From Knowledge to Cybersecurity: Serbia's Efforts to Build Cyber Resilience through Skilled Workforce

Author: Marko Stanković

DCAF's Young Faces in Cybersecurity
Governance Programme 2024/2025 Participant

Abstract

This policy paper explores Serbia's current cybersecurity landscape, briefly outlining the country's legal and regulatory framework, strategies for enhancing cybersecurity awareness, and initiatives to tackle the lack of cybersecurity skills. The paper summarises definitions of various stakeholders while underlining the importance of a broad, inclusive approach. It studies Serbia’s legal and regulatory basis, mentioning the Law on Information Security and the role of national bodies and civil society organisations in addressing cybersecurity risks. The paper also reviews Serbian Strategy for Information Society (2021-2026) and its main goals. One of the components includes the national Cyber Hero Programme as a good initiative of engaging youth and supporting talent. In the end, the recommendations are tailored to strengthen national cybersecurity infrastructure, including collaboration between the public and private sectors, increased educational initiatives and programmes, and the development of a more skilled cybersecurity workforce. Ultimately, the paper calls for continued investment in human resources, regional cooperation, and the creation of a sustainable cybersecurity framework to safeguard Serbia’s growing digital landscape.

Keywords: cybersecurity, cybersecurity workforce, cybersecurity education, cyber resilience.

Is there a standard definition for cybersecurity?

DCAF (2021), in Guide to the Good Governance in Cybersecurity stated that *'the meaning of the term cyberspace is unclear because the concept seems, by its nature, abstract and detached from the physical world'*. Society has gone through a digital makeover where new technologies now have a significant place in many academic disciplines. New technologies are important to government operations in advanced industrial countries, although with a delay in comparison to business and many civil society adjustments (Margetts and Dunleavy, 2013). Defining cybersecurity with its constantly changing nature is difficult. Since it is a largely used term, and it varies depending on the context, a more broad and inclusive definition is needed. The European Union Agency for Cybersecurity (ENISA) has accepted a very broad definition of cybersecurity as *'security of cyberspace'*. Security risks in the cyber world are highly diverse, ranging from cybercrimes targeting humans and legal entities through or with the aid of computer systems and networks to cyber operations that threaten the security of states and international organisations, including acts of terrorism or even aggression (Milošević, 2017). Cybersecurity can also be viewed from a human-centric approach. It is a part of the broader theory of good security sector governance (SSG). SSG prioritises not only the state's networks, systems, and stability but also the rights of individuals in a democratic society and their human rights (DCAF, 2023).

Legal and regulatory foundation in Serbia

In 2005, Serbia adopted the Law on the Organisation and Competence of State Bodies in Combating High-Tech Crime. Although not discussing in-depth cybersecurity struggles and providing solutions, there was a mention of computer systems and introducing the Cybercrime Department. Under this law, which governs procedures for cybercrimes, the Special Prosecution Office for Cybercrime in Belgrade is set to be responsible for handling such cases. This Office assumes responsibility for cybercrime cases during the preliminary proceedings upon receiving reports from the specialist Department for combating high-tech crime within the Ministry of Interior. However, its main challenge is a shortage of human resources.

Another important document is the Law on Information Security, adopted in early 2016. The Law requires operators of ICT systems of special importance, some of which will be classified as critical information infrastructure. It paved the way for more skilled individuals to be involved in these tasks. Additionally, the Law provides the space for the establishment of

the Body for the Coordination of Information Security, with the possibility of forming expert working subgroups that may include representatives from other public bodies, industry, academia, and civil society (DiploFoundation, 2016). In 2024, the need for amendments to the Law was introduced, aligning it with the new EU NIS 2 directive. The working group consisted of 57 members from 20 institutions and was led by the Ministry of Information and Telecommunications, with contributions from security agencies, regulatory bodies, and industry organisations (NALED, 2023). The updated Law now covers new sectors, including providers of services in the pharmaceutical industry, healthcare products, and postal services, which emphasise cybersecurity relevance in diverse industries (SecuritySee, 2024). One of the most important changes in the Law is the establishment of the Information Security Office. The Office will be tasked with efficiently responding in the event of a cyberattack, coordinating responses, and assisting in damage recovery (SecuritySee, 2024). Novelties include alignment with EU Cyber Security Act, Act on Risk Assessment and Creation of an Information Security Office.

