POLICY PAPER
NOTE DE RECHERCHE
N° 195

*Megghi Pengili * - 3 September 2026*

Knowledge as Armour: Adaptive Governance and the Western Balkan Cyber Revolution

Thirty-two severe cyberattacks** on critical infrastructures between 2000 and 2026[1] made one reality undeniable: traditional risk governance across the Western Balkans is no longer enough. Conventional research prioritises cyberconflicts and technical capabilities but overlooks the emergence of adaptive, learning-driven governance that affects resilience. This paper bridges this gap by pioneering a resilience model that integrates the EU's NIS2 directive, NIST CSF 2.0 and learning flows. This model is shaped by the region's cyberposture and presents a novel blueprint for national cyberreadiness which, in this case, is not just a domestic necessity for the region's countries but a cornerstone for EU membership and collective EU cyberresilience.

Foreword

Critical Infrastructure (CI) sectors in the Western Balkans (WB6), including energy, renewables, water, ICT, transportation, agriculture, public health, security and defence, have faced 32 attacks over the past 26 years[2]. Cybercrimes occur at a high frequency - over 2,348 attacks per day, totalling nearly 850,000 per year - with damages of $10.5 trillion only in 2025.[3] These figures highlight the complexity and uncertainty these incidents create for the CIs. While the region's economies leverage digitalisation and cybertechnologies to support their EU membership goals[4], cyberrisks threaten this digital transition. In response, WB countries, namely Albania, Bosnia and Herzegovina, Montenegro, Kosovo, North Macedonia and Serbia, advance adaptive cybergovernance as an approach to build resilience. Already introduced as a necessity in Niinistö's and Draghi's reports (2024), adaptive governance aligns stakeholders for proactive management and crisis preparedness.[5]

Beyond economic growth and employment, cybermarket developments define governance's material and human capabilities. By 2025, Serbia led with revenue of $28.95m, followed by Montenegro with $12.69m and Bosnia and Herzegovina with $11.17m.[6] Meanwhile, the region's economies are updating and aligning their national regulations with EU policies and strategies such as ECI Directive 2008/114, NIS2 Directive, and the Council of Europe Convention (CoE) on Cybercrime Directive 2013/40/EU.[7] Further, these economies cooperate regionally through resource-sharing initiatives such as the Western Balkans Cyber Capacity Centre (WB3C), the Geneva Centre for Security Sector Governance (DCAF), the Global Forum on Cyber Expertise (GFCE), and the e-Governance Academy.[8]

The WB6 advance unusual leadership strategies and a compelling vision that relies on peer learning, adoption of international and national norms and cooperation mechanisms. Ultimately, this approach provides participating countries with resilience and preparedness solutions that cannot be achieved nationally. This analysis offers a conceptual contribution to the ongoing dialogue between academia, technocrats and decision-makers, and an emerging model for cyberrisk management that explains how organisations translate lessons from cyberposture into capabilities. The suggested model integrates learning flows, the NIST Cybersecurity Framework (CSF) 2.0 for risk assessment and mitigation, and its translation into the NIS2 EU Directive. While both NIST CSF 2.0 and NIS2 are very technical (either law- or procedures-oriented), they overlook learning for resilience, which this model addresses and adds to the literature on adaptive governance in cyber.

Navigating the Cyberinterplay of Governance and Threats in a Turbulent Region

A country-scale cyberattack estimates damages of over €10m per day[9]. Multiplying this value by the number of attacks, the result is alarming for WB6, which considers critical infrastructure and connectivity indispensable to economic growth and EU integration.[10]

* **Megghi Pengili** *is a CIFE Alumna, Executive Master in EU Studies (2016-2018). Currently, she is an Adjunct Lecturer at Centro Formazione Logistiche Interforze (CeFLI)-Italian Army and an external expert for CIFE's "EU Connect" Programme. She holds a PhD in Defence Studies. Her research area centres on defence innovation governance and Mediterranean studies.*

** *For all cyber terms the paper refers to the Associated Press Style as the landmark for technical terminology, and the Economist style guide*

