Enhancing Kosovo's cyber resilience: Aligning NATO strategies and cyber diplomacy

By Marigonë Vrajolli

The views expressed in this paper are solely those of the author and do not necessarily reflect the official position of any institution.

Executive Summary

As an aspiring member of NATO, Kosovo confronts significant challenges in building cyber resilience, remaining vulnerable to sophisticated hybrid threats that undermine national security. This policy paper advances a high-level strategic framework aimed at strengthening Kosovo's defensive posture through the systematic alignment of national policies with Euro-Atlantic norms and standards, while elevating cyber diplomacy as a core instrument of statecraft.

The strategy adopts a comprehensive "whole-of-society" approach, integrating the Cyber Security Agency (CSA) within a broader, proactive diplomatic track. By addressing institutional fragmentation, enhancing inter-agency coordination, and enhancing democratic oversight, Kosovo can shift from a reactive stance to a responsible actor that actively contributes to regional and collective Euro-Atlantic security.

Introduction

The cyberspace has become a critical domain of international security, directly affecting state stability and institutional functionality. Cyberattacks, hybrid operations, and disinformation campaigns are increasingly used as instruments of aggression against other states by both state and non-state actors (UN GGE 2021; NATO, 2024). As a result, cybersecurity is regarded as a highly important component of foreign policy, national security, and multilateral diplomacy.

At the global level, the United Nations has played a key role in promoting responsible state behavior in cyberspace through the work of the Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG). Since 2010, UN GGE reports have identified cyber threats as among the most serious challenges of the twenty-first century. The 2015 UN GGE report represents a turning point by outlining a framework for responsible state behavior and a set of norms, while the 2021 report provides initial guidance for implementation and includes national views on the application of international law values and norms in cyberspace (UN GGE 2015, 2021).

Similarly, NATO recognizes cyberspace as an operational domain and has developed strategies to strengthen cyber resilience, counter threats, and ensure the collective defense of its members and partners (NATO, n.d). NATO also supports non-member countries in developing cybersecurity governance, institutional capacity, and technological capabilities to address hybrid threats (NATO Parliamentary Assembly, 2024). Programmes such as NATO SPS cyber projects, NALT, Cyber Coalition, and Locked Shields exercises offer practical avenues for Kosovo to build capacity and enhance interoperability.

Kosovo, as a state aspiring to NATO membership, participates in several cooperative initiatives but still faces challenges, including limited cyber capacity, exposure to hybrid threats, and incomplete implementation of a comprehensive national cybersecurity policy (Government of Kosovo 2023). Strengthening cyber diplomacy, the use of diplomatic tools to coordinate international cyber efforts is essential for Kosovo on building trust and enhancing cooperation with NATO and its member states.

Methodology

This policy paper employs a qualitative research approach based on desk research and policy analysis. It draws on primary policy documents from NATO, the European Union, and Kosovo's national institutions, as well as reports from the UN GGE and OEWG. The analysis is complemented by regional cybersecurity assessments and a comparative case study of North Macedonia's pre-accession reforms (DCAF, 2021b). This approach enables the identification of structural gaps and supports the development of policy recommendations aligned with Euro-Atlantic standards.

Kosovo's position in the international cyber environment

Kosovo has made significant progress in positioning itself as an increasingly active and constructive state in the international cyber environment. As a state aspiring to membership in NATO and other regional and international organizations, Kosovo has demonstrated a commitment to strengthening its cybersecurity position and aligning its policies with Euro-Atlantic standards (Government of Kosovo 2023).

In the National Cyber Security Strategy of Kosovo 2023-2027, one of the goals is to create an approach to cybersecurity, based on national objectives and priorities, expected to be achieved during the period 2023-2027. The strategy calls for the creation of a clear framework for cooperation with other countries to prevent, detect, warn and address cyber incidents. This includes promoting international cooperation on cybersecurity and cooperation in the fight against cybercrime, as well as using diplomacy to coordinate efforts against cyber aggression, otherwise known as cyber diplomacy (Government of Kosovo 2023).

