Kosovo's Cybersecurity Strategy:

Objectives 2 & 4 on the Path to EU Integration

Author: Sara Dumani

Reviewer: DCAF Young Faces 2025-2026

March 2026

Executive Summary

The Republic of Kosovo has been a target of malicious cyber-attacks that threaten critical infrastructure, businesses, and public services. In response, Kosovo adopted the National Cybersecurity Strategy 2023-2027, which introduces legal, technical, and institutional measures aimed at strengthening national cyber resilience. While cybersecurity governance remains a developing field in Kosovo, it presents opportunities to strengthen institutional governance, enhance national security governance, and support Kosovo's path toward European Union (EU) integration.

This policy brief examines the implementation of Objective 2: Promote cybersecurity awareness and a cybersecurity culture, and Objective 4: Build sustainable and mutually beneficial national and international cooperation within Kosovo's cybersecurity strategy. These objectives are particularly relevant in the context of Kosovo's efforts to align with EU cybersecurity frameworks such as the NIS Directive, the NIS2 Directive, and emerging regulatory initiatives like the Cyber Resilience Act. The analysis evaluates Kosovo's institutional readiness, human capacity development, and engagement with international cybersecurity networks.

The findings suggest that Kosovo has taken important steps toward strengthening its cybersecurity architecture, including establishing dedicated institutions and participating in regional cybersecurity initiatives. However, significant gaps remain in terms of human capital development, operational coordination, and structured public-private cooperation. These limitations constrain Kosovo's ability to respond effectively to cyber threats and may slow its progress toward its EU integration.

Drawing on research, international frameworks, and best practices, this policy brief provides policy recommendations to strengthen Kosovo's national cybersecurity capacity, develop public-private partnerships, and formalize regional and EU engagement. Implementing these measures will support Kosovo's strategic goals of cyber resilience, credible international cooperation, and convergence with EU norms.

1. Introduction: Kosovo's Cybersecurity Strategy

Cybersecurity has become a core component of national security and digital governance in Kosovo, particularly as the country experiences fast development of information and communication technologies (ICT) and internet-based services. In response to the growing frequency, scale, and sophistication of cyber threats, the Government of Kosovo adopted the National Cybersecurity Strategy for 2023-2027, aimed at strengthening cyber readiness and resilience across both the public and private sectors[1]. The strategy sets out an agenda of approaches and strategic objectives designed to improve the security and resilience of national infrastructures and services, increase public awareness, and align Kosovo's cybersecurity practices with international standards[2].

The protection of critical information infrastructure is important for the Government of the Republic of Kosovo, as cyberattacks can destabilize the economy and harm the reputation of businesses and individuals[3]. Strengthening Kosovo's cybersecurity ecosystem is essential for systemic governance and national stability, which is the goal of the National Cybersecurity Strategy 2023-2027. Through this strategy, the Government of Kosovo aims to create a vision for a secure cyberspace for citizens, businesses, and public institutions, outlined through six strategic objectives for the period of 2023-2027[4]. These objectives are:

- **Strategic Objective 1:** Create legal and institutional cyber security capacities at the national level.
- **Strategic Objective 2:** Promote cyber security awareness and a cyber-security culture in Kosovo.
- **Strategic Objective 3:** Support the development of the private sector in cyber security, Public-Private Partnership (PPP) and cross-sectoral information sharing.
- **Strategic Objective 4:** Build sustainable and beneficial national and international cooperation in cyber security.
- **Strategic Objective 5:** Develop lasting cyber security capacities for the government and the private sector.
- **Strategic Objective 6:** Advance the investigative and military cyber security capabilities

This strategy complements existing legislative reforms, including the Law on Cybersecurity (08/L-173) adopted by the Kosovo Assembly in 2023, which provides a legislative foundation for cybersecurity governance structures and contributes to the harmonization of Kosovo's legal framework with European standards[5]. Beyond domestic governance, Kosovo's cybersecurity strategy has a growing role in international credibility and regional engagement. Cybersecurity policy is viewed as part of the fabric of modern statecraft, intersecting with diplomatic engagement, international cooperation, and compliance with standards recognized by global and European institutions. Kosovo's inclusion of international cooperation and alignment in its

