DCAF - Geneva Centre for Security Sector Governance

Young Faces Programme (2025-2026)

Policy Paper

"Cybersecurity Governance under Constraint: How NATO Member States Balance Norms, Law, and Capacity in Cyberspace – The Cases of Albania, Montenegro and North Macedonia"



Author: Aleksandar Vanchoski

March 2026

Contents

Executive summary

Cybersecurity governance in Albania, Montenegro, and North Macedonia reflects strong alignment with NATO and EU frameworks but remains constrained by limited national capacity. While external support, particularly from NATO, the European Union, and the OSCE has accelerated institutional development, it has also exposed structural gaps in workforce sustainability, coordination, and implementation. This paper argues that the central policy challenge lies not in strategy design but in execution under conditions of limited resources. It proposes a shift toward institution-centric capacity building, better sequencing of external assistance, and stronger regional cooperation. Sustainable cybersecurity governance will depend on embedding capabilities within national systems while leveraging regional mechanisms as cost-effective force multipliers.

Introduction

Cybersecurity governance in Albania, Montenegro, and North Macedonia has evolved at the intersection of two powerful dynamics: accelerated Euro-Atlantic integration and increasing exposure to complex cyber threats. As members of NATO and candidates or aspirants for membership in the European Union, these states operate within a dense framework of normative expectations that require high levels of resilience, interoperability, and institutional coordination. At the same time, their relatively small administrative systems face persistent constraints in terms of financial resources, technical expertise, and human capital.

This structural asymmetry defines the core policy problem addressed in this paper. While cybersecurity strategies across the three countries demonstrate a high degree of formal alignment with NATO and EU standards, including whole-of-government approaches, protection of critical infrastructure, and incident response coordination, implementation remains uneven and often dependent on external support. Assistance from actors such as the OSCE, NATO capacity-building instruments, and EU regulatory and financial mechanisms has been instrumental in accelerating reforms. However, the increasing volume and complexity of such support risks overwhelming limited national absorption capacity, leading to fragmented implementation and reliance on short-term, project-based solutions.

In this context, the paper advances a central analytical argument: the effectiveness of cybersecurity governance in small states is less determined by the availability of external assistance and more by the ability to translate such support into sustainable institutional capacity. This requires a shift from compliance-driven reforms toward implementation-focused governance, where priority is given to workforce stability, inter-agency coordination, and the institutionalization of operational practices.

Furthermore, the paper situates regional cooperation in the Western Balkans as an underutilized but strategically relevant layer of capacity building. While NATO and EU frameworks provide essential standards and resources, regional mechanisms offer opportunities for cost-effective collaboration, shared learning, and improved situational awareness among states facing similar constraints and threat environments.

By combining comparative analysis with a governance-oriented perspective, this paper aims to move beyond descriptive assessments and contribute to a more operational understanding of how small states can strengthen cybersecurity resilience in practice. The subsequent chapters examine national frameworks, external capacity-building instruments, and regional cooperation dynamics, culminating in policy recommendations focused on feasibility, sequencing, and long-term sustainability.

Chapter I: Contextualizing Cybersecurity Governance in Albania, Montenegro, and North Macedonia

The cybersecurity governance frameworks of Albania, Montenegro, and North Macedonia have developed within a shared structural context characterized by small-state constraints, accelerated Euro-Atlantic integration, and increasing exposure to complex cyber threats. As NATO members - Albania since 2009, Montenegro since 2017, and North Macedonia since 2020, these countries have formally committed to collective cyber defence principles while simultaneously undergoing domestic institutional consolidation as well as continued EU accession processes. This dual trajectory places significant demands on national administrations that often lack the financial, technical, and human resources required to independently sustain comprehensive cybersecurity governance.

Across all three cases, cybersecurity has been elevated from a technical concern to a matter of national and collective security. NATO's recognition of cyberspace as an operational domain in 2016 fundamentally altered expectations for Allied preparedness, resilience, and interoperability. For smaller Allies, this shift has translated into expanded obligations related to critical infrastructure protection, incident response, information sharing, and participation in collective exercises and threat intelligence mechanisms. Yet, as multiple policy assessments by NATO, the EU, and the OSCE underline, these responsibilities often outpace national capacity, creating a persistent tension between normative alignment and practical implementation.

Albania's cybersecurity governance has evolved rapidly over the past decade, particularly following a series of high-profile cyber incidents that exposed systemic vulnerabilities in public administration and critical services. The National Cyber Security Strategy 2025-2030 (National Cyber Security Authority (AKSK), 2025) identifies cyber threats as a key national security risk and emphasizes state resilience, protection of critical information infrastructure, and international cooperation. Institutional responsibility is centralized under the National Cyber Security Authority (AKSK), which functions as both a regulatory and operational body. While this centralized model allows for relatively clear lines of authority, it also concentrates responsibility within a limited pool of specialized personnel, reinforcing dependency on external technical assistance and training.