Disclaimer - *The views expressed in this publication are solely those of the author and do not reflect the views of any affiliated institutions.*

Given that advancement of cybertechnologies is both a factor in cybersecurity and a cyberthreat, building adaptive governance on multiple and novel cybercapabilities amongst collaborative networks is an imperative.[11] In that regard, according to the Global Cybersecurity Index 2024, Serbia has progressed as a role model for cybersecurity compared with the rest of the region.[12] The data illustrating the innovation performance and performance in cybercapabilities in WB6 suggest that achieving effectiveness in cyber governance faces significant barriers, mainly due to the illiteracy of decision-makers on cybersecurity matters.[13] This illiteracy penalises cyberexpertise through scarce capacity-building and the lack of a solid cybersecurity culture.[14] Doing cyber resilience requires a cultural shift that "embodies learning into a capability".[15]

Learning invokes changes in actors and networks' actions; it can be formal, informal, or a hybrid of the two, and entails sharing tacit and explicit knowledge across the organisation or the institution. Formal and informal learning can be either external or internal depending on the strategic constraints of specific collaborative networks. Hybrid learning entails a more evolved approach with multiple methods and perspectives moving beyond organisational boundaries and rational thinking.[16] In other words, achieving cyberresilience requires hybrid learning that allows for continuous risk evaluation, comprehensive response and adaptability for effective decision-making.

Adaptive cyber governance which builds upon public-private capabilities, is not yet fully embedded in the long-term agendas of the region's economies. In that regard, compared to the rest of the region, Bosnia and Herzegovina lags behind.[17] Regionally, the WB6 support joint cyber capacity-building efforts, through training under the leadership of the WB3C in Montenegro and the e-Governance Academy Estonia,[18] which assist the region's EU membership ambitions to align with EU cyberlegislation.[19] So, building cyber capabilities serves dual purposes: fostering national interests and foreign policy agendas of allies and strategic partners.[20]

The WB6 have benefited from extensive international support to strengthen cyber capacity, foster resilience and promote regional governance. The US, via NATO engagement, has provided cyber expertise and training - e.g in Montenegro after its 2017 NATO accession - as well as support through institutions like Carnegie Mellon's Software Engineering Institute and the George C. Marshall Centre's.[21] Besides, Albania and North Macedonia participated in NATO- and EU-led cyber exercises and capacity-building efforts. Albania signed an MoU with the NATO Cyber Incident Response Centre (NCIRC) in 2013.[22] Also, the EU Digital Agenda guides the region's digital transformation through the Digital Agenda for the Western Balkans and funding initiatives such as the IPA program and ENCYSEC, focused on boosting cybercrime capacity, supporting CERTs and enhancing public-private collaboration.[23] Further, the UK's DCAF project and Chevening Fellowship and the World Bank's cybersecurity assessments, have further contributed to national and regional progress.[24] The World Bank undertook a Global Cybersecurity Capacity Program (2016-2019), funding Capability Maturity Model assessments by the Global Cybersecurity Capacity Centre (GCSCC) of Oxford University. This support included assessments in Albania, Bosnia and Herzegovina, Serbia and North Macedonia.[25] The OSCE promotes legal, democratic and strategic frameworks, supports public-private dialogue and national strategies, especially in Serbia and Bosnia.[26]

By collaborating on cyber capability building, these countries build stronger regional bonds, which add to the gradual buildup of the region's cyber posture. A cyber posture is a dynamic concept that requires understanding of information management, cyber capabilities, deterrence and resilience. As a key component of cyberposture, adaptive governance entails learning processes that help the region ensure the appropriate use of systems and comply with relevant laws, regulations and guidelines for risk management, such as the EUNIS2 and NIST CSF 2.0.

Building a Cyberposture: Governance & Engagement

The development of the Western Balkans' cyber posture consists of four progressive stages as described below. Each one is designed to strengthen governance to predict, prevent and mitigate threats. The posture suggests the emergence of an innovative model for cyber risk management, which, in the case of the WB, integrates EU NIS2, NIST CSF 2.0 and learning flows across all risk management steps. This model aggregates robustness, systemic resilience and defence, by touching upon regulations, operations for managing incidents through knowledge hubs.