[1] Government of Kosovo. (2023). National cybersecurity strategy 2023–2027. Ministry of Internal Affairs.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Government of Kosovo. Law on Cybersecurity (08/L-173). Official Gazette of the Republic of Kosovo. https://gzk.rks-gov.net/ActDetail.aspx?ActID=70933

strategic objectives positions cybersecurity as a key element of its efforts toward EU integration and convergence with EU policy frameworks[6].

For Kosovo, aligning national cybersecurity practice with EU expectations carries multiple benefits. Improved cyber governance can support regulatory alignment with EU instruments such as the NIS Directive and the NIS2 Directive, which require member states and partners to strengthen incident response teams, cybersecurity workforce capacity, and structured public-private cooperation mechanisms. Aligning with these standards also supports participation in regional cybersecurity networks and builds confidence with EU counterparts in areas of digital trust, information sharing, and coordinated incident response[7].

This policy brief evaluates Kosovo's current cybersecurity capacity and institutional readiness by focusing on Objective 2 (capacity building) and Objective 4 (international cooperation). By analyzing these objectives, it identifies key implementation gaps and proposes policy recommendations that could strengthen Kosovo's cybersecurity ecosystem and support its broader EU integration goals. The analysis uses a qualitative assessment of Kosovo's National Cybersecurity Strategy (2023-2027) and compares its objectives with relevant EU cybersecurity frameworks and benchmarks.

[6] Western Balkans Info Hub. (2025). Kosovo in the Digital Agenda of the Western Balkans. https://westernbalkans-infohub.eu/wp-content/uploads/2025/07/Kosovo-in-the-Digital-Agenda-of-the-Western-Balkans_ENG_final_revised.pdf

[7] OECD (2024), Western Balkans Competitiveness Outlook 2024: Kosovo, Competitiveness and Private Sector Development, OECD Publishing, Paris, https://doi.org/10.1787/ff74ae0e-en.

2. Objective 2: Capacity Building and Cyber Resilience

2.1. Objective 2: Promote cyber security awareness and a cyber-security culture in Kosovo

Within Kosovo's National Cybersecurity Strategy 2023-2027, Objective 2 focuses on strengthening national capacity and resilience against cyber threats through a combination of institutional, human, and systemic measures. This objective aims to develop an effective and inclusive public-private partnership (PPP) framework, grounded in mutual trust and shared responsibility for the security of Kosovo's national cyberspace[8].

Objective 2 prioritizes the creation and strengthening of cybersecurity competencies within public institutions, supported by measures to recruit, train, and retain skilled professionals. In parallel, capacity building under Objective 2 includes the development of a research and development system for projects that aim at identifying and addressing threats such as cyberstalking, online hate speech, and disinformation. The strategy also focuses on education and skills development, including the introduction of cybersecurity courses that incorporate ethical hacking components. Some of these initiatives are designed to engage high school students, with particular attention given to increasing the participation of girls[9].

However, despite these initiatives, the development of cybersecurity capacity remains uneven. A comparison with common EU practices illustrates the current gap between Kosovo's strategic ambitions and operational capacity.

Indicator	EU Benchmark	Kosovo Situation
National CSIRT Capacity	NIS2 requires well-resourced CSIRTs with operational response capability	KOS-CERT established but limited personnel and resources
Cybersecurity Workforce	EU encourages continuous training and professional development across institutions	Shortage of trained professionals (cybersecurity specialists) in public institutions
Cyber Education	Cybersecurity integrated into formal education programs at multiple levels	Limited integration beyond basic IT courses

[8] Government of Kosovo. (2023). National cybersecurity strategy 2023–2027. Ministry of Internal Affairs.
[9] Ibid.