Montenegro's cybersecurity framework reflects a more incremental institutional development path. The Cyber Security Strategy 2022-2026 (Ministry of Public Administration, 2021) emphasizes alignment with NATO standards and EU acquis, particularly in the areas of critical infrastructure protection and incident response coordination. The Directorate for Information Security within the Ministry of Public Administration plays a coordinating role, while the national Computer Emergency Response Team (CERT) handles operational incidents. Policy analyses supported by the EU and the OSCE consistently note that Montenegro's small administrative base limits its ability to maintain sector-specific cyber expertise, especially in energy, transport, and telecommunications, sectors explicitly prioritized in NATO resilience planning.

North Macedonia presents a hybrid model shaped by intensive reform efforts linked to both NATO accession and EU candidacy. The National Cyber Security Strategy 2022-2026 (Ministry of digital transformation, 2025) outlines an ambitious agenda focused on governance

coordination, public–private partnerships, and workforce development. The establishment of the National Cyber Security Council and the strengthening of the national CERT represent important institutional milestones. However, EU-supported assessments highlight persistent fragmentation across ministries and agencies, as well as limited budgetary allocations for cybersecurity relative to the scope of strategic objectives. As a result, implementation remains uneven despite strong political commitment.

Although all three countries formally recognize similar categories of cyber threats including state-sponsored attacks, cybercrime, hybrid operations, and threats to critical infrastructure, their threat perceptions are shaped by differing national experiences (Republic of Albania 2022; Government of Montenegro 2022; Government of North Macedonia 2022). Albania's recent exposure to politically motivated cyber operations has reinforced a security-centric framing of cyberspace, with strong emphasis on deterrence, attribution, and international solidarity (Republic of Albania 2022; European Commission 2023). Montenegro and North Macedonia, while also acknowledging state-based threats, tend to emphasize cybercrime and systemic vulnerabilities associated with digitalization and public sector reform (Government of Montenegro 2022; Government of North Macedonia 2022).

From a comparative perspective, NATO and EU analyses suggest that threat perception convergence among smaller Allies is driven less by domestic intelligence capacity and more by shared situational awareness mechanisms within NATO and regional information-sharing platforms (NATO 2022; ENISA 2022). This reliance on externally generated threat assessments underscores a broader governance challenge: while collective frameworks enhance awareness, they may also mask national blind spots and inhibit the development of autonomous analytical capabilities (NATO Parliamentary Assembly 2021).

NATO's cyber defence policy establishes cyber defence as part of the Alliance's core task of collective defence, requiring Allies to ensure the resilience of national networks and contribute to shared security (NATO 2021). Policy documents emphasize that cyber effects can, in certain circumstances, trigger Article 5, thereby integrating national cyber capabilities into the collective deterrence posture (NATO 2016). For Albania, Montenegro, and North Macedonia, this translates into obligations to protect national critical infrastructure, ensure secure military communications, and participate in NATO-led cyber exercises such as Cyber Coalition (NATO 2022).

However, NATO assessments also recognize the asymmetric burden placed on smaller Allies. While normative expectations are uniform, resource endowments are not (NATO Parliamentary Assembly 2021). Albania, Montenegro, and North Macedonia therefore rely heavily on NATO's cyber defence assistance mechanisms, including advisory support, training, and access to the Cooperative Cyber Defence Centre of Excellence (CCDCOE). Participation in these mechanisms enhances interoperability but does not fully compensate for limited domestic capacity, particularly in areas such as advanced threat detection, forensic analysis, and sustained workforce development (NATO 2021; CCDCOE 2022).

A comparative analysis of national cyber strategies reveals a high degree of formal alignment with NATO principles, including whole-of-government approaches, civil-military cooperation, and an emphasis on resilience. Yet implementation benchmarks frequently remain aspirational. Budgetary data from national policy documents indicate that cybersecurity funding represents a marginal share of overall defence and public administration expenditures, while staffing levels within national CERTs and coordinating bodies remain low, with high turnover driven

by competition from the private sector and international organizations (European Commission 2023; OSCE 2023).

This gap between formal commitments and operational capacity is particularly visible in the protection of critical infrastructure. NATO resilience requirements place increasing emphasis on sectors such as energy, transport, health, and digital communications (NATO 2022). While all three countries have adopted legal frameworks identifying critical infrastructure, OSCE-supported evaluations point to limited sector-specific risk assessments and insufficient testing through exercises (OSCE 2021; OSCE 2023). Consequently, resilience often depends on external support and ad hoc cooperation rather than institutionalized national capability.