Additionally, one of the mechanisms is the Serbian Telecommunication Agency (RATEL). RATEL is an independent state agency that houses the National Centre for the Prevention of Security Risks in ICT Systems of the Republic of Serbia (nCERT). Under the Law on Information Security, nCERT is tasked with gathering and sharing information on risks to ICT systems, as well as providing information, support, warnings, and advice to those responsible for managing ICT systems, along with the public. In addition to nCERT, other institutions, including the Ministry of the Interior (MoI), the Security Intelligence Agency (BIA), and the Serbian Army, each have their own CERTs. Also, academia (AMRES) and banks (FIN-CERT) have their own CERTs as well (Milovanović, 2024). Like other countries in the region, legal mechanisms exist to protect critical infrastructure and combat cybercrime; however, challenges in implementation remain (DiploFoundation, 2016).

In 2021, Serbia adopted the Strategy for the Information Society for the period 2021-2026 (Republic of Serbia, 2021). The adoption and implementation of this strategic document is important to continue advancing the digital knowledge and skills of all citizens. It serves as a tool to improve the capacity of employees in both the public and private sectors to use new technologies and improving digital infrastructure in educational institutions. On top of this, it is very important to improve information security, primarily through the development of the

capacity of competent institutions, raising citizen awareness, encouraging public-private partnerships, and increasing regional and international cooperation.

The strategy identifies several state administration bodies, including the Ministry of Information and Telecommunications, the Regulatory Agency for Electronic Communication and Postal Services (RATEL), and its Computer Emergency Response Team (CERT), along with the Serbian government's Coordination Body for Information Security Affairs. Further into the Strategy (Republic of Serbia, 2021), the main goal is to develop an advanced information society and e-government that serves both citizens and businesses. This goal is pursued through three specific objectives:

1. Improving digital knowledge and skills among citizens, strengthening the capacities of employees in both the public and private sectors for the use of new technologies and advancing digital infrastructure in educational institutions.
2. Digitalisation of services and business processes in both public and private sectors.
3. Enhancing cybersecurity for citizens, public administration, and businesses.

One of the practical examples of improving digital knowledge and skills involves organising numerous training sessions in this field. A recent example is the cybersecurity training held in January 2025, organised by National CERT in collaboration with DCAF. This training focused on cybersecurity in ICT systems of critical importance in the healthcare sector (National CERT, 2025). Another example is the *'Smart and Safe'* platform that promotes digital literacy, digital competencies, and a culture of digital security among all citizens of Serbia. Special attention is given to initiatives targeting young people, women, and individuals with disabilities. More details on this and similar initiatives will be discussed in the recommendations section (Government of Serbia).

The involvement of academia and the private sector is acknowledged as valuable for developing solutions and systems to enhance national information security (DCAF, 2021). While Serbia has made progress in cybersecurity education, particularly in technical fields, there is still a lack of comprehensive multidisciplinary education at the policy level. Most cybersecurity programmes focus on technical skills, with fewer opportunities for interdisciplinary education that integrates law, policy, economics, and international relations. Although the *'Smart and Safe'* campaign, led by the Ministry of Trade, Tourism, and

Telecommunications, seeks to raise general awareness of online safety, particularly among young people, its reach remains limited (DiploFoundation, 2016).

Empowering the next generation: Serbia's Cyber Hero Programme and youth engagement in cybersecurity

The Cybersecurity Network Foundation (CSN)**,** formerly informally known as the 'Petnica Group', developed alongside the process of establishing a regulatory and institutional framework for cybersecurity in Serbia. Important supporters in the field of cybersecurity include the international community, particularly the Geneva Centre for Security Sector Governance (DCAF), OSCE Mission to Serbia and Diplo Foundation, as well as civil society. These institutions promote cooperation between government bodies, citizen associations, academia, youth and businesses, showing how a multidisciplinary approach is needed (Milovanović, 2024). DCAF work on the Young Faces Programme is supporting young people and contributes to preparing tomorrow's leaders of cybersecurity (DCAF, 2022).

The CSN network is acknowledged in the Information Society and ICT Security Development Strategy, with its representatives managing the working group of the Coordination Body for ICT Security Affairs, establishing institutional ties with the state (Milovanović, 2024). Moving forward, the network is focusing on training and empowering young talents in Serbia through their Cyber Hero programme, supported by relevant state bodies, higher education institutions, associations, and businesses. (Milovanović, 2024). Since 2022, the OSCE Mission to Serbia has partnered with the CSN Foundation to organise the national cybersecurity competition for youth, the main event of the Cyber Hero Programme. The winners of the competition then join the national team and compete in the European Cybersecurity Challenge, supported by the EU Agency for Cybersecurity (ENISA) (OSCE, 2022, 2023 and 2024).