Kosovo's cybersecurity capacity remains in a developing phase when measured against international benchmarks. According to the National Cyber Security Index (NCSI), Kosovo ranks 89th globally with a score of 40 points, reflecting moderate institutional preparedness and gaps in areas such as cybersecurity education, research capacity, and international cooperation. National incident response capabilities are coordinated through KOS-CERT, the country's designated Computer Security Incident Response Team responsible for monitoring and responding to cyber threats.[10]. Despite these institutional developments, Kosovo continues to face shortages of trained cybersecurity professionals and limited technical capacity within public institutions, challenges that are also identified in EU-supported cybersecurity capacity-building initiatives in the Western Balkans.

2.2. International Alignment and Cyber Diplomacy

Capacity building under Objective 2 is not only a domestic governance necessity but also an essential component of cyber diplomacy and international credibility. In international cybersecurity norms and discussions, particularly those framed by the United Nations Group of Governmental Experts (UN GGE)[11] and the Open-Ended Working Group (OEWG)[12], link capacity building to trust, responsible state behavior, and the ability to implement agreed norms. These processes emphasize that adequate national capacity helps states to engage credibly in international cybersecurity cooperation. Kosovo's efforts to strengthen institutional and human capacity, therefore, align with foundational principles established by the 2010 UN GGE report, which calls for responsible state behavior, transparency, and confidence-building measures in cyberspace[13].

In European and regional contexts, capacity building also supports alignment with EU cybersecurity standards, such as those embedded in frameworks like the NIS Directive[14] and NIS2 Directive[15], which set baseline expectations for member states and partners regarding institutional readiness, risk management practices, and incident response capabilities. Kosovo's efforts to meet these standards signal its commitment to European security norms, supporting cooperation and trust with EU institutions and member states.

---

[10] e-Governance Academy (2025). Kosovo. National Cyber Security Index (NCSI)

[11] United Nations Office for Disarmament Affairs. (2022). The UN norms of responsible state behaviour in cyberspace. https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

[12] European External Action Service. (2021). EU key messages – United Nations Open-Ended Working Group on ICTs (formal session).

[13] United Nations. (2010). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN Doc. A/65/201).

[14] European Parliament & Council of the European Union. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

[15] European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).

The Organization for Security and Co-operation in Europe (OSCE) complements these frameworks by promoting regional cooperation, information sharing, and joint responses to cyber threats, providing practical models for strengthening national capacity[16].

Collectively, these norms and practices demonstrate that capacity building is both a technical and diplomatic tool that supports national resilience. States with stronger institutional and human capacities are better positioned to participate in international cybersecurity cooperation, implement agreed norms, and respond effectively to cross-border cyber incidents. Kosovo's focus on capacity building within its national strategy reflects a domestic governance priority and a commitment to integrate into these broader international practices and expectations.

[16] Organization for Security and Co-operation in Europe. Cyber/ICT security.

3. Objective 4: Regional and International Cooperation

3.1. Objective 4: Build sustainable and beneficial national and international cooperation in cyber security

Objective 4 of Kosovo's National Cybersecurity Strategy 2023-2027 is structured around two main dimensions: strategic and political cooperation, and technical and operational cooperation[17]. In terms of strategic and political cooperation, Objective 4 seeks to strengthen Kosovo's role in regional and international cybersecurity by increasing participation in forums and organizations, fostering cooperation across legislative, judicial, and law enforcement sectors to address cybercrime and cyber espionage, improving diplomatic communication to build trust and credibility as an international partner, collaborating with NATO on cyber defense and threat information sharing, and aligning national legislation with EU standards while supporting international cybersecurity policy and cooperation[18].

At the technical and operational level, Objective 4 aims to expand Kosovo's participation in international technical dialogues and build a network of partnerships to enhance knowledge exchange and operational capacity. This includes cooperation with the Internet Corporation for Assigned Names and Numbers (ICANN), exploring membership in EU DNS initiatives, adopting and implementing EU IPv6 regulations, strengthening collaboration with the European Union Agency for Cybersecurity (ENISA), establishing cooperation with the International Telecommunication Union (ITU), and increasing bilateral and multilateral engagement with national CERTs of other countries[19].

