economically, this slows down digital growth. Investors see the risks. Digital service adoption is slower. The country falls behind its neighbors in digital development[19].

3.0 Cyber Ambassadors of the Western Balkans

The **„CAWB“** initiative is a regional programme that brings young people to the centre of efforts to strengthen cybersecurity capacity and resilience. The idea is simple but urgent. The Western Balkans face rising cyber threats, but educational systems and formal institutions have not yet equipped young people with the skills they need to respond effectively. The gap between digital exposure and practical cybersecurity knowledge is wide, and this leaves both youth and society vulnerable. Engagement in cybersecurity education and training is low, and national strategies do not yet fully integrate youth contributions into policy and response frameworks[21] [23].

The "Cyber Ambassadors" model builds upon proven traditions of educational exchange and youth diplomacy. It draws inspiration from initiatives like the Council of Europe’s Youth Peace Ambassadors programme extending these principles specifically to cybersecurity cooperation[43]. This innovative capacity-building tool aligns with emerging UN youth engagement agendas[7] and the recommendations of the United Nations Open-ended Working Group (UN OEWG) which emphasize the inclusion of young professionals in cyber affairs[44]. Furthermore, the initiative leverages existing frameworks such as DCAF’s Young Faces programme[45]. Tracking the alumni outcomes of such programs demonstrates that peer exchange effectively builds trust and creates enduring channels for dialogue that persist as participants advance in their careers.

The programme trains selected participants intensively in both technical and practical aspects of cybersecurity. Young people learn to recognise threats, to understand how systems are attacked, and to apply protective measures in real settings. They also learn about **policy, governance and international cooperation**, so they can meaningfully take part in high-level discussions and contribute to designing local and regional responses. Training involves expert-led workshops, hands-on simulations and collaborative problem solving. The goal is not just to produce technically capable individuals but to nurture young leaders who can interpret complex digital challenges and communicate solutions effectively[21] [23].

Integration with existing regional platforms like the **Western Balkans Cyber Camp** and **Western Balkans Cyber Capacity Centre (WB3C)** creates strong support structures for continuous learning. At these events and centres, youth interact with cybersecurity professionals, public officials, and experts from civil society, which strengthens networks and deepens practical understanding of real threats. For example, the **Western Balkans Cyber Camp** gathered students from across the region to practice threat detection and learn from

incident response exercises provided with support from national CSIRTs and international partners[20]. The establishment of WB3C itself shows how regional collaboration can create hubs for ongoing education and cooperation in cybersecurity, with training targeting all Western Balkan countries and repeated programmes focused on cyber hygiene, cybercrime and cyber diplomacy[24].

The **role of youth outreach** in this model is central. Once trained, Cyber Ambassadors run workshops and awareness sessions in schools, universities and community groups. These sessions address digital safety, safe behaviour online, and basic steps to avoid common threats. Practical research shows that improving digital literacy and critical thinking skills is directly linked to safer online behaviour among students and better digital well-being overall[25]. When young people teach their peers, the impact spreads rapidly and becomes part of everyday digital habits. This is especially important in regions like Bosnia and Herzegovina, where research shows significant gaps in online safety awareness, digital rights awareness and protections for youth online[14].

Finally, the programme emphasises **cross-border cooperation** and network building. Cyber challenges do not stop at national borders and youth capacity-building must be coordinated regionally. This mirrors broader EU and international approaches that link youth empowerment with digital resilience and rights, such as projects boosting digital skills and participation in digital democracy across the Western Balkans and EU partners[26]. By connecting trained ambassadors across countries, the initiative fosters a shared sense of responsibility, teamwork and coordinated action against common threats.

3.1 Focus point

The **main objective** of the Cyber Ambassadors initiative is to develop a strong, youth-driven network of skilled and knowledgeable individuals across the Western Balkans who can contribute to cybersecurity capacity at local, national and regional levels.

The first objective is **advanced cybersecurity skills development**. Participants receive comprehensive training on threat detection, incident response, secure practices and cyber governance. They gain practical experience through simulations and exercises, which helps them move from theoretical knowledge to real-world application. This objective addresses the recognised regional shortage of cybersecurity professionals and the need for improved digital skills among young people[13].

