KCSS
Kosovar Centre for Security Studies

Ignita

OPEN SOCIETY FOUNDATIONS
WESTERN BALKANS

SECURING ENLARGEMENT

ADVANCING WB6 GRADUAL INTEGRATION IN THE EU THROUGH CYBERSECURITY, FDI SCREENING, AND RULE OF LAW

MENTOR **VRAJOLLI** AND RAMADAN **ILAZI**

EXECUTIVE SUMMARY

The Western Balkans Six (WB6) stand at a pivotal moment in the EU integration process. The dramatically changing geopolitical context and the need for resilience in critical sectors have put enlargement and security back at the heart of the EU agenda, creating urgency for the integration of the region.

Particularly, three key areas – cybersecurity, screening of foreign direct investments, and rule of law in the Western Balkans – sit on the edge between vulnerability and opportunity. If left unaddressed they risk weakening both the region and the EU. On the other hand, through phased integration in the EU, they can become early wins that strengthen security, democratic resilience and resolve towards the fundamental EU values.

Rising cyberattacks, corrosive capital and malign foreign influence through foreign investments, and weak rule of law expose the region as EU's "soft underbelly." At the same time, the EU's regulatory tools such ENISA (European Union Agency for Cybersecurity) (ENISA, n.d.), the Foreign Direct Investment Screening Regulation (FDISR) (EUR-Lex, 2019a), and the EU Rule of Law Report (EURoLR), offer means for phased integration. By advancing operational integration in these frameworks, the EU and the WB6 can turn political momentum into measurable progress, leading to greater confidence in the promise of EU perspective.

On their part, WB6 governments must move quickly on aligning legislation with relevant EU directives, adopting FDI screening legislation, and strengthening cybersecurity agencies and Computer Security Incident Response Teams (CSIRTs). At the regional level, WB6 should establish for regional coordination on cybersecurity and FDI screening. While the EU can extend observer participation and technical assistance, link milestones to IPA III and the Reform and Growth Facility, and mainstream information-sharing.

Tangible cooperation that reduces security risks at the EU's perimeter, protects the Single Market from regulatory arbitrage, and demonstrates that enlargement is a strategic investment in stability.

STATE OF AFFAIRS

The Western Balkans Six (WB6) are once again in the spotlight of the European Union (EU), where enlargement is increasingly seen not only as a political choice but also as a security imperative. Although the promise of membership dates back to the 2003 Thessaloniki Summit, progress has stalled in recent years, while the broader geopolitical context has changed significantly. Reforms have slowed in the absence of both a credible EU perspective and lack of political will among WB6 governments to implement them. Today, however, the geopolitical context has shifted. Russia's full-scale invasion of Ukraine, the EU's growing security concerns, and the importance of resilience in critical sectors have created a new opening for a more structured, phased enlargement approach towards the region. In this context, discussions on staged and gradual accession have created a policy window to advance integration incrementally in areas of mutual benefit. Three such areas stand out: cybersecurity, foreign direct investment (FDI) screening, and the rule of law. Each addresses an area of major vulnerability in the WB6 while, at the same time, reinforcing the EU's own security interests. Each also benefits from an existing EU regulatory or institutional framework that can serve as a vehicle for gradual integration. Together, these three areas offer concrete entry points for both the region and the EU to move beyond rhetoric commitments and achieve what might be called the operational integration of the WB6 into the Union.

- **Cybersecurity** has become a central challenge for the WB6, both as a domestic priority and as a prerequisite for EU accession. While WB6 countries have adopted appropriate national strategies and established Computer Security Incident Response Teams (CSIRTs), significant capacity gaps persist: budgets remain limited, coordination is not always effective, and links with EU structures are, at times, weak. Furthermore, regional cooperation on cybersecurity is notably underdeveloped. In this remit, the EU Cybersecurity Act (2019/881) (EUR-Lex, 2019b), which established the European Union Agency for Cybersecurity (ENISA), provides a ready framework for gradual WB6 integration with the EU and a platform to deepen intra-regional cooperation. Granting the WB6 observer status in ENISA's Management Board or working groups would strengthen regional capacities and capabilities, while simultaneously strengthening the EU's own security. Such steps would also align with the EU's stated commitment to integrate the WB6 into the single digital market. The urgency for cybersecurity integration of WB6 in EU was made clear by recent large-scale cyberattacks in Albania and Montenegro, which exposed the fragility of critical services in the region and the potential risks of spillover into EU systems.