Through these efforts, Kosovo aims to position cybersecurity as an important component of its broader cyber diplomacy strategy, demonstrating responsible state behavior and building international trust.

3.2. Regional and EU Engagement

In the regional context, Kosovo's cybersecurity efforts aim to strengthen collaboration with Western Balkans partners to develop collective resilience against cross-border cyber threats. These measures enable Kosovo to engage in multilateral cybersecurity dialogue, contribute to joint risk management initiatives, and build trust with neighboring states.

Examples of regional cooperation include collaboration with the National Cybersecurity Authority of Albania (AKSK), where partnerships aimed at enhancing regional cyber resilience were explored[20], participation in the WB6-EU Cooperation project for improving cybersecurity in the Western Balkans[21], and engagement in the Western Balkans Cyber Capacity Centre (WB3C)

[17] Government of Kosovo. (2023). National cybersecurity strategy 2023–2027. Ministry of Internal Affairs.
[18] Ibid.
[19] Ibid.
[20] Autoriteti Kombëtar i Sigurisë Kibernetike (AKSK). (2025). AKSK welcomes the delegation from Kosovo's cybersecurity institutions.
[21] CYBIL Portal. (2024). WB6 EU cooperation for improving cybersecurity in the Western Balkans

regional conference[22]. While these engagements mark important first steps, further progress is needed to formalize partnerships, expand joint capacity-building initiatives, and ensure sustained operational cooperation across the region.

Within the European framework, Kosovo aligns its cybersecurity practices with EU norms and standards, including the NIS2 Directive, which requires stronger risk-management practices, incident reporting obligations, and cooperation among national Computer Security Incident Response Teams (CSIRTs). These requirements are directly linked to Objective 4, which aims to expand Kosovo's participation in international cyber cooperation and information-sharing networks. Engagement with EU frameworks allows Kosovo to benchmark its cybersecurity capacity, adopt best practices in governance and incident response, and contribute to regional information-sharing initiatives. These efforts position Kosovo to collaborate more closely with EU member states and institutions. However, further work is required to deepen Kosovo's integration into EU cyber networks and increase its visibility in regional and EU cybersecurity policymaking, to fulfill the technical and operational level of the Objective 4.

[22] Ministry for Europe and Foreign Affairs. (2024). Cybersecurity: Joint communique of the Ministry for Europe and Foreign Affairs. French Government.

4. Kosovo's Cybersecurity Challenges: Objective 2 & 4

4.1. Challenges in Implementing Capacity-Building Measures (Objective 2)

Despite the strategic emphasis placed on capacity building under Objective 2, Kosovo continues to face several implementation challenges that limit the effectiveness and sustainability of its cybersecurity resilience efforts. While the National Cybersecurity Strategy 2023-2027 outlines ambitious goals related to human capital development, public awareness, and institutional strengthening, translating these objectives into practice remains uneven. One key challenge is the shortage of trained personnel and specialized expertise within public institutions[23]. Compared with EU practices, where national CSIRTs often employ dozens of technical specialists, Kosovo's cybersecurity institutions operate with significantly smaller teams, limiting their ability to monitor threats, conduct incident response, and develop long-term cybersecurity programs. Limited allocations for cybersecurity and cyber defense constrain investments in critical technologies, infrastructure, and workforce development necessary to protect against cyberattacks[24].

Furthermore, although awareness-raising initiatives and educational programs represent positive steps, these efforts are not yet embedded within a long-term national capacity-building framework. Key challenges include the limited integration of cybersecurity into primary and secondary education curricula beyond basic information technology modules, a shortage of qualified cybersecurity professionals to serve as educators and mentors, and the absence of a coordinated, centralized approach to cybersecurity training. In addition, there is no cl ear national assessment of labor-market and industry needs for cybersecurity expertise, which constrains the strategic development of skills and capacities[25]. International good practices emphasize capacity building should be continuous, coordinated, and supported by dedicated resources, rather than project-based or fragmented interventions[26]. Without sustained funding, structured career pathways, and institutional coordination, Kosovo risks gaps between strategic intent and operational impact.