The second objective is to **bridge the gap between technical skills and policy engagement**. Cybersecurity is as much about governance, law and strategy as it is about code and computers. The programme ensures that ambassadors understand how policies are formed, how legal frameworks operate, and how to advocate for better protections. This also prepares them to contribute to discussions with institutions, policymakers and regional forums.

The third objective is **community outreach and education**. Cyber Ambassadors run workshops and awareness sessions in educational institutions and community groups. This

peer-to-peer approach strengthens digital literacy, encourages safe online behaviour, and spreads foundational cybersecurity knowledge widely. Research shows that increased literacy directly influences digital well-being and reduces risky behaviour online[25].

The fourth objective is **regional collaboration and harmonisation**. The initiative connects youth across different Western Balkan countries, fosters knowledge sharing, and supports participation in regional and European cybersecurity activities. Examples like national cybersecurity competitions and youth challenges show how structured collaboration increases interest, participation and long-term commitment to cybersecurity fields[26].

The fifth objective is **career development and economic resilience**. By equipping youth with recognised skills and practical experience, the initiative helps close the cybersecurity skills gap and improves job prospects in a field that is growing rapidly in demand. Skilled cybersecurity professionals are highly employable and have a direct impact on the digital economy's growth and security[9]. Training young people in cybersecurity thus supports **both individual opportunities and regional economic resilience**.

Together, these objectives create a holistic framework for youth to become active contributors to cybersecurity resilience, not just beneficiaries of training. They foster a generation that is informed, skilled, connected and ready to respond to evolving digital threats.

4.0 Implementation Strategy

The **implementation of the Cyber Ambassadors of the Western Balkans** initiative is designed to be phased, structured, and regionally coordinated. The first phase focuses on **recruitment and selection**. Candidates are chosen from secondary schools, universities, and youth organisations across all Western Balkan countries. Selection is based on interest in technology, motivation to contribute to cybersecurity, and potential for leadership. Diversity is a key principle. The programme ensures representation from urban and rural areas, from different socio-economic backgrounds, and across genders[27].

The second phase is **training and capacity building**. Selected youth participate in intensive workshops, seminars, and practical exercises. Training covers threat detection, secure digital practices, incident response, policy and governance, and cross-border collaboration. The programme leverages regional centres, such as the **Western Balkans Cyber Camp** and **WB3C**, to provide realistic simulations and access to expert mentors[28]. Ambassadors gain skills not only in technical areas but also in communication, peer teaching, and policy engagement.

The third phase focuses on **peer-to-peer outreach and community engagement**. Ambassadors are assigned schools, universities, and local youth groups where they deliver workshops on cyber hygiene and online safety. This multiplies the programme's impact, allowing knowledge to spread beyond the trained ambassadors. By targeting younger students, the initiative builds long-term habits of digital awareness and resilience[29].

The fourth phase is **cross-border collaboration and regional networking**. Ambassadors participate in regional conferences, joint exercises, and knowledge exchanges. They share experiences and best practices with peers in other countries. This phase strengthens regional ties and ensures a coordinated approach to cyber threats, reflecting the borderless nature of cybersecurity challenges[30].

Finally, the programme integrates **career and professional development**. Ambassadors receive mentorship, access to internships with regional institutions, and opportunities to contribute to real cybersecurity projects. This ensures that skills gained translate into employment, entrepreneurship, or further education in cybersecurity fields[31].

4.1 Monitoring process

Monitoring is embedded in every stage of the programme. During **training**, progress is tracked through practical assessments, simulations, and project work. Participants must demonstrate technical competencies, understanding of policy frameworks, and ability to communicate solutions effectively.

During **community outreach**, ambassadors submit activity reports detailing workshops conducted, number of participants reached, and qualitative feedback from attendees. Regional coordinators review these reports to ensure consistency, effectiveness, and quality of engagement[32].

Monitoring also evaluates **regional collaboration**. Ambassadors' participation in cross-border activities is tracked through attendance records, peer evaluations, and collaborative project outputs. Regular surveys and interviews measure the ambassadors' understanding of regional threats and ability to share knowledge with peers[33].

4.2 Evaluation process

Evaluation focuses on **impact, sustainability, and improvement**. At the end of each programme cycle, independent assessments measure how well objectives were achieved. Metrics include the number of trained ambassadors, outreach reach, improvement in participants' skills, and measurable increases in cybersecurity awareness in schools and communities[34].To ground the proposal and demonstrate minimum viability, the evaluation process will also rely on clear success metrics. For example, a primary benchmark for success will be that after one year of the programme, at least 80% of participants report establishing and maintaining new cross-border professional contacts.

