European Union Institute for Security Studies

SHARED THREATS, SHARED RESILIENCE

BRIEF / 8
May 2026

Integrating enlargement partners in EU digital and cyber security

The EUISS is an agency of the European Union

by

Clotilde Bômont
Senior Policy Analyst

Bojana Zorić
Policy Analyst

Summary

- The EU and its enlargement partners already operate within a shared digital and cyber threat environment. Yet existing governance frameworks and cooperation mechanisms have not kept pace with this interdependence.
- This creates a gap between regulatory alignment and operational readiness. Initiatives such as ENISA-supported capacity building and the Western Balkans Cyber Capacity Centre provide avenues for cooperation, but engagement remains uneven and coherent pre-accession mechanisms are still lacking.
- Fragmented governance, skills shortages, limited resources, asymmetric information-sharing and dependencies on foreign providers also hinder efforts to strengthen regional and digital cyber security. At the same time, enlargement partners, notably Ukraine and Moldova, have valuable but underutilised operational experience developed under sustained pressure.
- Enhancing European cyber and digital security requires more operational and inclusive cooperation before accession. This entails reinforcing political, societal and industrial resilience across Europe.

Gaps in cyber and digital resilience in the EU neighbourhood pose a direct threat to European security. Cyberattacks and digital dependencies have become core instruments of coercion, destabilisation and influence across the EU's wider neighbourhood, targeting government services, critical infrastructure, electoral processes, supply chains and the information space[1]. At the same time, digital infrastructures and data flows are inherently cross-border, binding enlargement partners and EU Member States into a shared and interdependent digital environment.

Yet digital policy and cybersecurity in the enlargement context remains largely embedded in a gradual, compliance-driven accession process, focused on regulatory alignment and unevenly implemented across enlargement partners in the Western Balkans and the Eastern Neighbourhood. This approach sits uneasily with a fast-moving and transnational threat landscape. It hampers the capacity to respond collectively to shared threats, as cooperation remains fragmented and often reactive. Existing EU cybersecurity frameworks provide a basis for integration, but continue to expose shortcomings in capacity, coordination and

access to operational cooperation. In parallel, the enlargement partners are frontline actors who have capabilities that could be better used to strengthen regional security as a whole.

These realities underline the need to act before accession to the EU. This Brief argues that the EU should move beyond a focus on formal alignment and improve the practical conditions under which resilience can be built and sustained. This means addressing persistent shortages of human, financial and institutional resources, and enabling more participation in operational activities, including information-sharing and joint exercises.

A SHARED THREAT ENVIRONMENT

The EU and its enlargement partners are increasingly connected through digital infrastructure, service providers and information spaces, exposing them to common vulnerabilities and adversaries. The Russian Viasat attack targeting the satellite KA-SAT network, for instance, demonstrated how a cyber operation aimed at disrupting Ukrainian communications also affected satellite broadband users across Europe[2].

This shared environment is increasingly exposed to sophisticated cyberattacks, carried out by state actors including China, Russia, Iran and North Korea, as well as by non-state groups[3], through operations such as Volt Typhoon, NotPetya, the Homeland Justice attack, and the WannaCry and Andariel campaigns. The effects of these attacks are often systemic, with the potential to disrupt essential services, undermine elections and democratic processes and destabilise societies.

Recent data confirms the scale and intensity of this threat landscape. The EU Cybersecurity Agency (ENISA) recorded 4 875 incidents between July 2024 and June 2025, with a growing use of AI in malicious activities and an increase in attacks directly targeting strategic points in digital supply chains. Public services, transport, and digital infrastructure and services remain among the most targeted sectors, with public administration accounting for more than a third of recorded incidents alone. Around 80% of the reported attacks are ideologically driven, far exceeding financially motivated operations (13%) or cyber-espionage (7%)[4].