The central policy issue emerging from this comparative context is the tension between expanding cyber responsibilities as NATO members and the limited ability of small states to meet these obligations independently. As NATO continues to integrate cyberspace into operational planning and deterrence, expectations for national preparedness increase correspondingly (NATO 2021). Yet Albania, Montenegro, and North Macedonia face structural constraints related to scale, fiscal capacity, and human capital that cannot be rapidly overcome (European Commission 2023).

This tension is not merely technical but governance-related. Dependence on external assistance risks creating fragmented accountability and short-term, project-based capacity building rather than sustainable institutional development (Hathaway et al. 2018). At the same time, insufficient national capacity may undermine the credibility of collective defence commitments in cyberspace. NATO, the EU, and the OSCE have increasingly acknowledged this dilemma, emphasizing tailored assistance and capacity-building strategies that account for national constraints while reinforcing collective standards (NATO 2022; OSCE 2023; European Commission 2023).

The cybersecurity governance landscape in Albania, Montenegro, and North Macedonia is therefore defined by convergence at the level of norms and divergence at the level of capacity. Their experiences illustrate the broader challenges faced by smaller NATO Allies navigating the demands of collective cyber defence within constrained national environments (NATO Parliamentary Assembly 2021). This baseline context provides the foundation for analyzing, in subsequent chapters, the role of NATO and EU capacity-building instruments and the potential of regional cooperation to mitigate these structural limitations.

Chapter II: NATO and EU Cybersecurity Capacity-Building Instruments

As NATO and the European Union have become the primary providers of strategic guidance, operational assistance, and funding in the cyber domain, their instruments increasingly define both the pace and direction of reform in smaller Allied and partner states. For policy-makers, the central question is no longer whether external support is necessary, but how such support can be structured to produce durable national capabilities rather than procedural compliance or long-term reliance on external actors.

Furthermore, from a policy perspective, NATO and EU cybersecurity assistance operates at the intersection of collective security imperatives and national capacity constraints. On the one hand, these frameworks aim to enhance interoperability, situational awareness, and collective resilience against increasingly sophisticated cyber threats. On the other hand, they risk overburdening limited administrative systems through complex reporting requirements, parallel standards, and overlapping reform agendas. This chapter therefore evaluates NATO and EU capacity-building instruments not only in terms of their technical contribution, but also through their impact on institutional sustainability, absorptive capacity, and national ownership in Albania, Montenegro, and North Macedonia.NATO cyber defence assistance provides the primary operational and normative framework through which Albania, Montenegro, and North Macedonia translate Alliance-level commitments into national practice. Rather than imposing uniform capability benchmarks, NATO has increasingly relied on modular assistance tools, training, exercises, advisory missions, and centres of excellence, to accommodate disparities in national capacity (NATO, 2021). For smaller Allies, these instruments function as capability multipliers, allowing limited national teams to access advanced expertise, shared threat assessments, and standardized operational procedures without replicating costly infrastructure domestically.

A central pillar of this approach is engagement with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which serves as a hub for doctrinal development, legal analysis, training, and large-scale exercises. Participation in CCDCOE activities enables Albania, Montenegro, and North Macedonia to embed their national cyber professionals within Alliance-wide epistemic and operational communities, thereby enhancing interoperability while mitigating the constraints posed by small domestic cyber workforces.

Engagement with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn constitutes a core pillar of this support. All three countries participate in CCDCOE-led training, research, and policy development activities, which provide access to advanced expertise that would be difficult to sustain nationally. CCDCOE courses on cyber operations, cyber law, and strategic decision-making have been particularly relevant for developing small cohorts of specialized personnel within defence ministries and national cyber authorities (CCDCOE, 2022).

Participation in the annual Locked Shields exercise, widely regarded as the world's most complex live-fire cyber defence exercise, has become a key mechanism for enhancing operational readiness and interoperability. Albania, Montenegro, and North Macedonia have each contributed national teams or integrated experts into multinational teams, testing their ability to respond to large-scale cyber incidents under realistic conditions. Evaluations from

recent exercises indicate measurable improvements in incident response coordination, strategic communication, and legal decision-making, particularly in hybrid scenarios involving both civilian and military networks (NATO CCDCOE, 2023).

However, the benefits of CCDCOE engagement also reveal structural constraints. National participation often depends on a very limited pool of experts, meaning that the same individuals are repeatedly deployed for training, exercises, and international meetings. While this ensures continuity, it also creates risks of burnout and institutional dependency on a small number of specialists. As several NATO policy assessments note, smaller Allies face a persistent challenge in translating individual-level training into broader institutional resilience (NATO Parliamentary Assembly, 2021).