Another important aspect is its focus on gender. To endorse inclusivity, an all-female delegation represented Serbia at the Western Balkans Cyber Camp in Albania, in May 2024. Three of the girls were part of the winning team. Another member of the Serbian team, Milica Spasojević, highlighted how she and her *peers 'met people with similar interests from across the region; in the future, this will mean a lot for us, I think it gave us direction',* she said. As noted by the OSCE (2024), *'recognizing the important role the youth play in cybersecurity, the Mission to Serbia highlights the work of the well-known Serbian private-public partnership*

*with the CSN Foundation and its Cyber-Hero Programme to popularize the topic of cybersecurity among university and high school students in Serbia' (*OSCE, 2024). Nebojša Jokić, Executive Director of the CSN Foundation, said that the Cyber Hero Programme *'introduces young people to the field and helps them connect with one another'* (OSCE, 2024).As a good initiative, Women for Cyber (W4C) Serbia aims to support women who are already in the field of cybersecurity, but also to attract the ones who are not. As more girls join the field, gender representation in cybersecurity is gradually improving. However, they remain underrepresented.

Cybersecurity skills shortage

As observed by Maravić (2021) *'the cybersecurity workforce shortage and skills gap are also significant concerns for the economic development and national security, especially given the rapid digitization of global and regional economies'. Country report for 2023 of the European Commission also notes that 'in the field of cybersecurity, Serbia possesses the relevant legal framework and has a functioning national computer emergency response team (nCERT); however, capacities should*
be strengthened and upgraded. Work is under way to further align Serbia's legislation with the EU acquis on cybersecurity, including with the NIS2 Directive'. Another study (2019) by the Information Systems Security Association (ISSA) and Enterprise Strategy Group found *'that 74% of organisations are impacted by the cybersecurity skills shortage'*. This shortage has led to increased security incidents and emphasises the need for continuous professional development and competitive compensation to retain cybersecurity professionals. On a global level, the Cybersecurity Jobs Report (2025) indicates that *'global cybersecurity job vacancies have remained at 3.5 million since 2021, underscoring the persistent demand for cybersecurity professionals'*. Moreover, the WEF Global Cybersecurity Outlook (2025) highlights that *'since 2024, the cyber skills gap has increased by 8%, with two out of three organizations reporting moderate-to-critical skills gaps. Notably, only 14% of organizations are confident they possess the necessary talent and skills to meet their security requirement.'*

Recommendations

Based on the analysis throughout this policy paper, several recommendations have been identified to strengthen. The OECD's Western Balkans Competitiveness Outlook 2024 highlights that Serbia's cybersecurity system is constrained by insufficient human and financial resources. These recommendations focus on strengthening the operational capacities of national institutions, fostering public-private partnerships, advancing educational advancements, and encouraging regional cooperation.

Strengthening national cybersecurity framework and capacity

1. **Engagement of the private sector in cybersecurity**
   Due to the limited capacity of the public sector to develop a comprehensive national cybersecurity framework, there is a need to engage the capacities of the private sector (e.g. telecommunications operators and internet service providers), which possess the technical capabilities to support incident resolution and analysis (Rizmal, 2018). Governments should adopt a pragmatic approach to building PPPs that promote open communication, inclusive participation, and increased private sector participation (DCAF, 2021).
2. **Increasing institutional capacities for effective cybercrime response**
   The infrastructure capacities, the number of employees, and the technical equipment of the institutions (e.g. the above-mentioned Special Prosecutor's Office for High-Tech Crime) should be increased to allow it to perform its tasks effectively (Milovanović, 2024).
3. **Inclusive cybersecurity strategy development**
   Organisations representing marginalised groups in Serbia must be involved in the development of new cybersecurity strategies and laws to ensure that documents reflect their needs (Milovanović, 2024).
4. **Investment in research and innovation**
   Governments should invest more resources in research and innovation to develop new tools to deter, protect against, detect, and respond to new types of cyber threats (DCAF, 2021).

