CONTEMPORARY CHALLENGES OF HYBRID THREATS TO NATO AND THE EUROPEAN UNION: ANALYSIS AND EXPERIENCES OF MONTENEGRO

DOI: https://doi.org/10.37458/nstf.27.1.6
Original scientific paper
Received: October 27, 2025
Accepted: March 15, 2026

Nenad Koprivica*

Abstract: This paper examines the structure, dynamics, and effects of hybrid threats, focusing on Montenegro's experience and positioning with respect to NATO and the European Union. Using a comparative and empirical framework, it analyses institutional vulnerabilities, the role of proxy actors, cyber-attacks, and regional resilience practices. The study draws on policy documents and reports from NATO, the EU, the

* Nenad Koprivica, PhD, is independent researcher at CEDEM (Center for Democracy and Human Rights) from Podgorica, Montenegro. Can be reached ate nenad.koprivica@cedem.me

UK FCDO, and local research centres, the Digital Forensic Centre (DFC) and the Centre for Democratic Transition (CDT), as well as comparative data from Serbia, Bosnia and Herzegovina, North Macedonia, and Albania. Through a case study of Montenegro, the paper maps key vectors of hybrid action: cyber-attacks targeting electoral processes and critical infrastructure, media-narrative campaigns aimed at delegitimising Euro-Atlantic integration, the operation of proxy actors linking domestic political and religious structures to external centres of influence, and economic and energy penetration that constrains institutional autonomy. A comparative regional analysis reveals shared patterns of sequential attack, whereby initial cyber incidents are amplified by subsequent disinformation campaigns, while highlighting differences in institutional resilience across the Western Balkans. The findings indicate that Montenegro's primary weaknesses lie in the fragmentation of its security sector, insufficient inter-institutional coordination, limited digital literacy, and a reactive rather than preventive approach to hybrid threats. The paper concludes with policy recommendations centred on the establishment of a national hybrid-threat monitoring centre, the introduction of digital and media literacy programmes, greater transparency in financing flows, and enhanced regional and international cooperation.

Keywords: hybrid threats, NATO, European Union, institutional resilience, Montenegro

Introduction

Contemporary hybrid threats represent one of the greatest challenges to Euro-Atlantic security, with a particular focus on the Western Balkan states that find themselves in the process of European integration while also standing at the crossroads of geostrategic interests. As a NATO member state (since 2017) and the most advanced EU accession candidate, Montenegro offers a compelling case for analysing the impact of Russian hybrid activities and for testing the resilience of small systems in the face of combined cyber, information, and economic aggression (DFC, 2023; CDT, 2024).

Numerous international, regional, and local actors engage with this issue through research, reports, and policy analyses. Among the most prominent are NATO and the EU, as well as certain initiatives within the Berlin Process (UK FCDO, October 2025). At the local level, in the Montenegrin context, the most significant contributions to analysing hybrid influences come from the DFC (Digital Forensic Centre) and CDT (Centre for Democratic Transition), through numerous case studies: from cyber-attacks during electoral processes and the exploitation of religious and economic structures, to sustained disinformation campaigns.

A considerable body of analysis and scholarship on hybrid action already exists (see: European Parliamentary Research Service, 2017; Atlantic Council of Montenegro, 2024). However, the motivation for investigating this topic stems not solely from theoretical interest but also from practical concerns: mapping the challenges vis-à-vis society's resilience to sophisticated external influences. The aim of this paper, therefore, is

to provide an analysis of hybrid threats in Montenegro from a case-study perspective, drawing on domestic and international sources, empirical evidence, regional comparisons, and the potential for institutional resilience.

What particularly drew my attention was the difference in perception among various actors: while international institutions tend to focus on systemic solutions, local decision-makers often underestimate the vertical and horizontal complexity of the threats. It was precisely this gap between policy and practice that prompted me, through this paper, to attempt to map the real challenges - relying on domestic empirical evidence, and to formulate recommendations. Experience has shown that the key problems are weak communication between security services and civil society, low digital literacy among citizens, and a sluggish institutional response to new models of attack.