Beyond CCDCOE activities, NATO-led multinational cyber exercises such as Cyber Coalition and Crossed Swords provide additional platforms for capacity building. These exercises emphasize interoperability, information sharing, and coordination between civilian and military authorities areas identified as systemic weaknesses in all three countries' national cyber governance frameworks.

Empirical data from NATO after-action reports suggest that repeated participation in such exercises correlates with improved national procedures for incident reporting and crisis management (NATO, 2022). For North Macedonia, for example, lessons learned from Cyber Coalition exercises have informed updates to national incident response protocols and inter-agency coordination mechanisms. Montenegro has similarly integrated exercise-derived best practices into its defence sector cyber policies, while Albania has used exercise participation to justify increased investment in national cyber defence units.

Nevertheless, the absorption of exercise outcomes remains uneven. Limited staffing and high turnover in public administration often hinder systematic follow-up, reducing the long-term institutional impact of these activities. This underscores a recurring policy dilemma: while NATO exercises enhance short-term readiness, their sustainability depends on domestic administrative capacity to institutionalize lessons learned.

Parallel to NATO support, the European Union plays a critical role in shaping cybersecurity governance in Albania, Montenegro, and North Macedonia, particularly through regulatory alignment and financial assistance. The EU's NIS2 Directive establishes a comprehensive framework for network and information security, significantly expanding the scope of covered entities and imposing stricter supervisory and reporting obligations (European Union, 2022).

For candidate and potential candidate countries, alignment with NIS2 serves both as a technical reform process and a political signal of readiness for deeper integration into the EU's digital single market. National policy documents in all three countries explicitly reference NIS2 as a benchmark for updating cybersecurity legislation and institutional mandates. IPA funding has been instrumental in supporting this process, financing legislative drafting, institutional strengthening, and technical upgrades for national CSIRTs.

Participation in EU Cyber Rapid Response Teams (CRRTs) further complements these efforts by providing access to deployable expertise during significant cyber incidents. Although participation levels vary, engagement with CRRT-related initiatives has enhanced situational awareness and cross-border cooperation, particularly for North Macedonia, which has leveraged EU-supported exercises to test crisis response mechanisms in civilian sectors.

Yet, EU-driven reforms also introduce new administrative burdens. NIS2 compliance requires expanded supervisory capacity, регуляр reporting mechanisms, and sustained engagement with a large number of public and private stakeholders. Policy analyses supported by the OSCE and the EU caution that without phased implementation and targeted capacity support, smaller administrations risk formal compliance without effective enforcement (OSCE, 2023).

The combined impact of NATO and EU cybersecurity instruments has undeniably strengthened national resilience in Albania, Montenegro, and North Macedonia. Training, exercises, regulatory alignment, and financial assistance have filled critical capability gaps and accelerated institutional development. However, evidence from national evaluations and international assessments consistently points to a central challenge: external assistance can overwhelm limited human and administrative capacities if not carefully sequenced.

A comparative assessment reveals that the most effective interventions are those that prioritize sustainability over volume. Programs that focus on training trainers, institutionalizing standard operating procedures, and supporting inter-agency coordination have produced more durable outcomes than one-off technical deliveries. This aligns with broader findings in cybersecurity capacity-building literature, which emphasize local ownership and gradual scaling as key determinants of success (Hathaway et al., 2018).

In this context, the policy question is not whether NATO and EU support is beneficial, but how it can be optimized. For Albania, Montenegro, and North Macedonia, strengthening national resilience requires a shift from parallel assistance streams toward more integrated planning that accounts for domestic absorption capacity. Without such calibration, the risk remains that external support, while well-intentioned may reinforce structural dependency rather than fostering autonomous and sustainable cybersecurity governance.

Chapter III: Regional Cooperation and Information-Sharing Constraints

Beyond NATO- and EU-led instruments, regional cooperation in the Western Balkans represents an additional, and potentially cost-effective, layer of cybersecurity capacity building for Albania, Montenegro, and North Macedonia. Regional cooperation is particularly relevant for smaller NATO member states whose national cyber ecosystems remain constrained by limited human capital, modest budgets, and fragmented institutional responsibilities. In such contexts, cooperation with geographically proximate states facing similar threat environments and governance challenges can function as a force multiplier, enabling shared learning, pooled expertise, and enhanced situational awareness (OSCE, 2021).

The Western Balkans share several structural characteristics that shape the rationale for regional cyber cooperation. These include high interconnectivity of critical infrastructure systems, overlapping telecommunications providers, shared energy and transport corridors, and common exposure to transnational cyber threats such as ransomware campaigns, disinformation operations, and attacks on public-sector digital services. As ENISA has observed, cyber incidents in smaller and highly interconnected states often have spillover effects that transcend national borders, particularly where incident response capacities are uneven (ENISA, 2022). For Albania, Montenegro, and North Macedonia, this interdependence creates both a vulnerability and an opportunity: while cyber incidents can propagate quickly across borders, coordinated regional responses can also mitigate their impact more efficiently than isolated national actions.

Several regional initiatives provide an embryonic framework for cybersecurity cooperation in the Western Balkans. Although not exclusively focused on NATO members, these mechanisms include Albania, Montenegro, and North Macedonia and offer platforms for information exchange, confidence building, and capacity development.

One of the most relevant frameworks is the OSCE's confidence-building measures (CBMs) in cyberspace, which have been implemented in South-Eastern Europe through regional workshops, tabletop exercises, and information-sharing initiatives. OSCE-supported activities have focused on enhancing transparency regarding national cyber policies, promoting points of contact for incident response, and fostering dialogue between civilian and military cyber stakeholders (OSCE, 2020). For smaller NATO allies, these measures are particularly valuable in reducing uncertainty and building trust among neighboring states, which is a prerequisite for timely information sharing during cross-border cyber incidents.

Another important platform is the Regional Cooperation Council (RCC), which has increasingly incorporated cybersecurity and digital resilience into its agenda under the South East Europe 2030 Strategy. Through initiatives on digital transformation and secure connectivity, the RCC has facilitated policy dialogue among Western Balkan governments, including on cyber incident response coordination and public-private partnerships (RCC,

2022). While these initiatives remain largely policy-oriented rather than operational, they provide a forum for aligning national priorities and identifying common capacity gaps.

Operationally oriented cooperation has also emerged through Computer Security Incident Response Team (CSIRT) networks. Albania, Montenegro, and North Macedonia all participate in regional CSIRT meetings supported by the EU, OSCE, DCAF and donor-funded projects, which aim to improve technical coordination and peer-to-peer exchange. These networks enable practitioners to share indicators of compromise, lessons learned from incidents, and best practices in incident handling. According to EU-funded project evaluations, CSIRT-to-CSIRT cooperation in the Western Balkans has contributed to faster detection and containment of cyber incidents, particularly in the public sector (EU IPA Evaluation Report, 2021).

Confidence-building arrangements are a critical but often underestimated component of regional cybersecurity cooperation. In the Western Balkans, historical legacies of political tension and mutual distrust have traditionally limited the depth of security cooperation. In the cyber domain, these challenges are compounded by concerns over data sensitivity, attribution, and reputational risk. As a result, information sharing tends to be ad hoc, informal, and highly dependent on personal relationships between practitioners rather than institutionalized protocols (NATO StratCom COE, 2021).

Nevertheless, incremental progress has been observed. Regional cyber exercises supported by OSCE and EU instruments have incorporated cross-border incident scenarios, requiring participating states to exchange information and coordinate responses in simulated environments. These exercises serve not only technical training purposes but also confidence-building functions, as they familiarize institutions with each other's procedures and communication channels. Empirical assessments suggest that repeated participation in such exercises increases willingness to share information during real incidents, even in the absence of formal agreements (OSCE, 2022).

For Albania, Montenegro, and North Macedonia, confidence-building is particularly relevant given their dual positioning as NATO members and Western Balkan neighbours. While NATO provides secure channels for information exchange among Allies, many cyber incidents affecting these countries originate or propagate through regional networks that include non-NATO states. Regional confidence-building mechanisms can therefore complement NATO frameworks by enabling engagement with a broader set of actors without undermining Alliance obligations.

Despite its potential, regional cybersecurity cooperation in the Western Balkans remains underutilized and constrained by several structural limitations. One major challenge is uneven technical maturity among national cyber institutions. While Albania, Montenegro, and North Macedonia have made progress in establishing national CSIRTs and legal frameworks, significant disparities persist in staffing levels, analytical capabilities, and access to advanced threat intelligence tools. These asymmetries complicate cooperation, as more advanced partners may be reluctant to share sensitive information with counterparts perceived as less capable of safeguarding it (ENISA, 2021).

Legal and regulatory incompatibilities further limit effective cooperation. Differences in data protection regimes, incident reporting thresholds, and classification rules create uncertainty about what information can be shared, with whom, and under what conditions. Even among NATO members, national interpretations of confidentiality and national security exemptions

vary significantly. In the Western Balkans context, this problem is exacerbated by the coexistence of EU-aligned legal frameworks and transitional regulatory systems, particularly for states still harmonizing their legislation with the EU acquis (European Commission, 2023).

Trust deficits represent another persistent obstacle. While political relations among Albania, Montenegro, and North Macedonia are generally cooperative, regional cybersecurity cooperation remains vulnerable to broader geopolitical dynamics and domestic political changes. Stakeholder interviews conducted by OSCE projects indicate that concerns about misuse of shared information and lack of reciprocity continue to discourage systematic information exchange (OSCE, 2021). As a result, regional mechanisms often stop short of operational-level collaboration, remaining confined to dialogue and training activities.

Finally, the absence of standardized regional information-sharing protocols limits scalability. Unlike NATO's established procedures and secure platforms, regional cooperation relies heavily on project-based arrangements with limited sustainability. Once external funding ends, many cooperation mechanisms struggle to maintain momentum, reinforcing dependence on external actors rather than fostering durable regional ownership.

Regional cooperation should not be understood as an alternative to NATO and EU frameworks but as a complementary layer that enhances their effectiveness. For smaller NATO allies, regional mechanisms can address gaps that Alliance-level instruments are not designed to fill, particularly in relation to local context, language, and shared infrastructure. By facilitating early warning, peer learning, and informal coordination, regional cooperation can reduce the burden on national institutions and improve readiness to engage with NATO and EU mechanisms when incidents escalate.

Policy analyses by the EU and NATO increasingly emphasize the importance of regional approaches to cyber resilience, particularly in Europe's periphery (NATO, 2022; European Commission, 2023). However, translating this recognition into practice requires clearer articulation of how regional initiatives align with Alliance standards and EU requirements. Without such alignment, there is a risk of duplication, fragmentation, or initiative fatigue among already overstretched national administrations.

The underutilization of regional cooperation in cybersecurity reflects not a lack of relevance but a lack of strategic prioritization. For Albania, Montenegro, and North Macedonia, regional mechanisms remain secondary to NATO and EU engagements, often treated as optional or donor-driven activities rather than integral components of national cyber strategies. This hierarchy overlooks the potential of regional cooperation as a cost-effective means of capacity building, particularly for functions such as training, situational awareness, and incident coordination.

From a policy perspective, greater investment in regional cooperation could yield disproportionate benefits. Shared training programs, joint exercises, and standardized information-sharing arrangements can reduce duplication of effort and alleviate human resource constraints. Moreover, stronger regional networks can enhance trust and interoperability, enabling smaller NATO allies to engage more confidently within Alliance and EU frameworks.

Recommendations

Based on these findings, the following policy-oriented recommendations are proposed, with a focus on feasibility, sustainability, and implementability for Albania, Montenegro, and North Macedonia.

1. Prioritize institutional sustainability over breadth of reforms

National authorities in Albania, Montenegro, and North Macedonia in coordination with NATO and EU partners, should focus on consolidating core cybersecurity institutions rather than continuously expanding mandates. This includes stabilizing staffing within national CERTs and coordinating bodies, investing in mid-level managerial capacity, and embedding standard operating procedures across government. NATO and EU partners should support this shift by favoring fewer, longer-term interventions aimed at institutionalization rather than short-term technical deliveries.

- ***Objective:*** *Shift from expansion to consolidation of the core cybersecurity institutions*
  (Timeframe: 0-24 months)

- **Implementation steps:**

  - Conduct a **national institutional audit** (*0-3 months*) to identify overlaps and critical capacity gaps in CERTs and coordinating bodies.
  - Introduce **multi-year staffing plans** with protected budget lines (*3-9 months*).
  - Develop and adopt **standard operating procedures (SOPs)** across ministries (6-12 months).
  - Establish **inter-agency coordination units** with clear mandates (*within 12 months*).

- ***What's next:***

  Align future NATO and European Union assistance with these institutional priorities to avoid duplication and fragmentation.

2. Shift from individual-centric to institution-centric capacity building.

While advanced training through CCDCOE and multinational exercises remains indispensable, greater emphasis should be placed on translating individual expertise into organizational resilience. This includes formal knowledge-transfer mechanisms, internal training programs, and retention strategies for cyber professionals within public institutions. Without such measures, gains achieved through international engagement risk remaining person-dependent and fragile.

- ***Objective:*** *Institutionalize Knowledge Transfer from Training*

(Timeframe: 0-18 months)

- **Implementation steps:**

  - Require **post-training debriefs and internal workshops** after each international engagement *(immediate*).
  - Develop **"Train-the-Trainer" (ToT) programmes** within national institutions (*3-12 months*).
  - Create **centralized knowledge repositories** for lessons learned (*within 9 months*).