A similar trend is observable in enlargement partners. Ukraine recorded more than 5 900 cyberattacks in 2025 (approximately 16 per day), representing a 37% increase compared to 2024 (4 315 incidents). Moldova, meanwhile, faced over 1 000 cyberattacks in the first half of 2025 alone, many attributed to Russian-affiliated groups. Electoral processes have been a primary target: peaks in large-scale Distributed Denial of Service (DDoS) attacks were reported around the 2024 presidential and 2025 parliamentary elections, with the 2025 elections generating over 16 million malicious connection attempts against electoral and government systems, forcing the temporary blocking of 4,000 websites[5].

INTERLOCKING CHALLENGES

Addressing cross-border vulnerabilities requires a response at the regional level. Yet efforts remain constrained by fragmented governance, limited resources, uneven capabilities and insufficient information-sharing across the EU and enlargement partners.

Compliance over operational resilience: The European Commission's January 2026 cybersecurity package[6] emphasises the importance of extended partnerships and cooperation to address the current threat landscape, and the Commission's 2025 enlargement package[7] frames gradual integration to strengthen security and stability before accession. While regulatory compliance is an important driver of regional security in the pre-accession context, it should not be at the expense of operational resilience. Alignment with the EU *acquis* does not in itself guarantee preparedness.

The gradual uptake of key EU instruments – including the NIS2 Directive, the 5G Toolbox and broader digital policy frameworks – thus matters less as an end in itself than as a means to build resilience in practice. Yet instruments designed primarily for the Union's internal architecture are difficult to transpose operationally in enlargement contexts. Even across Member States, the implementation of frameworks such as NIS2 remains uneven[8]. To narrow this gap, ENISA and the European Commission (DG ENEST) have concluded a three-year contribution agreement to strengthen cybersecurity resilience in the Western Balkans, supporting targeted capacity-building efforts. Tools such as the AR-in-a-Box[9] ('Awareness Raising in a Box') support exercises and awareness-raising, while regional and bilateral formats – including the Western Balkans Cyber Capacity Centre (WB3C)[10], the EU-Ukraine Cyber Dialogue[11], and Moldova's access to the EU Cybersecurity Reserve[12] – reflect a growing emphasis on operational cooperation and solidarity. Alignment should focus on effective implementation and operationalisation.

Lack of resources and institutional constraints: Institutional fragmentation, complex governance and

the multiplicity of EU instruments also hinder coordination, especially in crisis situations where speed and clarity of responsibility are critical. At the same time, severe shortages of cybersecurity professionals remain a significant challenge both for the EU and for enlargement partners. While tools such as ENISA's European Cybersecurity Skills Framework[13] help address this issue by supporting the assessment and harmonisation of relevant competencies, the cybersecurity workforce remains insufficient, with more than half of European organisations (52%) struggling to retain qualified professionals[14]. This not only weakens governments' defensive capabilities, but also limits the development of domestic expertise and solutions, as well as the use of open-source alternatives which require advanced in-house skills.

Furthermore, asymmetries in information-sharing between the EU and enlargement partners hinder cross-sector coordination and preparedness for transnational cyber incidents, highlighting one of the limits of pre-accession integration. While existing initiatives, such as the EU-Ukraine Cyber Dialogue, support exchanges of good practices and situational awareness, access to more advanced operational structures remains restricted. The EU CSIRTs network is not open to enlargement partners, as it is legally defined under the Network and Information Systems (NIS) framework. This highlights a broader constraint: current mechanisms are either too limited in scope or too restrictive to match the level of interdependence already in place. Alignment must also catch up with the *de facto* level of integration with the EU.

Structural dependencies and vulnerabilities: Cooperation will remain fragile if the underlying digital stack is fragmented and relies extensively on foreign providers. This points to another mismatch in the enlargement process: between rapid digitalisation as an accession requirement and the structural conditions needed for secure digitalisation. While the enlargement process incentivises fast uptake, the EU increasingly prioritises digital sovereignty and the reduction of strategic dependencies[15]. In practice, however, enlargement partners rely on the most accessible solutions – often provided by dominant non-European actors, namely US and Chinese – because they are cheaper, scalable, user-friendly, and high- performing. As a result, current approaches risk entrenching the very dependencies the EU seeks to reduce.