The principal analytical contribution of this paper is the integration of empirical data and politico-security analysis, offering a specific insight into the dynamics, challenges, and response options for hybrid threats in Montenegro, together with a set of concrete measures to strengthen national resilience in line with international standards, centred on the most recent strategic documents, including the British recommendations from the Berlin Process (UK FCDO, 2025).

Theoretical and Conceptual Framework

Through my participation in numerous forums, I have become convinced of just how indispensable the concept of hybrid threats has become in contemporary security analysis. The notion of "hybrid action" is no longer

merely a segment of expert documents; it is a reality we confront through the coordinated use of political, economic, military, technological, and information tactics.

In contemporary international relations, the term encompasses the synchronised deployment of political, economic, military, technological, and information instruments aimed at destabilising targeted states or societies without a formal declaration of war or open military conflict (European Parliamentary Research Service, 2017; NATO Hybrid CoE, 2023). It emerged as a response to the transformation of Russian and Chinese security strategies, following the rapid expansion of cyber conflicts, disinformation, and hybrid action in the post-Soviet space, and particularly the crisis in Ukraine (Galeotti, 2014; Rácz, 2015).

According to the current definitions of NATO and the EU (NATO Hybrid CoE, 2023; European Parliamentary Research Service, 2017), hybrid threats manifest in four principal forms: cyber-attacks on state and private institutions; disinformation and cognitive operations involving reflexive control and the targeted dissemination of narratives through local media; economic and energy penetration through foreign investments and the financing of para-religious structures; and, finally, the deployment of proxy-actor networks - local politicians, NGOs, religious organisations, and radical groups (DFC, 2023; CDT, 2024).

The contemporary literature describes "vertical hybridity" as the exploitation of local divisions and weaknesses, most commonly through the use of proxy

actors and sophisticated information operations (e.g. through media, NGOs, and even church structures), whereby external actors, above all Russia, exploit existing internal divisions: ethnic, political, religious - thereby destabilising democratic institutions and slowing Euro-Atlantic integration (Atlantic Council of Montenegro, 2024; Vuković, 2022). In the Western Balkans in particular, hybrid threats transcend conventional security challenges and become a "normalised" instrument of foreign policy, exercised through regional media, church organisations, and political movements that function as proxy factors for broader geopolitical interests (DFC, 2023; UK FCDO, 2025).

The Gerasimov "non-linear doctrine" (the so-called "Gerasimov doctrine"), developed within Russian military theory, centres on the idea of a continuum between peace and war and on "the employment of all available national instruments of power, at every stage of strategic conflict, including information and psychological attacks, the creation of economic dependency, and the instrumentalization of cross-border institutions" (Galeotti, 2014; NATO Hybrid CoE, 2023).

This paper employs a broader analytical model that includes the identification and analysis of key institutional weaknesses, including questions of coordination, capacity, and procedures in the security sector. It also examines local-regional influence flows (the interference of Russian and Serbian structures) and provides an analytical framework that, through the case study of Montenegro, local-regional comparisons, and the author's own reflections, demonstrates how global

concepts of hybrid action manifest in the concrete context of the region.

Methodology

A combined methodological approach was applied in this research, grounded in analytical and comparative methods, with the integration of empirical data from domestic and international sources. I opted for a combined approach because the current challenges of hybrid action demand deeper interpretation: from reading and analysing official documents and reports of NATO, the EU, and regional partners, to integrating data from the expert analyses of the DFC and CDT, as well as specific news articles and communiqués from relevant institutions. The key foundation of the paper is the case study of Montenegro, selected on account of its specific geopolitical position, institutional evolution, and the intensity of hybrid operations over the past decade (DFC, 2023; CDT, 2024).

The following primary sources and methods were employed: analysis of policy documents and reports from relevant regional and international organisations (NATO, EU, Atlantic Council, UK FCDO); empirical data from Montenegro's Digital Forensic Centre (DFC), the Centre for Democratic Transition (CDT), local media, and reports of relevant institutions; comparative analyses of regional literature and examples from Serbia, Bosnia and Herzegovina, North Macedonia, and other Western Balkan states, alongside comparisons with Baltic and Eastern European cases (European Parliamentary Research Service, 2017; Atlantic Council of Montenegro, 2024). An indispensable component is also the quantitative data (statistics on cyber-attacks,

disinformation, investments, and political influences in the period 2016–2025), as well as tables and schematic representations of hybrid-action trends. Finally, a critical assessment of Montenegro's institutional responses and regional practices is offered.