· ***From Data Protection to Cyber Regulation***

WB6 are boosting cybersecurity for critical infrastructure through national reforms and regional cooperation. The WB Cyber Capacity Centre (WB3C) in Podgorica delivers EU-standard training in cybercrime, cybersecurity and digital diplomacy, supporting alignment with the EU NIS 2 Directive.[28] Serbia, Kosovo and North Macedonia have passed GDPR-aligned data protection laws, enhancing governance and breach reporting, while Albania, Montenegro and Bosnia and Herzegovina are progressing more slowly due to limited training for their authorities.[29] Serbia's 2025 Information Security Act, based on NIS2, expands coverage to more ICT entities and introduces stricter risk assessment requirements, distinguishing between "essential" and "important" operators.[30] Albania's National Cybersecurity Strategy 2025–2030 and its Action Plan 2025–2027 align national policies with the EU NIS2 directive, the eIDAS2 digital identity regulation and the EUCC cybersecurity certification framework.[31] North Macedonia's cybersecurity law came into force on 1 January 2026, bringing the country's legal framework in line with the EU's NIS2 Directive.[32] Following the 2022 cyber crisis, Montenegro adopted a new Law on Information Security aligned with the EU NIS2 Directive, reinforcing regulatory oversight and clarifying responsibilities across critical sectors.[33] The Directive requires national strategies for supply chain security, vulnerability management and education, addressing the growing threat of cyberattacks. These attacks threaten the confidentiality, integrity, and availability of digital assets, making regional cooperation and continuous improvement essential.

· ***From a National Governance Approach to a Compromised Regional Approach***

At the Prague Cybersecurity Conference in 2025, the session on Empowering Regions through Cyber Capacity Building emphasised the need for knowledge exchange to strengthen both regional and international capabilities through cooperation. Representatives from the Western Balkans highlighted uneven cybersecurity capabilities across their countries, increasing vulnerability to financial losses. Therefore, a standard security policy tailored to the countries' varied capabilities is critical to protecting information systems and assets for cyberstability.[34]

To build cyber resilience, the Global Forum on Cyber Expertise launched a regional project team for 2025, focusing on a cybersecurity needs database for the WB6 and updating its Cybil platform. Similarly, the Regional Cooperation Council's iniatives promote high-level dialogue among CSIRTs, helping regional governments align with EU standards.[35] The WB3C became operational in late 2023, using a train-the-trainers model, with extensive training scheduled for the coming years.[36] Talent management, retention and replenishment cycles are crucial to cybercapacity building. Governments in Albania, Kosovo and North Macedonia benefit from regional expertise, while private sector involvement and multistakeholder working groups in Kosovo support critical infrastructure information sharing.[37] There is no one-size-fits-all approach to capacity building; the context of each government and society matters. That said, building trust, effective regional cooperation and donor collaboration are necessary for defending critical infrastructure. Given the limited resources in the Western Balkans, international partnerships are vital for resilience and talent development.[38] The World Economic Forum Cybersecurity workshop, co-hosted with the WB3C and held in May 2025, addressed strategic approaches to close the cybersecurity talent gap.[39]

· ***Promoting Cyber Norms Through Cyberesilience***

Talent is not the only key challenge for the Western Balkans in cyberspace. Establishing collaborative state behaviour requires three elements: agreeing on nonbinding ICT norms, building confidence that states will follow these rules and ensuring all countries have the adaptive governance and capacity to participate effectively. The OSCE plays a vital role in raising awareness, building confidence and developing capacity. Its regional cyber Confidence Building Measures (CBMs), launched between 2013 and 2016, include joint training and exercises in the Western Balkans[40]. Some WB6 governments now contribute at the UN, but coordination between diplomats and technical experts remains difficult.

Serbia has tackled organisational hurdles by creating a cyberdiplomacy unit and a broad consultative process, with support from the Netherlands, OSCE and the EU. Montenegro joined the European Cybersecurity Organisation (ECSO) to boost collaboration and resilience.[41] Albania is forming a cyberdiplomacy unit and directory for international projects. In September 2022, Albania, a NATO country, cut diplomatic ties with Iran over the July cyberattack. This move marked the effort to establish international norms for behav-

iour in cyberspace.[42] While most of the Western Balkan states aspire to EU and NATO membership, the region still lacks a unified positions at the UN.[43] While there are aspirations to join the EU and participate in collective defence as NATO members, the region has no common position at the UN.

· ***From Cyberdefence to Deterrence by Punishment***

Malicious cyber activities targeting critical infrastructure and government services are continuously increasing, with the region experiencing state-sponsored attacks (notably from Iran and Russia). These cyberattacks often result from information system failures.[44] Because of this, coordination across institutions to address threats and develop robust information security is mandatory.[45] In that vein, the EU's €5 m Western Balkans IPA III project seeks to boost cybersecurity prevention, preparedness and response through three main pillars[46]:

- Cybersecurity governance and awareness

- Legal framework, cybernorms, and international law

- Risk and crisis management

Most WB6 states are aligning with international conventions like Budapest (except Kosovo).[47] North Macedonia leads in legal and cooperative domains; Albania and Montenegro show some progress, but Bosnia and Herzegovina lags. Kosovo is making legislative improvements. While challenges remain, adopting cyber sanctions and aligning conventions shows the WB6's determination to hold attackers accountable and present a unified voice.[48]

In conclusion, the cyberposture of the region underscores the critical need for a unified framework that harmonises and interprets the authoritative guidance, regulations and standards, ensuring private and public sectors in the WB6 can properly manage and oversee their cyberrisks. As countries embrace an adaptive governance model to promote active engagement across all sectors and organisational levels, at the same time this governance practice requires alignment with risk management framework.

Ultimately, bridging this gap requires explaining how knowledge impacts the maturity of cybercapabilities and how this maturity can interfere in the five phases of NIST CSF 2.0 by also adopting the EU NIS2. While NIS2 sets the legal bar in the EU, NIST CSF 2.0 provides a best-practice framework for managing risks in the U.S. and globally. Figure 1 translates WB6 cyberposture buildup into their model of cyberresilience, which integrates NIS2 and NIST CSF2.0 through learning processes. These processes, generated from the adaptive governance capabilities, feed into the 6 operations of the NIST CSF 2.0 and NIS2 in : protect, detect, respond, recover, identify and govern. The GOVERN function wraps around both frameworks by addressing whose cybersecurity is connected to strategy.