Recent cyber incidents targeting public institutions and critical digital services have underscored the urgency of these reforms. Disruptions to government platforms and attempts to compromise institutional networks highlight Kosovo's vulnerability to politically motivated cyberattacks and hybrid operations (CSIS, n.d.; Carnegie Endowment, n.d.). These incidents have served as catalysts for raising national awareness, accelerating institutional reforms, and strengthening the importance of cyber defense and international cooperation, particularly with strategic partners.

A central pillar of Kosovo's cybersecurity aim is the planned establishment of the Cyber Security Agency (CSA). This Agency serves as the technical "engine" for national resilience, centralizing incident response and infrastructure protection. By centralizing cybersecurity functions, the CSA aims to address existing fragmentation and improve efficiency in threat detection and response.

The strategy also introduces a regulatory framework for Operators of Essential Services (OES) and Digital Service Providers (DSP), aligning Kosovo's approach with the EU NIS Directive. This regulatory dimension is essential for protecting critical infrastructure and ensuring a minimum level of cybersecurity across key sectors (Government of Kosovo 2023).

At the international level, Kosovo has engaged actively with NATO and EU-supported initiatives, including training programs, exercises such as Cyber Coalition and Locked Shields, and capacity-building projects under the Science for Peace and Security (SPS) Programme (NATO, n.d;). These engagements have contributed to the development of technical expertise and interoperability with international partners.

Despite not being a member of the United Nations, Kosovo aligns its policies with the norms and principles developed through the UN GGE and OEWG processes. This alignment demonstrates Kosovo's commitment to responsible state behavior and enhances its credibility in the international cyber environment.

However, challenges remain. Institutional fragmentation continues to limit coordination among key actors, while legislative and regulatory frameworks are still evolving (DiploFoundation, 2018). Moreover, Kosovo's limited access to NATO platforms and intelligence-sharing mechanisms constrains its ability to respond effectively to emerging threats.

A critical dimension of Kosovo's cybersecurity strategy is the integration of technical and diplomatic functions. The CSA serves as the technical engine of cyber resilience, while the Ministry of Foreign Affairs leads cyber diplomacy efforts, representing Kosovo in international forums and facilitating cooperation with strategic partners. This internal-external linkage reflects a "whole-of-government" approach consistent with NATO's resilience framework and mirrors successful models observed in North Macedonia prior to its NATO accession (DCAF, 2021d).

Problem definition

Kosovo's limited engagement with international norm-implementation processes, particularly those promoted through the UN GGE and OEWG, creates gaps in the alignment of national policies with international best practices. Existing assessments of cyber threats in the Western Balkans indicate that the region faces cyber and hybrid challenges, while institutional coordination and long-term capacity development remain uneven (DCAF 2021a). As a result, regional cooperation on cybersecurity remains fragmented and underutilized (DCAF, 2021e).

The primary challenge to Kosovo's cyber resilience is a structural misalignment between its national technical capabilities and the "Whole-of-Society" resilience standards mandated by NATO's 2021 Enhanced Cyber Defence Policy. Currently, Kosovo's engagement is constrained by three specific gaps:

Status Gap: While Kosovo operates a national MISP ecosystem across its critical sectors (ASHI, KOSTT, telecoms, banks), its non-NATO and non-PfP status denies it access to restricted Allied threat repositories, creating an institutional "blind spot" in real-time international cyber intelligence.

Technical-Military Gap: Despite the creation of the State Cybersecurity Training Centre within the MoD/KSF, it needs to operate in close coordination with the national civilian CERT. Bridging this inter-agency gap is essential for achieving a unified national response to hybrid threats.

Diplomatic Gap: Cyber issues remain soloed within technical agencies (such as ASHI). Notably, there is no dedicated cyber diplomacy representation within Kosovo's mission/embassy in Brussels covering NATO and the EU, nor at NATO's CCDCOE in Tallinn. This limits Kosovo's ability to influence regional norm-setting and to secure high-level capacity-building projects in the field of cybersecurity.

Policy objective

The objective of this policy proposal is to enhance Kosovo's cyber resilience by integrating NATO-aligned capacity-building efforts with a structured cyber diplomacy approach. This integration would strengthen institutional preparedness, improve coordination with international partners, and enable more effective participation in global and regional cyber governance (NATO, n.d.). Complementary EU cooperation and regional initiatives can further support Kosovo's cyber readiness, drawing on the frameworks established by the ENISA Threat Landscape reports and the EU Cyber Diplomacy Toolbox.