Evaluation also examines **long-term outcomes**. This includes career progression of participants, continued engagement in cybersecurity projects, and the establishment of regional networks that persist beyond the programme cycle. Lessons learned are used to adjust training modules, improve outreach methods, and strengthen collaboration with regional institutions[35].

To transition the Cyber Ambassadors initiative from a conceptual proposal to a viable policy framework, evaluation will be grounded in the **Cybersecurity Capacity Maturity Model for Nations (CMM)** developed by the University of Oxford. Specifically, the programme targets Dimension 4: Cybersecurity Education, Training and Skills[46].

Beyond standard feedback, the success of the ambassadors will be measured through a specialized **"Regional Trust Coefficient"**, utilizing three data-driven metrics:

1. **The Informal Information Sharing Speed (IISS):** This metric tracks the time elapsed between a cyber-threat alert being shared by an ambassador in one Western Balkan country and its acknowledgement or action by peers in another. The target for Established maturity is a verified cross-border communication flow in under **60 minutes** for critical vulnerabilities[47].
2. **Peer-to-Peer Technical Validation:** Tracking the number of joint technical "situation reports" co-authored by ambassadors from at least two different WB nations. Success is defined as the production of **four regional briefings per year**, demonstrating a shift from national silos to regional synthesis.
3. **CMM Dimensional Shift:** The long-term goal is for the programme to contribute to a measurable advancement in the national CMM scores of participating WB countries, moving from Level 2 (Formative) to **Level 3 (Established)** within the sub-dimension of "Cybersecurity Awareness Raising" and "Education"[46].

By adopting these international benchmarks, the programme ensures it provides a measurable contribution to regional security rather than existing as a standalone youth workshop.

4.3 Potential Risks and Mitigation

Building a regional network in the Western Balkans is never without its friction points. To move this from a paper concept to a functional reality, the proposal identifies three primary operational hurdles and their respective workarounds, ensuring the program remains both resilient and effective.

The first major obstacle is the neutrality gap, often manifested through the politicisation of cyber-attribution. In a region where digital security can quickly become a tool for national agendas, any perception of bias would cause cross-border participation to stall. To navigate this, the initiative adopts a Technical First doctrine. By keeping the primary focus on common vulnerabilities and exposures (CVEs) and utilizing DCAF's neutral platform[48], the ambassadors are encouraged to speak the objective language of security rather than political rhetoric. This is further reinforced by conducting all high-level communication under Chatham House Rules, allowing for the honest and non-attributed sharing of incident data which is crucial for building regional trust.

Furthermore, the program must address the persistent risk of brain drain or the talent leak. There is a credible danger that highly trained ambassadors might be recruited by EU or US-

based firms, leaving the Western Balkans with a net loss of expertise. To mitigate this, the program focuses on creating a local prestige factor. Through a strategic partnership with the Regional Cooperation Council (RCC)[49], ambassadors will be granted Observer Status at prominent regional cybersecurity forums. This provides them with a direct seat at the table alongside key decision-makers, offering a level of professional influence and high-tier networking within the Balkans that an entry-level analyst position abroad simply cannot match.

Finally, the initiative seeks to overcome institutional inertia, commonly known as the pilot trap, where projects dissipate once initial grant funding is exhausted. The core of the sustainability strategy is integration over expansion. Instead of attempting to establish a new and costly independent agency, the Cyber Ambassadors program is designed to plug directly into the existing framework of the Western Balkans Cyber Capacity Centre (WB3C). By functioning as a Shadow Network ready-to-use and low-cost resource for established institutions—the program becomes a high-value asset that is easier for regional governments to support and maintain over the long term.

5.0 Regional Cooperation and Knowledge Sharing

Regional cooperation is at the heart of the **Cyber Ambassadors of the Western Balkans** initiative. Cyber threats are borderless, and attacks often affect multiple countries in the region simultaneously. Isolated national responses are not enough. Coordinated regional approaches allow youth to share knowledge, develop joint strategies, and respond to emerging threats collectively. The programme strengthens networks between Cyber Ambassadors, regional institutions, and international organisations to build a **resilient ecosystem of cybersecurity awareness and practice**[36].

Knowledge sharing is achieved through structured activities such as joint workshops, conferences, and simulation exercises. Ambassadors collaborate on case studies of regional cyber incidents, exchange solutions, and present lessons learned from national contexts. These activities are not only practical but also encourage **peer learning and cross-border mentorship**, enabling youth to act as multipliers of skills and information[37].

Integration with platforms like the **Western Balkans Cyber Camp** and the **Western Balkans Cyber Capacity Centre (WB3C)** allows participants to access updated threat intelligence, regional reports, and best practice frameworks. Coordinated efforts also link to EU and UN youth cybersecurity initiatives, aligning local knowledge with international standards[38]. By participating in these networks, ambassadors can compare national cybersecurity strategies, identify gaps, and propose youth-driven solutions that are adaptable across borders.

The ultimate aim is to create a **self-sustaining community of informed youth leaders** who not only respond to cyber incidents but also proactively shape policies and educational programs in their countries. This ensures that capacity-building efforts are reinforced at the local level while also contributing to regional resilience.

5.1 Monitoring and tracking

Monitoring regional cooperation focuses on **tracking participation, communication, and knowledge exchange**. Coordinators collect data on the number of joint workshops, cross-border projects, and collaborative exercises completed by ambassadors. They also evaluate engagement quality through feedback surveys, peer assessments, and reports of practical outputs[39].

Monitoring tools include online platforms where ambassadors share progress, document case studies, and upload joint project results. Participation in regional webinars and forums is also tracked to ensure ambassadors actively engage with peers from other countries. Coordinators assess how knowledge transfer occurs, how regional solutions are developed, and whether ambassadors apply shared practices in their local communities[40].

5.2 Long-term evaluation

Evaluation examines the **effectiveness of regional cooperation and the impact of knowledge sharing**. Key metrics include the number of successful joint projects, the adoption of best practices across multiple countries, and evidence of increased cybersecurity awareness among peers and communities. Evaluators also assess ambassadors' ability to present solutions to policymakers and contribute to regional discussions on cybersecurity[41].

Long-term evaluation considers the sustainability of the network. Are ambassadors continuing to collaborate beyond the programme? Are regional connections used to respond to real-world cyber threats? Are knowledge-sharing practices embedded in schools, universities, and youth organisations? Evaluators use these insights to refine the programme, strengthen cross-border ties, and ensure that youth-led initiatives have lasting impact[42].

By combining monitoring and evaluation, the programme creates a **continuous feedback loop**, ensuring that lessons learned from regional cooperation feed back into training, outreach, and policy engagement. This system guarantees that youth networks remain active, responsive, and capable of addressing evolving cyber threats across the Western Balkans.

6.0 Conclusion and Final Notes

The **Cyber Ambassadors of the Western Balkans** initiative represents a comprehensive approach to addressing the growing cybersecurity challenges in the region. By focusing on youth, the programme leverages a generation that is digitally literate, adaptable, and motivated to make a difference. It combines technical training, policy engagement, peer-to-peer education, and cross-border collaboration into a single, cohesive framework that builds skills while fostering regional resilience.

The programme demonstrates that **youth-driven initiatives are not just complementary to formal institutional measures** but are essential to strengthening overall cybersecurity. Through structured training, ambassadors develop the technical knowledge and governance

understanding necessary to identify threats, respond effectively, and contribute to policy discussions. Peer-to-peer outreach ensures that knowledge spreads beyond the selected ambassadors to schools, universities, and communities, creating a culture of cybersecurity awareness that is sustainable and scalable.

Regional cooperation and knowledge sharing are critical components of the initiative. By connecting youth across borders, the programme ensures that lessons learned, best practices, and innovative solutions are exchanged and applied throughout the Western Balkans. These networks enhance regional preparedness, harmonize responses to cross-border cyber threats, and align local actions with international standards.

Monitoring and evaluation embedded throughout the programme guarantee accountability and continuous improvement. Training effectiveness, outreach impact, regional engagement, and long-term sustainability are assessed systematically. Feedback loops allow the programme to evolve, addressing emerging threats and maximizing its impact.

Finally, the initiative has a dual purpose: it develops highly skilled cybersecurity practitioners and builds **regional youth leaders capable of shaping digital resilience**. The skills, networks, and experiences gained by ambassadors not only improve security in the short term but also create long-term human capital that will continue to benefit the Western Balkans. In conclusion, the Cyber Ambassadors programme is a practical, scalable, and youth-centered solution that strengthens cybersecurity, empowers the next generation, and fosters lasting regional collaboration.

7.0 List of sources

[1] RCC: All-inclusiveness is key for implementing cybersecurity measures across the Western Balkans, highlighting rising cyber incidents and the need for regional cooperation. RCC: All-inclusiveness in Western Balkans cybersecurity (09 Jul 2024)

[2] YEA: The Young European Ambassadors (YEA) platform is a creative network of young activists from across the Western Balkans promoting EU values, civic engagement and regional cooperation. Young European Ambassadors (YEA) – WeBalkans programme

[3] Western Balkans Cyber Camp: Open call for participation in the regional cybersecurity camp aimed at enhancing young people's practical knowledge and building a regional network of cyber specialists. Open call for Western Balkans Cyber Camp participation

[4] Western Balkans Cyber Camp: Students from Montenegro and other Western Balkan countries participated in the regional Cyber Camp to develop cybersecurity skills through practical exercises. Western Balkans Cyber Camp – Montenegro student participation (May 2025)

[5] WB3C: The Western Balkans Cyber Capacity Centre (WB3C) was inaugurated to serve as a central hub for advancing cybersecurity knowledge, collaboration and expertise in the region. Western Balkans Cyber Capacity Centre inaugurated – a day to remember

[6] EU Youth Strategy: The EU's youth strategy outlines frameworks for youth engagement, participation and empowerment across Europe, linking to broader goals of resilience, skills and integration. European Youth Strategy overview

[7] UN Security Council Resolution 2250 (2015): This UN resolution on youth, peace and security emphasizes the importance of structured youth engagement in decision-making processes, including areas related to security and governance. UN Security Council Resolution 2250 (2015) – Youth, Peace and Security

[8] Cyber Threat Report: over 9.2 million cyberattacks in BiH during one month of analysis https://bdf.ba/v2/wp-content/uploads/2023/05/Cyber-prijetnje-u-BiH-ENG-WEB.pdf

[9] Over 15.4 million cybersecurity threats in BiH by August 2023 https://www.media.ba/bs/magazin-novinarstvo/vise-od-15-miliona-prijetnji-cyber-sigurnosti-u-bih-do-augusta-2023

[10] BiH still lacks a national cybersecurity strategy and effective CERT mechanism https://bih.osce.org/hbs/node/601848

[11] Analyses show a lack of coordinated response and awareness of attacks in BiH institutions https://balkans.aljazeera.net/teme/2023/1/29/kako-bih-moze-povecati-otpornost-na-cyber-napade

[12] Data on low readiness and protection levels in private companies in BiH https://kfbih.com/edukacije-seminari-certificiranje/public-call-for-small-and-medium-sized-enterprises-for-participation-in-cybersecurity-training-and-technical-assistance