The methodological framework enables detailed mapping of hybrid-action vectors and the identification of vulnerabilities, while also permitting a multi-layered analysis: from socio-political to digital and economic dimensions (Rácz, 2015; NATO Hybrid CoE, 2023). Each phase of the analysis required balancing between policy literature, quantitative findings, and comparative practice from states confronting the most pronounced incidents of a hybrid nature. Through the case-study approach, it was shown how global and regional strategies are reflected in Montenegro, influencing domestic policies, public discourse, and security reforms.

Such a methodological model, combining policy analysis, quantitative and qualitative data, and local expertise, enables the results of this paper to be integrated into the existing policy literature and to contribute to the further development of preventive and responsive measures in combating hybrid threats (UK FCDO, 2025).

Regional Context and International Framework

Regional practice demonstrates how hybrid threats manifest as a concrete problem shaping political and economic everyday life. Over the course of numerous regional conferences and workshops, exchanging experiences, we often arrive at the conclusion that the Western Balkans effectively functions as a kind of

"laboratory of hybridity" - where the combination of domestic institutional weaknesses, systemic fragmentation, and low digital literacy becomes fertile ground for sophisticated external influences (DFC, 2023). In recent years, the Western Balkans has been one of the most dynamic theatres for hybrid-threat operations, with strong influence from external actors, particularly Russia, on the political, economic, and information stability of the region (Atlantic Council of Montenegro, 2024; UK FCDO, 2025). Cases from Serbia, Bosnia and Herzegovina, North Macedonia, and Albania display common patterns, yet also differ in institutional resilience and capacity for strategic response. One of the main challenges is the lack of coordination between state and independent actors, coupled with a pronounced vulnerability to disinformation campaigns disseminated through local and regional media.

In Serbia, hybrid activities are predominantly carried out through media-psychological operations, supported by political and religious structures, polarising the public, which results in anti-EU and anti-NATO narratives (DFC, 2023; Vuković, 2022). In Bosnia and Herzegovina, systemic heterogeneity and the fragmentation of political and religious communities facilitate the spread of disinformation, cyber-attacks, and the operation of proxy factors at the local level (CDT, 2024). North Macedonia faces challenges in digital security, protection of the electoral system, and combating regional propaganda, which aligns with the broader trends of hybrid threats in the region (European Parliamentary Research Service, 2017). The noticeable rise in the number of cyber incidents linked to public administration in Albania is an additional indicator that

hybrid threats in the region cannot be viewed in isolation from the wider European context.

Recent initiatives within the Berlin Process, through the reports of the British FCDO (London, 2025), clearly articulate the need for a joint approach, support for the development of national capacities, enhanced regional cooperation, and a precise definition of national resilience policies.

The European context is shaped by NATO, EU, and leading security-institute documents and strategies that affirm the importance of preventive digital education, the development of public-private partnerships, and the creation of joint databases for monitoring hybrid activities (NATO Hybrid CoE, 2023; Atlantic Council of Montenegro, 2024).

Data from comparative reports show the extent to which the frequency of cyber-attacks has risen in the period 2016–2025, and how various structures have attempted to influence political and economic processes through sophisticated information campaigns and the transfer of funds via NGOs and other channels. Analysing the data in the table, it is clear that the most vulnerable areas are precisely those where politico-economic fragmentation is most pronounced: electoral processes, energy infrastructure, and identity issues, which further confirms the importance of a comparative and regional approach to hybrid threats.

Data compiled on the basis of annual DFC and CDT reports, adjusted for periods not covered by all sources; they should therefore be read as indicative rather than absolute values.