- **Foreign Direct Investment (FDI) Screening** remains essential to the economic development of the WB6, yet the absence of robust screening mechanisms leaves the region vulnerable to the risks associated with strategic investments from authoritarian states. The EU FDI Screening Regulation (2019/452), in force since October 2020, established a cooperation mecha-

nism to assess risks to security and public order. While 23 EU member states have adopted screening systems, alignment across WB6 varies. Kosovo has taken the lead by adopting its 2024 Law on Sustainable Investments, which creates a national screening mechanism and institutional responsibilities. Albania has drafted legislation, while other states are at earlier stages or have yet to initiate reforms. Without adequate and credible screening frameworks, the WB6 risk regulatory arbitrage and exposure to malign foreign influence and corrosive capital, particularly in energy, telecommunications, and media sectors. For the EU, this represents a direct challenge to advancing WB6 integration into the Single Market, as it is detrimental to its coherence. Accordingly, gradual integration of WB6 into the FDI Screening Expert Group and access to the EU's Contact Points network would both incentivize reforms and strengthen collective resilience.

- **Rule of law** remains the cornerstone of the enlargement process, as well as the most persistent challenge in the WB6. The EU Rule of Law Report (EURoLR) (European Commission, 2024), has become a central monitoring tool for Member States and, since 2024, has also included Albania, Montenegro, North Macedonia, and Serbia. The exclusion of Kosovo and Bosnia and Herzegovina, however, risks undermining the credibility and comprehensiveness of the exercise. Weak judicial independence, pervasive corruption, and limited checks and balances continue to constrain democratic consolidation in the region. Extending the EURoLR' structured framework to all WB6 would anchor reforms in an annual cycle of assessment, dialogue, and conditionality, ensuring consistent monitoring and reinforcing the message that rule-of-law progress is measurable and comparable across all aspirants.

The WB6 remain exposed to cyber threats, malign foreign investment, and persistent rule of law deficits. At the same time, EU mechanisms already exist that could serve as vehicles for phased integration. Extending ENISA cooperation, including WB6 in FDI screening structures, and fully integrating the region into the EURoLR process would provide tangible progress in line with the EU's evolving enlargement debate. For the WB6, these steps would build credibility in the accession process; for the EU, they would strengthen internal security, protect economic sovereignty, and demonstrate that enlargement remains a strategic investment in stability.

CHALLENGES

➤ Exclusion from EU cybersecurity structures

The WB6 remain outside ENISA, despite the EU's commitment to bring the region closer to the Digital Single Market. This disconnect creates a gap between policy objectives and institutional practice. Without structured participation, WB6 cannot benefit from EU expertise, joint exercises, or certification schemes, and the EU cannot ensure that its own digital space is uniformly secure.
Deeper integration into ENISA structures would help close this gap. Granting observer status and participation in ENISA working groups would enable WB6 to align earlier with EU standards, strengthen their national CSIRTs, and improve resilience of regional digital infrastructure. For the EU, including WB6 would ensure that security in the Digital Single Market extends seamlessly across its immediate neighborhood.

➤ Non-participation in the EU's FDI screening system

The WB6 are not part of the EU's cooperation framework under Regulation 2019/452 (EUR-Lex, 2019a). While Kosovo has introduced a national screening law, the region as a whole lacks access to the EU Expert Group and Contact Points network (European Commission, n.d.). This gap hinders systematic information-sharing on high-risk investments and leaves a blind spot at the EU's external border. Closer integration into the EU's FDI screening system would address these vulnerabilities. Participation in the Expert Group and Contact Points network would help WB6 governments to identify and manage risks linked to opaque or strategic investments, while reassuring investors of transparent and predictable rules. For the EU, it would strengthen the integrity of the Single Market and reduce the scope for regulatory arbitrage.