Despite these challenges, the Government of Kosovo has taken several steps to address cybersecurity. These include the establishment and strengthening of institutional actors such as the National Cybersecurity Unit (KOS-CERT), the Agency for Information Society of Kosovo (ASHIK), the Kosovo Security Council (KSC), the Kosovo Police Cybercrime Unit, and the Cyber Security Centre of Excellence (CSOC). In parallel, the government has increased budgetary allocations for cybersecurity and adopted updated cybersecurity-related legislation to improve the legal and institutional framework[27]. Nevertheless, these measures remain insufficient to fully address existing capacity gaps, and further coordinated and sustained efforts are required to ensure effective implementation and long-term resilience.

---

[23] Neziri, S., & Këpuska, K. (2025). *Securing our critical infrastructure*. Kosovo 2.0.
[24] Balkans Group. (2023). Cyber security in the Western Balkans [Policy report].
[25] Kosovo Center for Security Studies (KCSS). (2023). Kosovo's Take on Cybersecurity. Security Brief.
[26] Organization for Security and Cooperation in Europe. Cyber/ICT security.
[27] Balkans Group. (2023). Cyber security in the Western Balkans [Policy report].

4.2. Gaps in Regional and International Cybersecurity Cooperation (Objective 4)

Objective 4 places strong emphasis on regional and international cooperation; however, Kosovo's engagement remains exploratory and informal rather than institutionalized. Several factors may explain this limited engagement, including political constraints related to Kosovo's international recognition, limited financial and human resources for cybersecurity institutions, and a lack of structured public-private dialogue mechanisms. These factors can slow the development of formal partnerships and operational cooperation frameworks. While Kosovo participates in regional dialogues and initiatives, such as meetings with Western Balkans counterparts and involvement in EU-supported regional cybersecurity projects, many of these interactions have yet to mature into formalized cooperation mechanisms with clear mandates, shared protocols, or joint operational capacities. This limits Kosovo's ability to respond effectively to cross-border cyber threats, which by nature require coordinated regional responses.

International and regional frameworks stress the importance of structured cooperation through trusted networks, national CERT partnerships, and institutionalized information-sharing arrangements[28]. Kosovo's partial participation in these mechanisms reflects broader political and institutional constraints, but it also highlights the need for clearer prioritization and follow-through in implementing Objective 4 at both the strategic and technical levels.

Kosovo's standing in the National Cyber Security Index (NCSI) features additional gaps in national and international coordination, particularly in strategic planning and the implementation of structured action plans[29]. Although a national strategy exists, operationalization and alignment with regional and EU cybersecurity frameworks remain incomplete.

In 2025, the Kosovo Banking Association (KBA), through its Cybersecurity Committee, reached an agreement to join MISP (Malware Information Sharing Platform), an international platform for sharing cybersecurity threat intelligence headquartered in Luxembourg[30]. This represents a significant step toward strengthening the resilience of Kosovo's banking sector against cyber threats and crimes by fostering collaboration with a global cybersecurity network. Similar initiatives across other industries would further improve national cyber resilience and support broader objectives of capacity building and international cooperation.

[28] European Union Agency for Cybersecurity (ENISA). National cybersecurity.
[29] Estonian e-Governance Academy (EGA). (2025). *National Cyber Security Index – Kosovo*.
[30] Kosovo Banking Association. (2025). *Kosovo Banking Association joins the international cybersecurity platform MISP*

4.3. Alignment with EU Cybersecurity Frameworks and Cyber Diplomacy Practices (Objectives 2 and 4)

A further policy issue concerns the gap between Kosovo's strategic alignment with EU cybersecurity norms and the practical implementation of these standards. While Kosovo has committed to EU frameworks such as the NIS Directive and the NIS2 Directive, achieving effective alignment requires more than legislative approximation. It also depends on institutional readiness, risk management capabilities, incident response coordination, and participation in EU cyber cooperation mechanisms.