Table 1: Trends in Hybrid Threats in Western Balkan Countries (2016–2025)

Country	Cyber-attacks (2016–2025)	Principal proxy actors	Disinformation campaigns (annual average)	Most vulnerable areas
Montenegro	180+	SOC, local media, political parties	420+	Electoral process, economic and investment vulnerability, identity
Serbia	240+	SOC, political parties, media networks	500+	Media, political polarisation
Bosnia and Herzegovina	200+	Religious communities, political parties	350+	Local government, ethnic divisions
North Macedonia	100+	NGOs, political parties, regional media	150+	Elections, digital services
Albania	90+	Political parties, social networks, online media	80+	Public sector, cyber infrastructure

Sources: DFC, NATO Hybrid CoE, CDT, Atlantic Council of Montenegro, UK FCDO (2023 - 2025). Figures are based on aggregate DFC reports (2017–2023), CDT reports (2020–2024), and comparative NATO Hybrid CoE/UK FCDO documents.

Montenegro as a Case Study

Montenegro has been exposed to a high intensity of hybrid threats over the past decade, characteristic of transitional political systems in the region. Empirical data point to the dominance of several key vectors of influence:

Cyber Attacks and Electoral Processes

Montenegro's experience shows that the most intensive cyber-attacks almost invariably coincide with sensitive political moments, above all with electoral cycles and crisis situations within governing coalitions. On the day of the parliamentary elections of 16 October 2016, government portals (gov.me) and several key media websites became inaccessible due to a multi-hour DDoS attack. According to data from the Ministry of Public Administration, over 200 attacks on government institution websites were registered in 2016, compared with a mere six in 2012, a stark indicator of the dramatic growth and increasing sophistication of threats. The American cybersecurity firm FireEye identified that the group APT28 (also known as Fancy Bear), linked to Russian intelligence services, had targeted Montenegrin officials with infected Word documents in the period January-February 2017, using the so-called Dealers Choice exploit framework, in the period immediately preceding Montenegro's formal accession to NATO in June 2017.

The most devastating attack, however, occurred in August 2022. On the night between 19 and 20 August, shortly after the fall of Prime Minister Dritan Abazović's government, Montenegro suffered what the Minister of Public Administration, Maraš Dukaj, described as an "unprecedented" cyber-attack on critical state

infrastructure. The attack lasted for days and struck multiple sectors: transport systems, water supply, electricity distribution, online portals of state services, and even immigration systems, prompting the United States Embassy in Podgorica to issue a warning to its citizens. The state energy company EPCG switched to manual operations to avoid potential infrastructure damage. The National Security Agency (ANB) attributed responsibility to Russia, and the Minister of Defense, Raško Konjević, explicitly pointed to the Russian government as the most probable actor. Subsequently, the ransomware group Cuba claimed responsibility for the attack, asserting that on 19 August it had exfiltrated financial documents, bank correspondence, tax records, and source code from the systems of the Parliament of Montenegro, demanding a ransom of 10 million US dollars. The international community's response was swift: France dispatched a team of experts from the ANSSI agency, the FBI confirmed it was providing assistance, and NATO allies actively engaged in remediation efforts.

As someone who was professionally monitoring security processes during that period from the vantage point of civil society and research work, I was able to observe first-hand the extent to which this attack exposed systemic weaknesses: a slow crisis response, insufficient coordination between institutions, and a high degree of dependence on international assistance in crisis situations. From the perspective of electoral integrity, these attacks did not lead to a formal annulment of results or an interruption of voting, but they had an important psychological effect: among the public, they reinforced narratives about "controlled" or "endangered" elections, while within institutions they laid bare

inadequate preparedness for crisis communication. In direct conversations with actors from the civil sector and the electoral administration, which I conducted through various projects in the period 2016–2023, the key problem identified was precisely the combination of technical vulnerability and the absence of clear procedures for communicating with citizens in real time. It was the 2022 attack that proved to be the turning point leading to the adoption of the Cyber Security Strategy of Montenegro 2022–2026, including the introduction of multi-factor authentication, separate back-up systems, and closer cooperation with international partners.

Media and Narrative Campaigns

The media-narrative dimension of hybrid threats in Montenegro has developed in parallel with cyber incidents and political crises. DFC and CDT analyses consistently record a manifold increase in the number of disinformation posts on social networks and web portals, particularly during periods when sensitive decisions are taken: from the recognition of Kosovo's independence, through NATO accession, to the adoption of the Law on Freedom of Religion and the formation of new governments. The dominant narratives range from the delegitimization of NATO and EU membership ("Montenegro as a colony of the West"), through the contestation of Montenegrin identity and statehood, to attempts to present every reform step as an externally imposed condition rather than an expression of domestic political will.