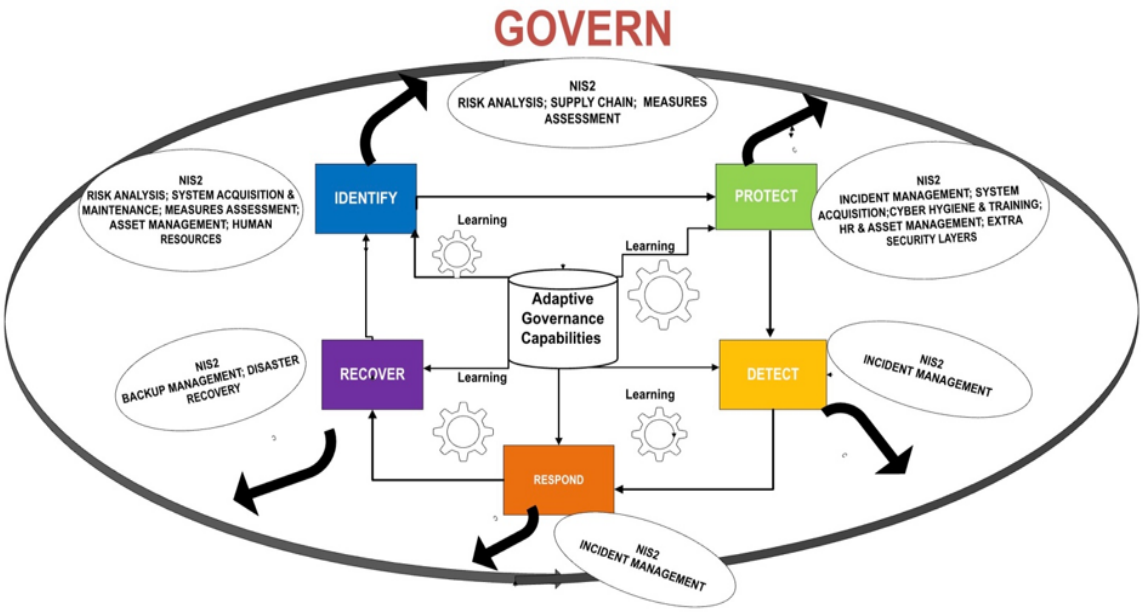

Figure 1- WB6 model for cyberresilience through learning processes, NIST 2.0 and EU NIS2 - *Source: Pengili 2026*

Conclusions

This analysis explored how the Western Balkans countries engage in adaptive governance to achieve resilience by unified standards, shared best practices and coordinated regional action. At domestic level, WB6 pursue cyber security through regulations. Collectively, they build capabilities to solidify their cyberposture. Such efforts are shaped by organisations like the EU, NATO, the UN, the OSCE, and the Berlin Process. The WB6 Cyber Resilience Framework introduced in this analysis seeks to encapsulate the existing processes, context and requirements disclosed in the regional cyberposture buildup. This model seeks also to guide cyberrisk management phases, enabling decision-makers to evolve their security strategies to thrive in the digital age. The analysis highlights the need for more research into regional cybergovernance by exploring the adaptive capacity, integrating the knowledge systems and process by which governance learns, and stakeholders' influence on cybercapabilities through networks and cross-sector cooperation.

References

1. Stiftung Wissenschaft und Politik. 2026. European Repository of Cyber Incidents (EuRepoC)
2 Ibid 1
3 BDEMERSON. 2026. Cybercrime Statistics 2026: Cost, Threats & Trends
4 Kosovar Centre for Security Studies . 2024 Integration of the Six Countries of the Western Balkans (WB6) in the European Union Agency for Cybersecurity.
5 Niinistö, S. (2024). Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness-. Brussels: European Commission; Also, Draghi, M. (2024). The future of European competitiveness Part A | A competitiveness strategy for Europe. Brussels: European Commission
6 Statista 2026, Digital security services market revenue in the Western Balkans from 2016 to 2030, by selected country
7 Blueprint Energy Solutions GmbH. 2019. Final Report - Study on cyber security in the energy sector of the Energy Community. Final Report, Vienna: Blueprint Energy Solutions GmbH.
8 Stiftung Neue Verantwortung. 2023. A Platform for Sustainable Cybersecurity Cooperation in the Western Balkans. Regional Profile, SNV.p.8: OECD. 2024. "Western Balkans Competitiveness Outlook 2024: Regional Profile." Competitiveness and Private Sector Development.
9 Minović, Adriana, Adel Abusara, Eranda Begaj, Vladimir Erceg, Predrag Tasevski, Vladimir Radunović, and Franziska Klopfer. 2016. Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities. Research Report, Geneva: Diplo Foundation. P.5
10 Op cit 8
11 White Paper: Maija Nikkanen, Aleksi Räsänen, Sirkku Juhola, Adaptive governance of disaster preparedness? The case of regional networks in Finland,International Journal of Disaster Risk Reduction, Volume 108, 2024,
12 ITU. 2024. Global Cyber Index 2024. Country Profile, ITU; Ministero degli Affari Esteri e della Cooperazione, 2025 Serbia at the top of cybersecurity and with a booming market
13 Ibid note 12
14 Op cit 9, p.47
15 Douglas, Stephanie, and Gordon Haley. 2023. "Connecting Organizational Learning Strategies to Organizational Resilience." Development and Learning in Organizations 1-5. p.3
16 Zweibelson, Ben. 2023. Beyond the Pale Designing Military Decision-Making Anew. 1st. Alabama: Air University Press. P.38-39
17 UNDP. 2022. "Project Document: Strengthening Cybersecurity Capacities in Bosnia and Herzegovina." 4 July. Accessed May 2, 2025.
18 EGA. 2025. Cyber Balkans
19 Op cit 4
20 Barbero, Fabio, and Nils Berglund. 2021. "Cybersecurity Capacity Building and Donor Coordination in the Western Balkans." Regional Profile. p.5
21 Bechev, Dimitar. 2023. Energy in the Western Balkans
22 Global Cyber Security Capacity Centre. 2018a. "CYBERSECURITY CAPACITY REVIEW- Albania." Country Profile.
23 European Commission 2025 NIS2 Directive: new rules on cybersecurity of network and information systems.
24 Maravić, Dražen. 2021. "DCAF." Cybersecurity Policy Development and Capacity Building – Increasing regional cooperation in the Western Balkans.
25 Op cit 21
26 Ibid note 26
27 Saalman, Lora, Fei Su, and Lrisa Saveleva Dovgal. 2022. Cyber Posture Trends in China, Russia, the United States and the EU. Solna: SIPRI.
28 Cybilportal.org. 2024. Project- WB6-EU Cooperation for Improving Cybersecurity in the Western Balkans
29 Regional Cooperation Council. 2020. Compliance of Legal Framework in the Western Balkans Economies with the General Data Protection Regulation (GDPR) Requirements. Regional Profile, Sarajevo: European Commission.
30 Ivanišević, Bogdan. 2025. New cybersecurity law enters into force in Serbia
31 Autoriteti Kombetar per Sigurine Kibernetike. 2025. The National Cyber Security Strategy 2025–2030 and Action Plan are approved
32 Vexelon. 2026. NIS2 in North Macedonia: The Complete Guide for Essential and Important Entities (2026).