Kosovo has aligned its cybersecurity legal framework with EU standards through the Law on Cybersecurity (No. 08/L-173), passed in 2023, which transposes EU Directives (EU) 2013/40 and (EU) 2016/1148[31], and the Law on Critical Infrastructure (06/L-014), passed in 2018, which implements EU Directive 2008/11/EC[32]. However, it is important to note that EU Directive 2008/114/EC, which initially served as the foundation for Kosovo's law, has been repealed and replaced by the new Directive (EU) 2022/2557. This change signifies a major shift in the EU's approach to critical infrastructure, moving from a protection-based model to a resilience-oriented framework[33]. As a result of this evolution in EU policy, there is an urgent need for Kosovo to revisit and amend its Law on Critical Infrastructure to ensure alignment with Directive (EU) 2022/2557 and to incorporate the latest standards in critical infrastructure management.

In the field of cyber diplomacy, international norms state that credible engagement requires robust domestic capabilities. UN resolutions on responsible state behavior in cyberspace[34] underline that capacity building (Objective 2) and international cooperation (Objective 4) are interdependent. If Kosovo lacks sufficient domestic capacity, its ability to engage effectively in cyber diplomacy is compromised. Conversely, limited international collaboration hampers learning, trust-building, and institutional development.

In this context, cyber diplomacy is not just about participating in international initiatives; it is a policy capability that relies on robust domestic institutions. Kosovo faces challenges such as limited technical capacity, fragmented coordination, and unclear institutional leadership, which restrict its participation in cyber diplomacy. This includes participation in norm-setting discussions, confidence-building measures, and coordinated diplomatic responses to malicious cyber activities. Therefore, strengthening domestic capacity under Objective 2 is key for Kosovo to be viewed as a credible and reliable partner in international cyber diplomacy frameworks.

Kosovo's Ministry of Internal Affairs and the Ministry of Foreign Affairs and Diaspora have important roles by developing policies and participating in cyber diplomacy training through the

---

[31] Government of Kosovo. Law on Cybersecurity (No. 08/L-173). Official Gazette of the Republic of Kosovo.
[32] Government of Kosovo. Law on Critical Infrastructure (No. 06/L-014) Official Gazette of the Republic of Kosovo.
[33] Limaj, B. (2024). Aligning Kosovo's Critical Infrastructure Law with the EU's Directive on the Resilience of Critical Entities and EU's NIS2 Directive. A Comparative Study. Kosovar Center for Security Studies (KCSS).
[34] United Nations. (2021). *Developments in the field of information and telecommunications in the context of international security: Report of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security*. United Nations.

Cyber Balkans project[35]. This initiative aims to build resilient cyber teams capable of meeting both regional and EU expectations.

Overall, these challenges suggest that while Kosovo's cybersecurity strategy is normatively aligned with international and EU expectations, greater emphasis is needed on implementation, coordination, and sustainability to ensure that Objectives 2 and 4 effectively support Kosovo's broader goals of cyber resilience, international credibility, and EU integration.

[35] EU Support to Western Balkans Cybersecurity Capacity Building. (2025). CILC.

5. Conclusion & Recommendations

After several cyber-attacks, the Government of Kosovo recognized the need to develop the National Cybersecurity Strategy 2023–2024. This strategy establishes a comprehensive framework for creating secure cyberspace, which is essential for the development of ICT and internet-based services for citizens, businesses, and government institutions, while aligning with the objectives of Kosovo's Digital Agenda 2030[36].