In empirical terms, this involves a combination of three types of campaigns. The first type consists of campaigns that originate on anonymous or semi-anonymous portals

and Telegram channels, are then picked up by media outlets in the region, most frequently from Serbia and certain pro-Russian platforms, where the message is further radicalized and then fed back into the Montenegrin media space. The second type comprises campaigns that formally originate from domestic sources (e.g. a statement by a politician, a senior representative of a religious community, or a public figure), but are amplified through social networks to such a degree that they lose their connection to the original context and begin to take on "a life of their own." The third type relates to targeted attacks on civil society organizations and independent media, employing labels such as "foreign mercenaries" or "traitors" in order to delegitimize actors who advocate for Euro-Atlantic integration and the rule of law.

From my personal experience working in the civil sector and on political education programmes, the shift in target groups is particularly evident, whereas disinformation was previously directed primarily at older voters and consumers of traditional media, the focus has now shifted markedly towards young people and users of digital platforms. The use of visual content (memes, short video clips, manipulated photographs), as well as TikTok and Instagram formats, has proven especially effective in normalizing anti-EU and anti-NATO narratives among a segment of the younger population. This poses an additional challenge for the education system and for digital and media literacy programmes, which often lag behind the pace of change in communication habits.

Institutional Cooperation and Proxy Actors

Hybrid pressures on Montenegro can scarcely be understood without examining the role of so-called proxy actors: domestic political, media, religious, and economic structures that mediate the interests of external centers of power. During the political crises of 2019–2020 and 2022–2023, there was a noticeable synchronization between statements by certain representatives of the Serbian Orthodox Church, messages from pro-Russian political entities, and campaigns in regional media, creating an "echo chamber" effect in which the same narrative was reproduced simultaneously through multiple channels. In practice, this meant that key security and integration decisions, from the Law on Freedom of Religion to NATO membership, were not viewed solely through the prism of domestic politics, but became part of a broader geopolitical contest.

In conversations with actors from civil society and international organizations, which I conducted within the framework of projects dedicated to the rule of law and hybrid threats, a frequent observation was that the boundary between "domestic" and "external" actors is increasingly porous. A portion of political entities and media simultaneously communicates messages to the domestic public and adopts narratives originating from Belgrade or Moscow, while certain business structures exploit market openness to forge economic ties that can be leveraged as instruments of political pressure. This confirms that the analysis of hybrid threats must simultaneously encompass both internal systemic weaknesses and the ways in which external actors instrumentalize them.

Economic, Energy, and "Soft Power" Penetration

The economic and energy dimension of hybrid threats in Montenegro is often less visible than cyber-attacks or media campaigns, but in the longer term it may be even more consequential. Foreign investments in the energy sector, tourism, and real estate (particularly those originating from states whose policies are not aligned with the foreign and security policy of the EU and NATO) create a web of interests that can constrain the maneuvering space of domestic institutions on critical decisions. In the period following 2014, Russian capital had a significant presence in certain energy and tourism projects, which repeatedly raised the question of whether economic dependence can be exploited as an instrument of political pressure in the context of sanctions, voting in international organizations, and strategic infrastructure decisions.

Beyond the "hard" economic dimension, there is also a visible "soft power" component through sport, cultural events, religious gatherings, and media, that shapes citizens' perceptions of where Montenegro "naturally" belongs. In conversations with young people, particularly from the northern and central parts of the country, one frequently hears that their everyday media and cultural space is shaped more by content from Serbia and Russia than from the EU, which has direct implications for resilience against disinformation and anti-Euro-Atlantic narratives. The picture that emerges is one in which economic, energy, and cultural penetration are not separate spheres.

Institutional Response and Resilience

The response of Montenegrin institutions to hybrid threats has evolved gradually, often reactively, in the wake of major crises or incidents. The adoption of the Cyber Security Strategy 2022–2026 represents an important step forward, as it systematically maps competencies for the first time, identifies critical infrastructure, and envisages the development of a national CSIRT/CERT capacity in accordance with EU standards. At the same time, cooperation with NATO and the EU through support programmes, joint exercises, and expert assistance, has visibly raised the level of technical readiness within parts of the security and IT sector.