❖ ***What's next:***

Tie participation in international exercises (e.g., CCDCOE activities) to mandatory institutional follow-up actions.

3. Invest in workforce retention and career pathways

Human capital remains the most critical vulnerability across all three cases. Governments should prioritize competitive remuneration, clear career progression, and continuous professional development for cybersecurity professionals in the public sector. Targeted incentives, such as bonded training schemes or regional secondments, could help mitigate turnover while maximizing the return on investment from NATO and EU-funded training.

- **Objective:** Reduce turnover and dependency on small expert pools.
  (Timeframe: 0-36 months)

- **Implementation steps:**
  - Introduce **competitive salary supplements or retention bonuses** (*6–12 months*).
  - Develop **clear career pathways** for cybersecurity roles in public administration (*12-24 months*).
  - Pilot **bonded training schemes** (state-funded training with minimum service obligations) (*12-24 months*).
  - Establish **regional secondment programmes** across Western Balkan institutions. (*36 months*)

❖ ***What's next:***

Coordinate with donors to ensure training investments include retention conditionalities.

4. Systematize the implementation of lessons from exercises and training

Participation in NATO and EU cyber exercises should be systematically linked to national follow-up mechanisms. After-action reviews, updated protocols, and inter-agency drills at the national level can help translate individual learning into organizational resilience. Assigning clear responsibility for implementation within ministries and agencies would reduce the risk that lessons identified at the international level dissipate domestically.

- **Objective:** Ensure lessons from exercises translate into operational improvements. ***(Timeframe: 0-12 months)***

- **Implementation steps:**
  - Mandate **after-action reports *within 30 days*** of each exercise.
  - Assign **implementation leads** in each institution (*within 3-6 months*).
  - Conduct **national simulation exercises** based on identified gaps (*within 6-12 months*).

❖ ***What's next:***

Integrate exercise outcomes into national cybersecurity strategies and annual planning cycles.

5. Establish Regional Information-Sharing Protocols

Building on existing CSIRT networks and OSCE-supported confidence-building measures, the three countries should pursue standardized regional protocols for information sharing on cyber incidents, including clear rules on classification, data protection, and reciprocity. Even limited-scope agreements focused on technical indicators and early warning could significantly improve situational awareness without raising sensitive political concerns.

- **Objective:** Move from ad hoc to structured regional cooperation. ***(Timeframe: 0-24 months)***

- **Implementation steps:**
  - Develop **minimum regional agreements** on sharing technical indicators (e.g., malware signatures) (*6-12 months*).
  - Harmonize **data classification and confidentiality rules** (*12-24 months*).
  - Create **secure communication channels** between national CSIRTs. (*12-24 months*)

❖ **What's next:**

Leverage platforms supported by the OSCE and RCC to **pilot regional early-warning systems**.

6. Sequence External Assistance with Absorptive Capacity

To prevent institutional overload and ensure sustainable impact, external cybersecurity assistance should be systematically aligned with national absorptive capacity rather than driven by the volume of available programmes.

- **Objective:** Avoid overload from overlapping NATO/EU initiatives.
  (Timeframe: Immediate-Ongoing)

- **Implementation steps:**
  - Establish a **national coordination mechanism for donor support** (*within 6 months*).
  - Introduce **absorption capacity assessments** before accepting new projects. (*within 6 months*).
  - Prioritize **fewer, longer-term programmes** over multiple short-term interventions. *(immediate*).

❖ **What's next:**

Develop a **joint NATO-EU coordination roadmap** tailored to each country's capacity level.

Conclusions

This policy paper has examined cybersecurity governance in Albania, Montenegro, and North Macedonia through three interlinked lenses: national capacity constraints, the role of NATO and EU capacity-building instruments, and the underutilized potential of regional cooperation in the Western Balkans. Taken together, the analysis demonstrates a consistent pattern of normative convergence alongside persistent operational divergence. All three countries have made significant progress in aligning their legal frameworks, strategic documents, and institutional arrangements with NATO and EU standards. Cybersecurity is now firmly embedded within national security agendas, and political commitment to collective cyber defence is evident across all three cases.

At the same time, this convergence masks enduring structural limitations. Small administrative systems, limited fiscal space, and chronic shortages of specialized cyber professionals continue to constrain implementation. NATO and EU assistance has played a decisive role in mitigating these gaps by providing access to training, exercises, expertise, and funding that would be unattainable domestically. Engagement with mechanisms such as the NATO Cooperative Cyber Defence Centre of Excellence, multinational cyber exercises, NIS2 alignment processes, and EU-funded capacity-building projects has enhanced interoperability, situational awareness, and crisis response readiness.