Dependence on non-European providers is a challenge not limited to enlargement partners. The EU's digital infrastructure relies heavily on a small number of external providers, particularly in cloud services, where Amazon, Google and Microsoft control 63% of the regional market[16]. While the Commission's 2026 cybersecurity package – including NIS2 – acknowledges the security of ICT supply chains, addressing technological dependencies requires broader industrial policy choices. The issue extends beyond technical mitigation to questions of digital sovereignty and strategic autonomy. Aligning enlargement-driven digitalisation with the EU's sovereignty agenda is thus essential to limit structurally embedded dependencies.

ENHANCING RESILIENCE BEFORE ACCESSION

In order to enhance Europe's capacity to address digital threats, the EU and its enlargement partners need to improve political, societal and industrial resilience.

Political resilience: The EU and its enlargement partners need to be able to sustain swift and collective action under pressure. This requires clear

How to build digital and cyber resilience before accession?

Enhancing the EU's and its enlargement partners' capabilities

	Short term 0-24 months	Medium term 2-5 years	Long term 5+ years
Political resilience Coordinate, decide and respond under pressure	> Increase information sharing > Participate in joint cyber exercises > Expand existing coordination platforms (Cyber Dialogue, WB3C, EU Cybersecurity Reserve)	> Develop a joint-CSIRT-like network > Harmonise threat assessment and crisis-response procedures	> Integrate enlargement partners into EU cyber cooperation frameworks
Societal resilience Absorb, withstand and recover from disruption	> Scale population-wide basic digital skills > Use ENISA training tools and AR-in-a-Box > Share operational experience and know-how	> Develop advanced cyber expertise through specialised university programmes and professional training > Strengthen cybersecurity of critical infrastructure and essential services	> Improve the reliability, transparency and security of digital public services
Industrial resilience Sustain trusted capabilities and limit external dependencies	> Apply 5G Toolbox measures where feasible > Strengthen collaboration between private sector and academia to support technological development	> Reduce exposure to high-risk vendors > Improve data governance frameworks > Support the growth of regional digital providers	> Integrate EU-neighbourhood digital markets > Build multi-vendor digital supply chains

institutional mandates, interoperable procedures, effective crisis-management mechanisms and trusted information-sharing channels, supported by cooperation between cybersecurity agencies at EU, Member State and enlargement partner level, and by instruments such as NIS2 or the 5G Toolbox. Engagement with EU structures also needs to be more accessible and functional. Where full participation is not possible, alternative formats should be developed to enable closer interaction with relevant actors, including EU CSIRTs. Existing platforms, such as the WB3C, can play a key role in facilitating coordination, notably through joint exercises and the development of shared practices. Peer exchanges and practical collaboration on implementation challenges (such as managing high-risk vendors) should also be reinforced, as they can reduce fragmentation and support mutual learning.

Societal resilience: European societies must also be able to withstand and recover from cyber and hybrid disruption without major political or social destabilisation. This requires robust digital architectures for critical infrastructures and essential services, supported by regional incident response mechanisms and improved sharing of operational experience. It also requires stronger basic and advanced digital skills among the population, both in the EU and in enlargement partners. In practice, this means better cyber awareness and hygiene, more practice-oriented university training, stronger links between public institutions, academia and the private sector, and greater resilience against disinformation and manipulation. EU tools, including ENISA's Cybersecurity Skills Framework, could support training, align skills and strengthen expertise; in parallel, simulations – such as the eight large-scale cyber exercises conducted by Ukraine since 2023 – could help develop practical know-how and operational readiness. These efforts can be further reinforced by leveraging broader European capacity-building initiatives, such as GLACY-e, the Octopus Project and EU CyberNet[17].