Policy recommendations

Recommendation 1: Formalize Cyber Diplomacy through a Dedicated Attaché

The Ministry of Foreign Affairs (MFA) should establish a Cyber Security Attaché role within the Mission of the Republic of Kosovo to the EU and NATO. The Government of Kosovo should capitalize on its existing Diplomatic Mission to NATO (currently at the Ambassadorial level) and its Military Attaché accredited to Belgium to bridge the Diplomatic Gap. Additionally, the government should expand the mandate of the existing Military Attaché to include a specialized "Cyber Defense Portfolio."

This official will liaise with NATO's Public Diplomacy Division and secure a seat for Kosovo as a "Contributing Participant" in exercises like Locked Shields and Cyber Coalition (CCDCOE, 2025).

Recommendation 2: Leverage the NATO Science for Peace and Security (SPS) Programme

Kosovo should shift from general training participation to technical, project-based alignment by proposing a multi-year SPS Cyber Defence project focused on "Cyber Incident Response and Malware Analysis" (NATO, n.d).

Kosovo could be a partner with a NATO member state (e.g., Estonia or Croatia) to co-lead the project, ensuring the KSF receives NATO-standard hardware and software for a tactical cyber lab. Kosovo have excellent relations with Croatia in the field of security.

Recommendation 3: Expand the NATO Advisory and Liaison Team (NALT) Mandate

The government should request an expansion of the NALT's advisory scope to include the development of a "Cyber Defence Concept" for the KSF. Align the KSF's cyber units with NATO's Multi-Domain Operations doctrine, ensuring that Kosovo units become interoperable even before formal membership.

Recommendation 4: Establish a Regional "Cyber-Transparency" Track via the Adriatic Charter (A5)

Kosovo should propose a "Western Balkans Cyber Resilience Hub" under the A5 framework. Hosting annual exercises on Critical Infrastructure Protection (CIP), (OSCE, n.d.). To build Confidence Building Measures (CBMs) with regional neighbors and demonstrate to NATO allies that Kosovo is a proactive security provider in the Western Balkans (Cybil Portal, 2025).

Recommendation 5: Professionalize through "Shadowing" at the CCDCOE

Even without formal NATO or PfP membership, Kosovo should seek a Memorandum of Understanding (MoU) with one of NATO's 30 centers of excellence, such as the NATO Collaborative Cyber Defense Center of Excellence (CCDCOE). The government should fund a "Visiting Fellowship" for a senior technical expert from ASHI and a military officer from the KSF.

Recommendation 6: Strengthen Parliamentary Oversight

In accordance with international DCAF standards for good governance (DCAF, 2021*c*), the Assembly of Kosovo should establish a specialized sub-committee on cybersecurity within the Committee on Security and Defense Affairs. This committee must have the clear mandate to audit the CSA's operations and the KSF's cyber-budget, ensuring democratic accountability and transparency (DCAF, 2023).

Recommendation 7: Human Rights and Data Protection

All new cyber regulations must include mandatory Data Protection Impact Assessments (DPIAs) (DCAF, 2023). Aligning with GDPR standards ensures that cybersecurity measures do not infringe upon the privacy rights of Kosovo's citizens, fulfilling a core requirement for EU integration.

Conclusion

By linking cyber capacity-building with proactive cyber diplomacy, Kosovo can enhance its resilience to cyber and hybrid threats, improve interoperability with NATO, and establish itself as a credible and responsible actor in international cyberspace governance. This integrated approach would contribute not only to Kosovo's national security, but also to broader regional and Euro-Atlantic stability.

By adopting these targeted measures, Kosovo transitions from passive alignment to active partnership. This strategy mitigates the limitations of non-membership by utilizing existing NATO "side-doors" (SPS, NALT, A5), ultimately proving Kosovo's readiness for the NATO Cyber Defence Pledge requirements.

In the National Cyber Security Strategy 2023–2027, the establishment of the Cyber Security Agency (CSA) is the most important part of Kosovo's digital protection and its harmonization with international standards such as the EU NIS Directive.

The cooperation between the Cyber Security Agency and the Ministry of Foreign Affairs and Diaspora in Kosovo (MFA) is structured mainly around Cyber Diplomacy and Kosovo's international representation. According to the strategy and supporting legal framework in this regard:

The CSA is tasked with providing the technical expertise necessary for the MFA to lead cyber diplomacy efforts. This includes representing Kosovo in international forums.

The Agency acts as the main point of contact for international technical cooperation. It works with the MFA to establish frameworks for mutual legal assistance and information sharing with other countries and organizations such as NATO and the EU as well as Kosovo's partner states.

While the Ministry of Internal Affairs (MIA) initially leads the drafting of the strategy, the ACS and the MFA cooperate to ensure that national cyber policies are aligned with Kosovo's foreign policy goals, such as integration into NATO and the EU and other mechanisms of both organizations.

In conclusion, the Agency essentially serves as the technical engine that allows the MFAD to act as a diplomatic shield in the international cyber environment.

Sources

Carnegie Endowment for International Peace (n.d.) *International cybersecurity norms*. Available at: carnegieendowment.org (Accessed: 29 March 2026).

CSIS (n.d.) *Significant cyber incidents database*. Center for Strategic and International Studies. Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (Accessed: 27 March 2026).

Cybil Portal (2025) *Resilient and responsive cybersecurity in the Western Balkans 2024-25*. Available at: cybilportal.org (Accessed: 27 March 2026).

DCAF (2021a) *Cybersecurity capacity building and donor coordination in the Western Balkans*. Geneva Centre for Security Sector Governance. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CybersecurityCapacityBuilding_DonorCoordination_inWB_mar2021.pdf (Accessed: 17 March 2026).

DCAF (2021b) *Cybersecurity policy development and capacity building: increasing regional cooperation in the Western Balkans*. Geneva Centre for Security Sector Governance. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CybersecurityPolicyDevelopment_CapacityBuilding_in_WB_mar2021.pdf (Accessed: 31 March 2026).

DCAF (2021c) *Guide to good governance in cybersecurity*. Geneva Centre for Security Sector Governance. Available at: dcaf.ch (Accessed: 19 February 2026).

DCAF (2021d) *National cybersecurity strategies in Western Balkan economies*. Geneva Centre for Security Sector Governance. Available at: dcaf.ch (Accessed: 25 February 2026).

DCAF (2021e) *Western Balkan CERT cooperation*. Geneva Centre for Security Sector Governance. Available at: dcaf.ch (Accessed: 31 March 2026).

DCAF (2023) *Cybersecurity and human rights in the Western Balkans: mapping governance and actors*. Geneva Centre for Security Sector Governance. Available at: dcaf.ch (Accessed: 25 February 2026).

DiploFoundation (2018) *Cybersecurity in the Western Balkans: policy gaps and cooperation opportunities*. Available at: diplomacy.edu (Accessed: 31 March 2026).

Government of Kosovo (2023) *National cyber security strategy 2023–2027*. Pristina: Ministry of Internal Affairs. Available at: rks-gov.net (Accessed: 14 January 2026) [Government of Kosovo 2023].

ISAC Fund (2022) *Western Balkans: emerging cyber threats – cybersecurity ecosystem report*. Produced in cooperation with PwC. Available at: isac-fund.org (Accessed: 24 March 2026).

NATO (2024) *Washington Summit Declaration.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. Available at: nato.int (Accessed: 20 January 2026).

NATO (n.d.) *Cyber defence*. Official Policy Topic Overview. Available at: nato.int (Accessed: 22 March 2026).

OSCE (n.d.) *ICT security and confidence-building measures*. Organization for Security and Co-operation in Europe. Available at: osce.org (Accessed: 20 March 2026).

UN GGE (2021) *Report of the group of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security*. United Nations. Available at: https://digitallibrary.un.org/search?ln=en&as=0&p=subjectheading:[UN.+Group+of+Governmental+Experts+on+Developments+in+the+Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security] (Accessed: 23 March 2026).