Educational initiatives and talent development

To address the skills gap in cybersecurity, Serbia should invest in comprehensive educational advancements, and there are several recommendations related to how to potentially achieve it:

1. **Continue to integrate cybersecurity into school curricula**
   Keep integrating cybersecurity modules into school curricula is already ongoing. From primary schools to universities, students should be exposed to cybersecurity concepts early on. Also, there is a need to equip the teachers with the necessary resources and training to effectively and quality teach cybersecurity through interactive and well-rounded workshops.
2. **Co-produced curriculum for active student engagement**
   When discussing methods to engage students, there is a need for a co-produced curriculum that actively involves students in the learning process. This could be achieved by providing structured opportunities for learning through connections to real-world situations (e.g. 9/12 competition supported by the CSN Foundation).
3. **Industry Collaboration and Career Development**
   This could be achieved to fairs that can be organised once or twice per year on a wider range with the cooperation of schools and institutions. Actively promote career opportunities in cybersecurity to raise awareness and interest among students.
4. **Apprenticeship and graduate programmes to attract talent**
   The development of apprenticeship and graduate programmes, alongside a comprehensive outreach initiative targeting underrepresented groups, will help attract cybersecurity talent into entry-level roles. In the context of Serbia, the focus must be on how to increase the participation of women and other marginalised groups in these programmes, addressing existing gender disparities and sustaining diversity (e.g. women4cyber).

Awareness-raising

- **Promoting Cybersecurity as a Shared Responsibility**

Serbia should turn towards nurturing a cybersecurity culture. Good examples are *'Let's Be Cyber Aware'* campaign launched in October 2022 by the National CERT in Serbia. The campaign provided updates on current cyber threats to citizens, companies, and state institutions (RATEL, 2022). Good examples are mentioned above - CyberHero Programme and Smart and Safe platform. SHARE Foundation conducts training sessions, offers support, and raises awareness of digital security for journalists, activists, civil society, and human rights defenders, observed from a human-centric approach (Perkov, 2024).

Regional efforts

- **Active involvement in regional cybersecurity initiatives**

Serbia should be actively involved in regional initiatives such as the Western Balkans Cyber Capacity Center (WB3C) with the aim of improving the cyber capacities in the region of the Western Balkans. The WB3C will develop a contribution to policymaking. It could help bring together specialised services, which would facilitate information sharing at the regional level (Embassy of France in Montenegro, 2024). Another good initiative is the 'Western Balkans Cyber Camp', held annually in Albania.

Conclusion

The need for a comprehensive and integrated approach to cybersecurity in Serbia is a good path to follow. As the country navigates its digital "makeover", both in the public and private sectors, strengthening its cybersecurity resilience will be indispensable for maintaining national security, protecting economic assets, and safeguarding citizen trust. As Serbia is influenced by the standards provided by the international community, enriching educational programmes, improving talent development, and engaging in regional efforts can benefit from becoming closely aligned with the best practices.

These recommendations are not easy to fulfill, that is for sure. It will involve the coordinated and unified efforts of all involved parties. As the focus is on the development of a skilled cybersecurity workforce, it should minimise the skill shortage that is present in the field of cybersecurity. When we observe the efforts in cybersecurity training, youth engagement

programmes, and diverse collaborations, we can notice some positive trends in safeguarding the cybersecurity ecosystem. The paper also calls for the integration of cybersecurity education into the academic sphere. That can open doors of wider interest in the topic and potentially create more skilled talents dealing with cybersecurity.

Looking from this perspective, innovation and brand-new research in terms of making those recommendations come to life seem inevitable. Finally, these holistic ideas can potentially position Serbia as a regional frontrunner. While on a good path, Serbia's cybersecurity resilience would need extra working hours to be on égal footing with the fast-advancing cyber dynamics.

References

AkoKvo (2023) Accredited Master's Interdisciplinary Study Programme in English - Cyber Security. Available at: https://akokvo.me/en/accredited-masters-interdisciplinary-study-programme-in-english-cyber-security/

DCAF – Geneva Centre for Security Sector Governance (2021) National cybersecurity strategies in the Western Balkans: a regional perspective. Geneva: Geneva Centre for Security Sector Governance (DCAF). Available at: https://www.dcaf.ch/sites/default/files/publications/documents/NationalCybersecurityStrategiesWB_2021.pdf

DCAF – Geneva Centre for Security Sector Governance (2022). Preparing Tomorrow's Leaders in Cybersecurity. Available at: https://www.dcaf.ch/preparing-tomorrows-leaders-cybersecurity

DCAF – Geneva Centre for Security Sector Governance (2023) Cybersecurity and Human Rights in the Western Balkans. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CybersecurityHumanRightsWesternBalkans_EN_March2023.pdf