[13] BDF report on monthly cyber threats in BiH https://bdf.ba/v2/wp-content/uploads/2023/05/Cyber-prijetnje-u-BiH-ENG-WEB.pdf
[14] Media.ba article on over 15 million cyber threats in BiH https://www.media.ba/bs/magazin-novinarstvo/vise-od-15-miliona-prijetnji-cyber-sigurnosti-u-bih-do-augusta-2023
[15] OSCE report on lack of national cybersecurity strategy https://bih.osce.org/hbs/node/601848
[16] Al Jazeera Balkans article on weak institutional response https://balkans.aljazeera.net/teme/2023/1/29/kako-bih-moze-povecati-otpornost-na-cyber-napade
[17] Balkan Diskurs report on citizen exposure to identity theft and fraud https://balkandiskurs.com/en/2023/11/23/bosnia-and-herzegovina-at-a-crossroads-for-strengthening-cybersecurity/
[18] KFBiH data on SME cybersecurity readiness https://kfbih.com/edukacije-seminari-certificiranje/public-call-for-small-and-medium-sized-enterprises-for-participation-in-cybersecurity-training-and-technical-assistance
[19] OECD report on SME Policy Index Western Balkans and Turkey 2022 https://www.oecd.org/en/publications/sme-policy-index-western-balkans-and-turkey-2022_b47d15f0-en/full-report/component-23.html
[20] Balkan Insight report on BiH lacking capacity to fight millions of cyber attacks https://balkaninsight.com/2023/04/14/bosnia-lacks-capacity-to-fight-millions-of-cyber-attacks-monthly-report-warns/
[21] Western Balkans Cyber Camp supports practical skills and regional cooperation https://wb3c.org/event/50/spotlight-on-emerging-cybersecurity-technologies
[23] Western Balkans Cyber Capacity Centre inaugurated to advance knowledge and training https://www.gov.me/en/article/western-balkans-cyber-capacity-centre-inaugurated-a-day-to-remember
[25] Systematic review linking literacy skills to digital wellbeing and safer online behaviour https://link.springer.com/article/10.1186/s40359-025-03573-4
[26] Youth digital skills and participation initiatives in Western Balkans and EU https://scidevcenter.org/2024/02/19/youth-participation-in-digital-democracy-in-the-western-balkans-eydr/
[27] Recruitment and selection of youth for cybersecurity programs in Western Balkans https://www.rcc.int/pubs/102/youth-engagement-in-cybersecurity
[28] Training and mentorship in WB Cyber Camp and WB3C https://www.gov.me/en/article/open-call-for-application-western-balkan-cyber-camp
[29] Peer-to-peer outreach and digital hygiene education in schools https://balkaninsight.com/2023/12/06/bosnias-youth-lack-protection-from-online-risks-birn-report-warns/
[30] Regional collaboration and cross-border networking in Western Balkans youth programs https://www.coe.int/en/web/digital-education/western-balkans-youth-digital-skills
[31] Career and professional development for young cybersecurity leaders https://digital-skills-

jobs.europa.eu/en/cybersecurity-skills-academy

[32] Monitoring youth engagement in cybersecurity programs https://www.osce.org/files/f/documents/5/c/536062.pdf

[33] Peer evaluation and cross-border collaboration assessment https://wbcybersecuritynetwork.org/monitoring-and-evaluation

[34] Measuring impact and sustainability of youth cybersecurity initiatives https://www.undp.org/balkans/projects/youth-cyber-resilience

[35] Lessons learned and continuous improvement in cybersecurity capacity building https://www.eca.europa.eu/en/Pages/NewsItem.aspx?nid=15704

[36] Regional cooperation and youth networks in cybersecurity https://rcc.int/news/1121/regional-cyber-resilience-youth-initiative

[37] Peer learning and cross-border mentorship programs https://www.coe.int/en/web/digital-education/youth-cyber-skills

[38] Integration with EU and UN youth cybersecurity initiatives https://youth.europa.eu/strategy_en

[39] Monitoring cross-border youth projects and workshops https://wbcybersecuritynetwork.org/monitoring-and-evaluation

[40] Tools for tracking knowledge sharing among youth networks https://www.osce.org/files/f/documents/5/c/536062.pdf

[41] Evaluation of cross-border collaboration in cybersecurity https://www.undp.org/balkans/projects/youth-cyber-resilience

[42] Sustainability and long-term impact of youth networks https://www.coe.int/en/web/digital-education/sustainable-digital-youth

[43] Council of Europe: Youth Peace Ambassadors programme framework and regional trust-building initiatives. https://www.coe.int/en/web/youth-peace-dialogue/youth-peace-ambassadors

[44] United Nations Open-ended Working Group (OEWG) https://disarmament.unoda.org/oewg-ict-2021-2025/

[45] DCAF Young Faces programme framework and alumni outcomes in the Western Balkans. https://www.dcaf.ch/young-faces-network

[46] Global Cyber Security Capacity Centre (GCSCC), University of Oxford: *Cybersecurity Capacity Maturity Model for Nations (CMM)- Dimension 4: Education, Training and Skills*. https://gcscc.ox.ac.uk/cmm-2021-edition

[47] ITU *Global Cybersecurity Index (GCI)* https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[48] DCAF *Principles of Good Governance in the Cybersecurity Sector.* https://www.dcaf.ch/cybersecurity-governance

[49] Regional Cooperation Council (RCC) *Western Balkans Digital Agenda and Graduate Survey on ICT Skills Retention.* https://www.rcc.int/priority_areas/39/digital-agenda-for-the-western-balkans