An analysis of the National Cybersecurity Strategy reveals both progress and shortcomings in Kosovo's cybersecurity landscape, particularly concerning Objectives 2 and 4. International and regional frameworks, including EU Directives (NIS/NIS2), UN guidelines on responsible state behavior in cyberspace, and OSCE capacity-building practices serve as valuable benchmarks for Kosovo in its strategic planning. While Kosovo has shown year-on-year improvement, more effort is needed to meet the objectives regarding capacity building and cyber diplomacy, which are critical for enhancing cybersecurity and mitigating potential threats.

Drawing on these findings, several policy recommendations can help strengthen Kosovo's cybersecurity capacity and improve the implementation of Objectives 2 and 4 of the National Cybersecurity Strategy.

First, Kosovo should prioritize strengthening national cybersecurity capacity by expanding training initiatives and professional development opportunities for cybersecurity personnel within public institutions. This could be achieved through partnerships with reputable international training organizations, universities, and credible online learning platforms that specialize in cybersecurity education. In addition, integrating cybersecurity topics, such as ethical hacking, cyber awareness, and digital safety, into the educational curriculum at different levels would contribute to building a sustainable pipeline of skilled professionals. The government should also develop programs aimed at attracting and retaining information security and IT professionals in the public sector by offering competitive compensation packages, professional development opportunities, and clear career advancement pathways.

Second, greater emphasis should be placed on promoting public-private partnerships in cybersecurity. Strengthening collaboration between government institutions and private sector actors can improve the overall resilience of Kosovo's digital infrastructure. Joint initiatives and coordinated programs can facilitate the sharing of cyber threat intelligence across sectors, allowing institutions to detect and respond to cyber incidents more effectively. Platforms such as the Malware Information Sharing Platform (MISP), which enable collaborative threat intelligence exchange, offer practical examples of how structured cooperation between stakeholders can strengthen collective cybersecurity defenses.

[36] Government of Kosovo. (2023). National cybersecurity strategy 2023–2027. Ministry of Internal Affairs.

Third, Kosovo should advance regional and international cybersecurity cooperation in order to address the cross-border nature of cyber threats. Formalizing participation in regional cybersecurity frameworks, including WB6-EU initiatives and other Western Balkans cyber networks, would help institutionalize existing cooperation and strengthen operational coordination. Kosovo should also increase its engagement in EU-oriented cybersecurity networks, including collaboration with the European Union Agency for Cybersecurity (ENISA) and participation in EU cyber diplomacy initiatives. Continuous training and participation in international cyber diplomacy programs would further strengthen Kosovo's capacity to engage credibly in international cybersecurity governance.

Fourth, Kosovo should continue to update and align its legal and regulatory framework with evolving European cybersecurity standards. In particular, revising the Law on Critical Infrastructure to align with EU Directive (EU) 2022/2557 on the resilience of critical entities would strengthen the country's approach to infrastructure protection. Regular legislative reviews are also necessary to ensure that Kosovo's legal framework remains responsive to emerging cyber threats and clearly defines the responsibilities of both public and private sector stakeholders in cybersecurity governance.

Fifth, strengthening Kosovo's cyber diplomacy capacity is essential for improving international cooperation and policy coordination. Clarifying institutional leadership for cyber diplomacy between the Ministry of Foreign Affairs and Diaspora and the Ministry of Internal Affairs would improve policy coherence and coordination in international cybersecurity engagements. Developing a national cyber diplomacy strategy aligned with EU and United Nations cybersecurity frameworks would further support Kosovo's ability to participate effectively in international cybersecurity discussions and initiatives.

Finally, Kosovo should establish mechanisms to monitor and benchmark progress in cybersecurity governance. Utilizing international indices such as the National Cyber Security Index (NCSI), alongside EU benchmarking frameworks, would help evaluate national cybersecurity performance and identify areas requiring improvement. In addition, establishing measurable key performance indicators (KPIs) for the implementation of Objectives 2 and 4 would enable institutions to track progress in capacity building and international cooperation more effectively.

By strengthening institutional capacity, improving international cooperation, and aligning its governance framework with EU standards, Kosovo can enhance its cyber resilience while supporting its broader objective of integration into European security and digital governance structures.