33 InteregGovernance Regione Puglia. 2026. Montenegro strengths national cybersecurity framework through institutional and legislative reforms.
34 The Geostrata 2024. Balkan Nations on Cyber Threats - Measures Needed for Information Security Deterrence.
35 Regional Cooperation Council 2024. The Data Protection Academy for Western Balkans and Eastern Partnership Region Starts in Brussels Today.
36 National Cyber Security Authority of Albania. 2024. "Meetings Summary." Global Cyber Policy Dialogues: Western Balkans. National Cyber Security Authority of Albania (NCSA); the Ministry of Foreign Affairs of the Netherlands; ORF America. 1-10.
37 Op cit 4
38 Op cit 37
39 Western Balkans Cyber Capability Centre. 2025. Western Balkans Cyber Capacity Centre (WB3C)'s Post.
40 OSCE 2013. Our mandate on cyber/ICT security
41 European Cyber Security Organisation. 2025. Montenegro Ministry of Public Administration joins ECSO.
42 Gil Baram, Cyber Diplomacy through Official Public Attribution: Paving the Way for Global Norms, International Studies Perspectives, Volume 26, Issue 4, November 2025, Pages 391–411
43 Op cit 37
44 Op cit 1
45 Op cit 35
46 Center for International Legal Cooperation. 2025. EU Support to Western Balkans Cybersecurity Capacity Building.
47 UN General Assembly. 2024. "Draft United Nations convention against cybercrime Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious "
48European Commission. 2020. "IPA II- MULTI-COUNTRY EU support to cybersecurity capacity building in the Western Balkans 2014-2020." Regional Profile.

Rédaction: Laurent Baechler et Aline Palige
Policy Paper / Note de recherche est publiée par le Centre international de formation européenne, association dont le siège est 81, rue de France, F-06000-Nice.
© CIFE 2026, tous droits réservés pour tous pays.
www.cife.eu

Financé par l'Union européenne. Les points de vue et avis exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne sauraient être tenues pour responsables.

Cofinancé par l'Union européenne