The findings also highlight that external assistance, while indispensable, cannot substitute for sustainable national institutions. Capacity building that remains project-based or overly reliant on a small number of trained individuals generates short-term gains but limited resilience. This dynamic is particularly evident in national CERTs and coordinating bodies, where staffing shortages, high turnover, and insufficient career incentives undermine continuity and institutional memory. As a result, progress in cybersecurity governance remains uneven and vulnerable to political or personnel changes.

Regional cooperation emerges as a complementary but underdeveloped response to this challenge. Existing Western Balkan mechanisms demonstrate clear potential to function as cost-effective force multipliers by pooling expertise, enhancing early warning, and building trust among neighbouring states facing similar threat environments. Yet regional cooperation remains fragmented, project-based, and politically secondary to NATO and EU engagement. Trust deficits, uneven technical maturity, legal incompatibilities, and the absence of standardized information-sharing protocols continue to limit its operational impact. As a result, an opportunity to strengthen national and collective resilience at relatively low cost remains largely untapped.

Overall, the experience of Albania, Montenegro, and North Macedonia illustrates a broader structural issue within collective cyber defence: uniform expectations applied to unequal capacities. Addressing this imbalance requires a shift from volume-driven assistance toward more selective, sequenced, and sustainability-oriented approaches that reinforce national ownership while leveraging regional and Alliance-level cooperation.

References

Albania – National Policy Documents

- Republic of Albania. 2022. National Cyber Security Strategy 2022–2025. Tirana: Council of Ministers of the Republic of Albania.

- Republic of Albania. 2024. National Cyber Security Strategy 2025–2030 (Draft/Adopted Version). Tirana: Council of Ministers of the Republic of Albania.

Montenegro – National Policy Documents

- Government of Montenegro. 2022. Cyber Security Strategy of Montenegro 2022–2026. Podgorica: Ministry of Public Administration.

North Macedonia – National Policy Documents

- Government of the Republic of North Macedonia. 2022. National Cyber Security Strategy of the Republic of North Macedonia 2022–2026. Skopje: Government of the Republic of North Macedonia.

NATO – Policy Documents and Assessments

- NATO. 2016. Warsaw Summit Communiqué. Brussels: North Atlantic Treaty Organization.

- NATO. 2021. Comprehensive Cyber Defence Policy. Brussels: North Atlantic Treaty Organization.

- NATO. 2022. Cyber Defence Pledge – Progress Report. Brussels: North Atlantic Treaty Organization.

- NATO Parliamentary Assembly. 2021. Cyber Defence in NATO: Building Resilience and Deterrence. Brussels: NATO PA.

- NATO Strategic Communications Centre of Excellence (StratCom COE). 2021. Hybrid Threats and Cyber Security in the Western Balkans. Riga: NATO StratCom COE.

NATO CCDCOE

- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2022. Annual Report 2022. Tallinn: CCDCOE.

- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2023. Locked Shields 2023: After Action Report. Tallinn: CCDCOE.

European Union – Legal and Policy Frameworks

- European Union. 2022. Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive). Brussels: European Union.

- European Commission. 2023. Cyber Resilience and Cybersecurity Capacity Building in the Western Balkans. Brussels: European Commission.

- European Union. 2021. Instrument for Pre-Accession Assistance (IPA III): Programming Framework. Brussels: European Union.

ENISA

- European Union Agency for Cybersecurity (ENISA). 2021. Cybersecurity Capacity Building in the Western Balkans. Athens: ENISA.

- European Union Agency for Cybersecurity (ENISA). 2022. Threat Landscape for the Western Balkans. Athens: ENISA.

OSCE

- Organization for Security and Co-operation in Europe (OSCE). 2020. Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of ICTs. Vienna: OSCE.

- Organization for Security and Co-operation in Europe (OSCE). 2021. Cyber/ICT Security Capacity Building in South-Eastern Europe. Vienna: OSCE.

- Organization for Security and Co-operation in Europe (OSCE). 2022. Regional Cybersecurity Exercises and Confidence Building: Lessons Learned. Vienna: OSCE.

- Organization for Security and Co-operation in Europe (OSCE). 2023. Cybersecurity Governance and Legal Harmonisation in the Western Balkans. Vienna: OSCE.

Regional Cooperation

- Regional Cooperation Council (RCC). 2022. South East Europe 2030 Strategy. Sarajevo: RCC.

EU-Funded Evaluations

- European Union. 2021. IPA Evaluation Report: Cybersecurity and CSIRT Cooperation in the Western Balkans. Brussels: European Union.

Academic Literature

- Hathaway, Melissa E., et al. 2018. Building a Sustainable Cybersecurity Ecosystem. Washington, DC: Global Cybersecurity Capacity Centre.