Industrial resilience: The EU and its enlargement partners need a robust digital industrial base to reduce dependencies on non-European providers. This requires not only access to, but the ability to build, procure, maintain and scale trusted digital infrastructures and services. Industrial resilience thus extends beyond cybersecurity: it encompasses diversified ICT supply chains, effective data governance frameworks, strategic procurement policies, and the capacity to sustain regional solutions. A more integrated market across the wider European digital space could expand demand and enable regional providers to scale up and offer viable alternatives to dominant external actors. This would require targeted procurement, provider diversification, and sustained investment in skills, research and innovation ecosystems. Platforms such as the WB3C could serve not only as training hubs, but also as facilitators of regional industrial uptake, innovation and cross-border cooperation.

References

* The authors thank Maria Loredana Campione and Alessandro Vitiello, EUISS trainees, for their research assistance.

(1) EEAS, 'Countering hybrid threats – strategic communications', 2024 (https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en).

(2) European Council/Council of the European Union, 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union', 10 May 2022 (https://www.consilium.europa.eu/en/press/press-releases/2022/05/10).

(3) CERT-EU, *Threat Landscape Report 2024: A Year in Review*, 2025 (https://cow-prod-www-v3.azurewebsites.net/publications/pdf).

(4) European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape*, October 2025 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025).

(5) Data collected during a EUISS workshop on 12 March 2026, gathering enlargement partners, cybersecurity agencies and EU institutions.

(6) European Commission, 'Proposal for a Regulation for the EU Cybersecurity Act', January 2026 (https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act).

(7) European Commision, '2025 Communication on EU enlargement policy', November 2025. (https://enlargement.ec.europa.eu/document/Policy.pdf).

(8) European Cyber Security Organisation, 'NIS2 Directive Transposition Tracker', 2026 (https://ecs-org.eu/activities/nis2-directive-transposition-tracker/).

(9) ENISA, 'Cybersecurity Awareness Raising: The ENISA-Do-It-Yourself Toolbox' (https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/ar-in-a-box).

(10) Western Balkans Cyber Capacity Centre (https://wb3c.org/).

(11) EU-Ukraine Cyber Dialogue (https://enlargement.ec.europa.eu/news).

(12) EU Cybersecurity Reserve (https://eur-lex.europa.eu/eli/dec_impl/2025/1458/oj/eng).

(13) ENISA, 'European Cybersecurity Skills Framework (ECSF)' (https://www.enisa.europa.eu/topics/skills-and-competences).

(14) ISACA, ' Budgets, staffing and skills fail to keep pace with rising cyber threats', September 2025 (https://www.isaca.org/about-us/newsroom/press-releases/2025/state-of-cybersecurity-2025-europe-press-release)

(15) European Commission, *State of the Digital Decade 2025* report, 2025 (https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2025-report).

(16) Bômont, C., 'Technical is political: When a cloud certification scheme divides Europe', Brief no. 26, EUISS, November 2025 (https://www.iss.europa.eu/publications/briefs).

(17) GLACY-e (https://global-threats.europa.eu/our-projects_en); Octopus (https://www.coe.int/en/web/cybercrime/octopus-project); EU CyberNet (https://global-threats.europa.eu/our-projects/eu-cybernet-ii-bridge-cybersecurity-eu_en).

euiss

Published by the European Union Institute for Security Studies.
Printed in Luxembourg by the Publications Office of the European Union.

Cover image credit: Based on Atul Vinayak/Unsplash

Publications Office of the European Union

PRINT ISBN 978-92-9462-504-5
CATALOGUE NUMBER QN-01-25-067-EN-C
ISSN 2599-8943
DOI 10.2815/1290225

WEB ISBN 978-92-9462-503-8
CATALOGUE NUMBER QN-01-25-067-EN-N
ISSN 2315-1110
DOI 10.2815/6124121