However, the analysis I have conducted through this paper indicates that institutional resilience still has three key weak points. First, capacities within the state administration remain limited, both in terms of the number of specialized IT and analytical staff and in terms of their retention within the system, given the competition from the private sector and international organizations. Second, cooperation between security services, regulators, independent bodies, and civil society is often ad hoc and personality-dependent rather than institutionalized through clear protocols and procedures. Third, the area of digital and media literacy remains insufficiently integrated into the education system and public administration training programmes, leaving ample space for disinformation campaigns to operate.

Despite these weaknesses, it is important to emphasize that Montenegro has in recent years demonstrated the

capacity to learn from crises, emulating good practices from the Baltic and Nordic states, investing in the strengthening of CERT structures, and establishing cooperation with partners who possess decades of experience in confronting similar threats. The success of this process will depend on the political will to treat questions of cybersecurity, financing transparency, and media-space regulation as priorities, rather than as technical issues to be addressed only within the confines of projects.

Comparative Regional Context

Montenegro's experience is not isolated - similar patterns of cyber-attack are visible across the Western Balkans, confirming the thesis of coordinated hybrid action in the region. Albania is, in this regard, a particularly illustrative case. In July 2022, the state portal e-Albania, which consolidates digital services ranging from school enrolment to the issuance of personal documents, was inaccessible for several days following an attack that Microsoft attributed to actors linked to the Iranian government. The group Homeland Justice, whose servers are connected to Iran, claimed responsibility, and the consequence was the severance of diplomatic relations between Albania and Iran in September 2022. The attacks continued: in December 2023, hackers targeted the Albanian Parliament and the telecommunications company One Albania, temporarily blocking parliamentary services, and in January 2024 the Institute of Statistics (INSTAT) was attacked. What makes the Albanian case relevant for comparison with Montenegro is the fact that the attacks were politically motivated and directed against a state that, like Montenegro, is a NATO member and an EU candidate,

suggesting that external actors use cyberspace as a tool for disciplining small Euro-Atlantic states.

In Bosnia and Herzegovina, the situation is further complicated by the fragmentation of the institutional system. According to data from the national CERT, in the period from 17 November to 17 December 2022 alone, more than 9.2 million cyber threats were registered, the majority of which were DDoS attacks. In October 2025, a coordinated ransomware campaign targeted energy companies in Bosnia and Herzegovina, including solar operators and electricity distributors, using advanced techniques to bypass firewalls through compromised third-party access. What distinguishes the Bosnian context from the Montenegrin one is the pronounced institutional fragmentation that precludes a rapid and coordinated response to cyber threats.

Serbia represents a specific case in which cyber activities manifest not only as attacks from abroad but also as state instruments of surveillance from within. In March 2025, Amnesty International documented that Serbian security services had used the Cellebrite forensic data-extraction tool together with zero-day exploit chains to compromise the phones of student activists and journalists. This finding confirms the broader picture in which cyber tools in the region are used not exclusively by external actors but also by domestic authorities to suppress critical voices, a dimension of hybrid action that is often overlooked in the literature.

The common pattern running through all these cases, and one I have had the opportunity to observe through exchanges of experience with colleagues at regional workshops and conferences, is a sequential model of

attack: after the initial cyber incident, a disinformation campaign almost invariably follows, magnifying the effect of the attack many times over and undermining citizens' trust in institutions and digital services. This is particularly pronounced in pre-election periods and during political crises, when societal polarization reaches its peak.

Discussion and Analysis

The complexity of the "vertical" and "horizontal" vectors of hybrid operations makes Montenegro a distinctive case, both in scale and in the dynamism of changes, revealing the intricate interplay of external and internal factors. The empirical data, presented through the study of cyber-attacks, media warfare, and economic vectors, point to specific weaknesses in Montenegro's institutional system: the system's frailty is most acute where the security sector is fragmented, procedures lack standardization, inter-ministerial cooperation is insufficient, and, above all, where digital literacy remains limited at all levels of the state administration (DFC, 2023; CDT, 2024).

When I set this Montenegrin picture alongside what I have seen reported in the rest of the region, several things stand out. Serbia relies on a strikingly similar combination of proxy influence and media amplification, yet the scale of its domestic media infrastructure gives disinformation campaigns a much larger echo chamber than anything Montenegro can produce on its own. Bosnia and Herzegovina adds another layer: the constitutional fragmentation of the state means that hybrid actors can exploit not just ethnic and religious divisions but also jurisdictional gaps,

something that became painfully clear during the 2022 ransomware wave, when no single entity had the mandate or the capacity to coordinate a rapid response. North Macedonia has invested more heavily in digital protection, particularly around elections, but remains exposed to regional propaganda flowing through shared-language media channels. Albania, while less frequently targeted, revealed through the 2022 e-Albania incident just how vulnerable even a NATO member's public digital infrastructure can be to a determined state-level attacker.

Turning to Montenegro's own institutional response, the picture is one of real but incomplete progress. The Cyber Security Strategy 2022–2026 and the strengthening of cooperation with the EU and NATO have raised the baseline. Yet from my experience following monitoring reports and participating in related projects, I can confirm that two structural problems remain stubbornly persistent: the hemorrhage of IT specialists from public administration to the private sector and international organizations, and the gap between formal cooperation frameworks and their actual operationalization. Regional information exchange, for instance, continues to be more declarative than operational, a point that analysts from across the Western Balkans have raised repeatedly.

There are, however, examples worth emulating. The Baltic states and Poland have moved well ahead in building automated disinformation-monitoring capacity, investing in digital education at scale, and developing public-private databases that enable real-time threat tracking. What makes their experience transferable, at least in part, to Montenegro is that they, too, faced the

challenge of building resilience in small states with limited resources and porous information environments. The key difference is sustained political commitment over more than a decade, something Montenegro has yet to demonstrate consistently. Without the digitalization of security analytics, continuous professional development, and genuinely operational regional task-force units, the domestic system will struggle to keep pace with the evolutionary character of hybrid threats.

Montenegro, in this sense, functions as a barometer for the limits of Euro-Atlantic resilience, but its reading will depend on whether all societal actors can be brought into the effort, institutional barriers overcome, and international models adapted without deepening the very divisions that hybrid actors seek to exploit.

Policy and Institutional Practice Recommendations

Recommendations for strengthening Montenegro's resilience to hybrid threats are necessarily multidimensional and require a systemic approach. Based on the analysis of trends in Montenegro and the region, several priority areas emerge.

The most urgent need is the establishment of a national center for monitoring cyber-attacks, disinformation, and proxy activities, one that would bring together state structures, regulators, and civil society in a permanent, operational framework rather than the ad hoc arrangements that have prevailed so far. Models from Estonia and Poland have demonstrated how such centers can be built from the ground up, incorporating both horizontal and vertical information exchange. Public-private partnerships with technology companies and telecommunications operators, which Montenegro has

begun developing in recent years, represent the fastest path towards an advanced cyber-threat response capability.

A second area that deserves far more attention than it currently receives is digital and media literacy. Programmes for deconstructing disinformation need to extend beyond the education sector into public administration, with continuous training for journalists, teachers, and civil servants. At CDT panel discussions, these initiatives have frequently been identified as priorities for the local community (CDT, 2024). Without sustainable support for investigative journalism and regional fact-checking projects, public trust will remain low and hybrid manipulation will continue to find fertile ground.

Finally, and this is something I have encountered repeatedly in following project work across the region, the problem of hidden funding flows, particularly to media outlets, NGOs, and para-religious structures, undermines every other effort. Legal mechanisms for full transparency, including mandatory disclosure of all donations and robust independent oversight, are a prerequisite for a healthy information environment. The Atlantic Council of Montenegro has proposed such measures on multiple occasions. Alongside domestic transparency, the enhancement of regional and international cooperation through bilateral and multilateral exercises, shared threat databases, and deeper integration with EU and NATO frameworks is indispensable.

All of these steps should be embedded in a national strategy, implemented over the long term, and supported

by the broad participation of the academic, private, and civil sectors. What I have learned from experience of working on domestic and regional projects is that no amount of technical capacity can substitute for political will and professional competence. These remain the true prerequisites for systemic transformation.