DCAF – Geneva Centre for Security Sector Governance (2023) Online actions, offline harms: Preventing and countering gender-based cyberviolence. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/Online-actions-offline-harms_EN-2nov2023.pdf

DCAF – Geneva Centre for Security Sector Governance (2021) Guide to good governance in cybersecurity. Geneva: Geneva Centre for Security Sector Governance (DCAF). Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_EN_Jan2022.pdf

DiploFoundation (2016) Cybersecurity in the Western Balkans. Policy gaps and cooperation opportunities. Available at: https://www.diplomacy.edu/wp-content/uploads/2014/03/Cybersecurity-in-Western-Balkans.pdf

European Commission. (2023). *Serbia 2023 Report*. (Retrieved from https://enlargement.ec.europa.eu/document/download/9198cd1a-c8c9-4973-90ac-b6ba6bd72b53_en.

Embassy of France in Montenegro. (2024) Western Balkans Cyber Capacity Center (WB3C). Available at: https://me.ambafrance.org/Western-Balkans-Cyber-Capacity-Center-WB3C

Government of Serbia (n.d.) Pametno i bezbedno – Zvanična internet prezentacija. Available at: https://pametnoibezbedno.gov.rs/

Maravić, D. (2021) Cybersecurity policy development and capacity building – Increasing regional cooperation in the Western Balkans. Geneva: Geneva Centre for Security Sector Governance (DCAF). Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CybersecurityPolicyDevelopment_CapacityBuilding_in_WB_mar2021.pdf?utm_source=chatgpt.com

Margetts, H. and Dunleavy, P., 2013. The second wave of digital-era governance: a quasi-paradigm for government on the Web. Philosophical transactions of the royal society A: mathematical, physical and engineering sciences, 371(1987), p.20120382.

Milovanović, D. (2024) Cybersecurity context in Serbia: Legislative and strategic framework. Barcelona Economics Network. Available at: https://racef.es/archivos/publicaciones/web_racef_semprimavera_ms85_24.pdf

Milosevic, M.M. and Putnik, N.R., 2017. Cyber Security and the Protection from Cyber Crime in Serbia-Strategic and Legal Framework. Kultura polisa, 14, p.177.

NALED (2023) Šta nam donose izmene Zakona o informacionoj bezbednosti. Available at: https://naled.rs/vest-sta-nam-donose-izmene-zakona-o-informacionoj-bezbednosti-8194

National CERT (2025) Održana obuka za predstavnike zdravstvenog sektora. Available at: https://www.cert.rs/rs/vest/1340-Održana-obuka-za-predstavnike-zdravstvenog-sektora.html

N1 Beograd, 2021. Vlada Srbije usvojila Strategiju razvoja informacionog društva i bezbednosti. N1. Available at: https://n1info.rs/magazin/scitech/vlada-srbije-usvojila-strategiju-razvoja-informacionog-drustva-i-bezbednosti/

OSCE, 2024. Engaging youth to forge a robust future for cybersecurity in Serbia. [online] Available at: https://www.osce.org/mission-to-serbia/570774

Perkov, B. (2024) 'Digital security in Serbia: another challenge to media freedom', Osservatorio Balcani e Caucaso Transeuropa, [online] Available at: https://www.balcanicaucaso.org/eng/Areas/Serbia/Digital-security-in-Serbia-another-challenge-to-media-freedom-232447

Pencheva, D., Hallett, J. and Rashid, A., 2020. Bringing cyber to school: Integrating cybersecurity into secondary school education. IEEE Security & Privacy, 18(2), pp.68-74.

Regulatory Agency for Electronic Communications and Postal Services (RATEL) (2022) 'National Cyber Conference "Let's Be Cyber Aware" takes place in Belgrade', National CERT of the Republic of Serbia, 31 October. Available at: https://www.cert.rs/en/vest/945-Održana-Nacionalna-sajber-konferencija-"Budimo-sajber-svesni".html

Rizmal, I. (2018). Vodič kroz informacionu bezbednost u Republici Srbiji 2.0. Beograd: Misija OEBS-a u Srbiji, Unicom Telecom, IBM, Juniper. Available at: https://www.osce.org/files/f/documents/3/8/404258.pdf

SecuritySee (2024) Šta donosi Zakon o informacionoj bezbednosti u Srbiji?. Available at: https://www.securitysee.com/2024/11/12/sta-donosi-zakon-o-informacionoj-bezbednosti-u-srbiji/