KCSS
Kosovar Centre for Security Studies

SECURE FUTURES SERIES

#3, SEPTEMBER 2025

Dealing with Hybrid Threats in Kosovo and Potential for Improvement

By Denora Gashi[1]

Hybrid threats are not abstract risks for Kosovo; they are becoming a growing reality. What makes Kosovo particularly vulnerable is the combination of its dispute with Serbia, fragile interethnic relations, and the country's ambition to consolidate its statehood and sovereignty, as well as its Euro-Atlantic integration aspirations. This mix makes it a testing ground for hostile actors seeking to undermine NATO and EU credibility, such as Russia and China. The challenge, then, is not only defensive. Kosovo has not ignored these challenges. In recent years, it has adopted the National Cyber Security Strategy 2023–2027, passed the Law on Cyber Security, and begun operationalizing the Cyber Security Agency and related coordination bodies. These steps align Kosovo with Euro-Atlantic standards and provide an institutional framework to address threats. Yet, progress remains uneven. Kosovo can demonstrate that small states are capable of building resilience by incorporating foresight and fostering alliances, as well as promoting societal cohesion within their national security doctrine. Responding to hybrid threats in Kosovo requires building on existing capacities and leveraging partnerships. The following six areas represent feasible yet impactful steps that Kosovo can take to strengthen its resilience against hybrid threats.

1 **Developing a National Hybrid Threat Doctrine.** Kosovo's institutions are addressing hybrid threats in silos: counter-terrorism here, cyber defense there, and sporadic responses to disinformation elsewhere. By adopting the 2023–2027 Cybersecurity Strategy and the Law on Cyber Security, Kosovo has established the legal and institutional foundations for defending its digital domain. The creation of the

[1] Denora Gashi is a junior non-resident research fellow at the Kosovar Centre for Security Studies (KCSS), and is currently pursuing postgraduate conflict studies at the London School of Economics (LSE)

Cybersecurity Agency, the designation of a National Coordinator, and the formation of a State Cybersecurity Council represent critical first steps. However, these instruments primarily address cyber threats and do not yet encompass the broader spectrum of hybrid risks—such as disinformation, foreign influence, and economic coercion. This fragmentation weakens deterrence. A National Hybrid Threat Doctrine would bring coherence, defining typologies of threats specific to Kosovo's context, clarifying institutional responsibilities, and setting out mechanisms for coordination. Such a doctrine would not require the creation of new institutions, but rather aligning existing ones under a common framework. This would improve readiness, resource allocation, and also foster cooperation with partners, by increasing the understanding of how to support Kosovo's resilience towards hybrid threats.

2 **Treating Disinformation as a Cohesion Challenge.** Kosovo also recognized disinformation as a threat in its Security Strategy 2022-2027, and research by thinks-tanks such as KCSS have shown disinformation affects Kosovo's security and societal cohesion. The problem is not only informational but societal, in the sense that malign narratives consistently target ethnic divisions, presenting institutions as illegitimate or hostile to non-majority communities. Current responses include some fact-checking by civil society and occasional official rebuttals bu these are insufficient to address the deeper problem of interethnic trust. Disinformation in Kosovo primarily seeks to undermine trust particularly between the Kosovo Albanians and the Kosovo Serbs. Addressing this cannot rely solely on fact-checking; it requires building communication channels that reinforce inclusion and shared citizenship. A feasible step would be to establish a permanent interethnic communication platform that brings together local media, municipal leaders, and civil society actors to respond quickly and credibly to divisive narratives. By institutionalizing inclusive messaging in both Albanian and Serbian, Kosovo can mitigate the impact of disinformation campaigns and enhance its social cohesion.

3 **Cybersecurity as Public Confidence.** The adoption of the Cyber Security Strategy and the Law on Cyber Security already provides Kosovo with an institutional framework for digital defense, and the establishment of KOS-CERT has improved coordination with service providers. Yet, recent cyberattacks, including DDoS disruptions against government websites in 2024, show that the perception of vulnerability remains high. For citizens, confidence in state resilience is as important as technical protection. Building on the progress made, Kosovo should introduce a National Cyber Resilience Plan that emphasizes transparency and recovery, with clear public communication during incidents, annual national exercises to test systems, and a reporting regime that ensures timely notification without excessive bureaucracy. These measures would consolidate existing frameworks and reinforce trust in institutions..

4 **Reducing Foreign Economic Leverage.** Kosovo's has strong legal basis for protection of critical infrastructure, including the Law on Sustainable Investments (Law No. 08/L-209). However, recent controversies, such as the case of Elektrosever operating outside Kosovo's regulatory framework, illustrate how external actors can exploit economic arrangements to undermine sovereignty. The next logical step is to complement existing policies with a foreign investment screening mechanism focused on critical sectors such as energy, media, and real

estate near strategic assets. In addition to this, the government should increase cooperation with think-tanks and media on supporting the screening of foreign economic presence in Kosovo, from countries that have malign approach towards Kosovo, such as Russia and China.

5 Linking Digital and Physical Security. The Banjska terrorist attack in 2023 showed the hybrid nature of Kosovo's security challenges: online disinformation, cross-border support networks, and armed violence converged in a single terrorist act. Investigations and indictments indicate that Kosovo's institutions responded firmly; however, attribution processes remain fragmented across various agencies. Building on the institutional reforms in cyber and security policy, Kosovo should establish an integrated mechanism for attribution and accountability. By pooling intelligence, law enforcement, and cyber forensics, such a mechanism would reduce ambiguity, strengthen legal proceedings, and provide Kosovo with credible evidence in diplomatic engagements.

6 Leveraging NATO Centres of Excellence for Cybersecurity and Hybrid Threats. Kosovo has already aligned parts of its institutional and legal architecture with Euro-Atlantic standards. The National Cyber Security Strategy 2023–2027 and the Law on Cyber Security establish structures that mirror practices in NATO and EU member states. However, these frameworks remain young, and Kosovo still lacks advanced expertise in areas such as cyber forensics, coordinated attribution, and hybrid-threat scenario planning. Building strong partnerships with NATO's network of Centres of Excellence (CoEs) would therefore be a cost-effective way to accelerate capacity development and anchor Kosovo's security reforms in allied practice. The most relevant centres for Kosovo are the Cooperative Cyber Defence CoE (CCDCOE) in Tallinn, which leads NATO work on cyber doctrine, legal frameworks, and technical exercises, and the European Centre of Excellence for Countering Hybrid Threats - Hybrid CoE in Helsinki, which focuses on resilience across political, economic, and information domains. Kosovo cannot yet join these centres as a full participant, but it can seek observer or affiliate status, building on its existing cooperation with NATO through KFOR and the enhanced dialogue on resilience. Such engagement would provide Kosovo with access to best practices, participation in table-top exercises and simulations, and opportunities to train officials and technical staff, and all the while increasing interoperability with NATO.