Conclusion

This paper is oriented not only towards analysis but also towards the development of competencies needed to meet the complex demands of institutional resilience. Responses to hybrid threats as contemporary security challenges, in Montenegro and across the wider Western Balkans, require a multidisciplinary approach. Practice demonstrates that responses cannot be grounded in a single dimension alone. The integration of the digital, educational, and energy sectors into public policy-making, as well as the strengthening of public-private partnerships alongside the monitoring of local actors, is highly needed. Equally essential is coordination, grounded in strong institutions and regional cooperation. The analysis shows that Montenegro, as a kind of barometer for Euro-Atlantic resilience, remains exposed to sophisticated forms of external destabilization that instrumentalize local weaknesses and prolong conflicts.

The research indicates that the solution lies in the systemic strengthening of institutional capacities, transparency, and digital literacy, but also in continuous engagement with regional and international partners and in the development of new models of public-private cooperation. The specificity of this region, its institutional weaknesses, but also the qualitative advantages of partnership with Baltic and Northern

European states, are key areas for developing new models of resistance to hybrid threats.

The next phase of research should include a deeper comparative analysis of institutional resilience models from the Baltic and Nordic countries. Experience confirms that precisely these practices offer innovative and stable solutions that can be partially adapted to local conditions. Deeper empirical mapping of the influence of specific proxy actors (local, regional, and global) on electoral processes and economic flows is also needed, along with the preparation of periodic national reports on incidents and responses, with detailed policy recommendations and measurable progress indicators.

This paper arose from the need to enrich the domestic literature with empirical evidence, systematic comparisons, and practical recommendations. When I began this research, my working assumption was that Montenegro's primary vulnerability lay in its technical infrastructure, the hardware and software gaps that the 2022 attack so dramatically exposed. The evidence gathered here has, however, pointed to a deeper problem: the institutional and human dimension. Technical systems can be upgraded relatively quickly; building a culture of inter-institutional cooperation, retaining skilled professionals in the public sector, and embedding digital literacy across an entire society is the work of a generation. Whether Montenegro rises to that challenge will determine not only its own resilience but will also signal to the wider Euro-Atlantic community how seriously small frontline states can be supported, and how effectively they can protect themselves.

Literature

1. Amnesty International (2025). "A Prison Without Walls": Digital Surveillance of Civil Society in Serbia. London: Amnesty International.
2. Atlantic Council of Montenegro (2024). Hybrid Influence and Regional Security. Podgorica: Atlantic Council of Montenegro.
3. Center for Democratic Transition (CDT) (2024). Regional Vulnerabilities to Hybrid Threats. Podgorica: CDT, Montenegro.
4. Digital Forensic Center (DFC) (2023). Mapping Hybrid Threats in Montenegro. Podgorica: DFC, Montenegro.
5. European Parliamentary Research Service (2017). Countering Hybrid Threats: EU and the Western Balkans case. Brussels: EPRS.
6. European Union Hybrid Centre of Excellence (NATO Hybrid CoE) (2023). Building Resilience to Hybrid Threats. Helsinki: NATO Hybrid CoE.
7. FireEye (2017). APT28: At the Center of the Storm. Milpitas, CA: FireEye Inc.
8. Galeotti, M. (2014). The 'Gerasimov Doctrine' and Russian Non-Linear War. In Moscow's Shadows [blog], 6 July 2014.
9. Microsoft Threat Intelligence Center (2022). Microsoft Investigates Iranian Attacks Against the Albanian Government. Redmond, WA: Microsoft Corporation.
10. Ministry of Public Administration (2022). Cyber Security Strategy of Montenegro 2022–2026. Podgorica: Ministry of Public Administration of Montenegro.
11. Montenegro Chamber of Commerce (2025). Launch of the MontEDIH Project Implementation. Available at: https://komora.me/projekti/pocela-implementacija-projekta-montedih

12. Rácz, A. (2015). Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist. FIIA Report No. 43. Helsinki: Finnish Institute of International Affairs.

13. UK Foreign, Commonwealth & Development Office (FCDO) (2025). Western Balkans Summit on the Berlin Process, London: Chair's Conclusions. London: FCDO.

14. Vuković, S. (2022). Hybrid Threats and Security in Southeast Europe. European Security Studies, 12(2). 49–68.