➤ Incomplete integration in the EU Rule of Law Report

The EU Rule of Law Report covers four WB6 countries, with Kosovo and Bosnia and Herzegovina remaining excluded. This partial coverage undermines the credibility and consistency of EU monitoring. Without full participation, reform incentives are uneven, and gaps in judicial independence and anti-corruption efforts fall outside a common EU framework. Extending the Rule of Law Report to all six countries would help address these weaknesses. It would place every each of the WB6 countries under the same standards of assessment, strengthen reform incentives, and improve comparability across the region. For the EU, it would enhance the coherence of its conditionality framework and reinforce its message that the rule of law is the foundation of gradual integration.

RECOMMENDATIONS

Recommendations for national governments

Adopt and operationalize FDI screening laws (short-term)

Governments in Albania, Bosnia and Herzegovina, Montenegro, North Macedonia, and Serbia should adopt legislation aligned with Regulation 2019/452 by mid-2026, following Kosovo's example. Laws should designate clear institutional responsibilities, provide appeal mechanisms, and be supported by staff training. EU technical assistance (IPA III, Structural Reform Support Programme) can facilitate rapid implementation.

Strengthen CSIRTs and cybersecurity strategies (medium/long-term)

All WB6 governments should update national cybersecurity strategies by 2026, allocate dedicated budgets to CSIRTs, and ensure inter-ministerial coordination. Embedding EU standards for certification and resilience testing will help prepare for participation in the Digital Single Market. Financing can be drawn from IPA III and the Reform and Growth Facility.

Western Balkan governments should adopt national legislation aligned with the EU's NIS2 (for a high common level of cybersecurity) and RCE/CER (on the resilience of critical entities) Directives

WB6 governments should adopt legislation that transposes the EU's NIS2 (EUR-Lex, 2022b) and RCE/CER directives (EUR-Lex, 2022b). This requires clearly defining critical infrastructure sectors, designating 'essential' and 'important' entities using transparent, risk-based criteria, and assigning oversight responsibilities to competent authorities. Establishing or strengthening national cybersecurity agencies and CSIRTs is essential to ensure compliance and coordination.

Recommendations for regional bodies

Establish a Regional Cybersecurity Forum (short/medium-term)

Within the framework of the Berlin Process or the Common Regional Market, WB6 governments should jointly launch a standing Regional Cybersecurity Forum with a dedicated secretariat and regular meetings. The forum should develop a shared alert system, coordinate threat assessments, and standardize best practices across national CSIRTs. It should also serve as the official channel for structured engagement with ENISA, preparing the WB6 for gradual participation in the EU's Digital Single Market.

Coordinate FDI screening practices (medium/long-term)

A regional task force should be created to harmonize thresholds, procedures, and risk criteria for FDI screening. This would reduce fragmentation, prepare countries for participation in the EU FDI Screening Contact Points network, and strengthen the region's collective economic security.

Recommendations for EU institutions

Include WB6 in the EU's FDI Screening Expert Group and Contact Points network (short-term/medium-term)

The European Commission should extend observer participation to WB6 governments in the EU's FDI screening cooperation framework. This would enable structured information-sharing on high-risk investments, prepare the region for full legislative alignment, and reduce vulnerabilities at the EU's external borders.

Extend the Rule of Law Report to all WB6 countries (medium/long-term)

The European Commission should include Kosovo and Bosnia and Herzegovina in the 2026 Rule of Law Report cycle. Comprehensive coverage would enhance the credibility of EU monitoring, provide consistent benchmarks across the region, and reinforce the centrality of the rule of law in staged accession.

REFERENCES

European Commission. (2024). 2024 Rule of law report. European Commission. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/annual-rule-law-cycle/2024-rule-law-report_en

European Union Agency for Cybersecurity (ENISA). (n.d.). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/

European Commission, (n.d.). Directorate-General for Trade. Investment screening. https://policy.trade.ec.europa.eu/enforcement-and-protection/investment-screening_en

EUR-Lex (2019a, March 19). Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union. Official Journal of the European Union, L 79, 1–14. https://eur-lex.europa.eu/eli/reg/2019/452/oj/eng

EUR-Lex (2019b, April 17). Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, 15–69. https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

EUR-Lex (2022a, December 14). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

EUR-Lex (2022b, December 14). Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union, L 333, 164–195. https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng