InvigoratEU

Invigorating Enlargement and Neighbourhood Policy for a Resilient Europe

Long Policy Report on a Common Framework for the Protection of Critical Infrastructure in the EU and its Neighbourhood

Authors

Ramūnas Vilpišauskas, Marts Ivaskis, Svitlana Chekunova, Danijela Jacimovic, Marco Siddi, Nana Tabagua, Teemu Tammikko

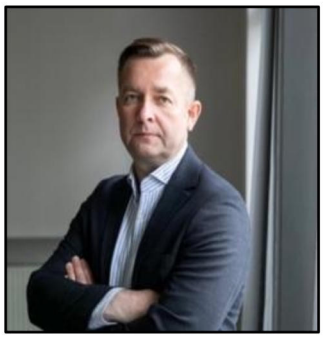
Funded by the European Union

Executive Summary

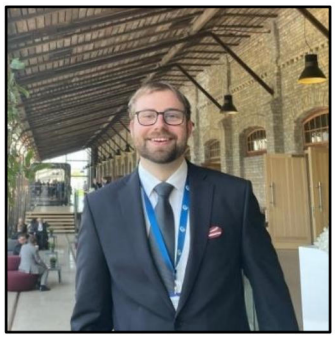
Long Policy Report on a Common Framework for the Protection of Critical Infrastructure in the EU and its Neighbourhood

The report provides detailed analysis of the evolution and exiting policies of the EU in the field of the critical infrastructure (CI) protection and resilience as well as structured assessment of how CI related policies are adopted and implemented in selected EU Member States and candidate countries. To structure the comparative analysis of the national policies and institutions it proposes an analytical framework based on the policy implementation and compliance with EU norms literature focusing on the threat landscape, policy and institutional context as well as incentives and capacities for implementing CI related policies. This allows to provide an assessment of the current state of CI related policies in three selected EU Member States and three candidate countries which is based on original material collected for the purpose of this report, including primary and secondary sources. The conclusions and recommendations section elaborates on the differences and similarities of national CI related policies as well as challenges and opportunities for their alignment taking into the functional needs originating from existing interdependencies as well as specificities of national contexts. They also illustrate the ways and means of further contributions of the EU, in particular, the European Commission in advancing the goals of CI related policies and their alignment in the enlarging EU and its neighbourhood.

Authors



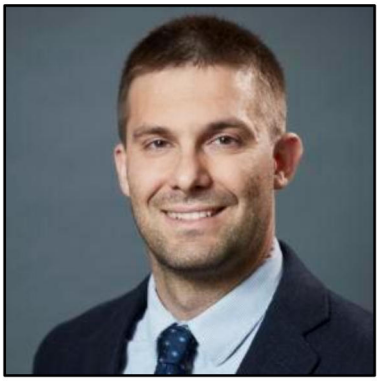
Ramūnas Vilpišauskas
Professor
Institute of International Relations and Political Science
Vilnius University



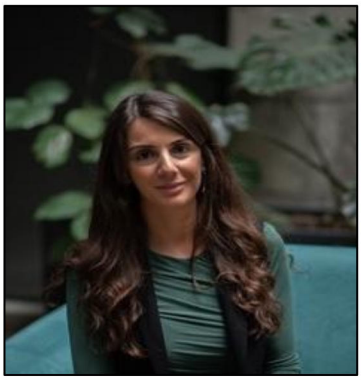
Marts Ivaskis
Researcher / Head of the European Union Research Programme
Latvian Institute of International Affairs (LIIA)

Svitlana Chekunova
Research Associate
The Razumkov Centre

Danijela Jacimovic
Professor
University of Montenegro (UoM)



Marco Siddi
Assistant Professor
Finnish Institute of International Affairs (FIIA)



Nana Tabagua
Lead Researcher
PMCG - Research

Teemu Tammikko
Senior Research Fellow
Finnish Institute of International Affairs (FIIA)

Approved by:

Funda Tekin, Director Institute for European Politics, Scientific Lead, InvigoratEU
Michael Kaeding, Professor for European Integration and European Union Politics at the Department of Political Science at the University of Duisburg-Essen, Germany, Project Coordinator, InvigoratEU

About InvigoratEU

InvigoratEU is a Horizon Europe-funded project, coordinated by the EU-Chair at the University of Duisburg-Essen (UDE) together with the Institut für Europäische Politik (IEP) in Berlin. The project, with a duration of 3 years from January 2024 until December 2026, examines how the EU can structure its future relations with its Eastern neighbours and the countries of the Western Balkans. The consortium has received around three million euros for this endeavour.

DOI 10.5281/zenodo.17630178

Funded by the European Union

About the project: www.invigorat.eu

Contents

1 Introduction

This policy report provides analysis of the evolution of the rules on the protection and resilience of critical infrastructure (CI) in the EU, its selected member states and candidate countries with a view to the need to align their policies and identifying the needs and opportunities to increasing connectivity between the EU and candidate countries.

It builds on the policy report D.7.1, which discussed the evolving threat landscape in the Europe, the turn among policy makers and analysts from policy focus on protecting CI to focusing on increasing its resilience as well as different challenges arising to CI in the EU and selected candidate countries, provision of vital services to society, state and methods of coping with those challenges. It thus provides the assessment of the most recent policy trends and pathways forward in the search for effective policy and institutional solutions in terms of aligning approaches of the EU Member States and candidate countries in facilitating integration of their economies and increasing their resilience in an increasingly hostile geopolitical environment.

As it will be discussed in the Chapter 2, the first EU-wide regulatory initiatives aimed at protecting and, more than a decade later, increasing the resilience of critical infrastructure emerged in response to terrorist attacks in the US and some European countries in early 2000s. Although the EU legislative initiatives at the time focused on the threat of terrorism as a priority to be addressed, they adopted an all-hazards approach to the protection of CI encompassing variety of threats ranging from man-made and technological to natural disasters.

The evolution of the EU norms on protection and resilience of CI presented in the Chapter 2 shows that during a decade the supranational norms were extended to cover more domains and increasingly more sectors in addition to shifting attention from protection to resilience. The expansion of the scope of CI regulatory policy has been motivated by the growing interdependencies between member states as well as different sectors and CI operators in the background of technological transformation and expanding landscape of threats. This functional spill-over was further complemented by geographical spill-over as candidate countries in the Western Balkans and, since geopolitical shock of 2022, Ukraine, Moldova and Georgia gradually aligned their policies with a view towards integrating into the EU, although at a different pace (and increasingly uncertain direction in the case of Georgia).

However, the evolution of the EU-wide policy on protection and resilience of CI was also partly motivated by the recognition of the evidence that actual application of common norms regulating CI and the provision of vital services in its member states continued to diverge. This points to the need to be attentive to national politics and the patterns of state-society relations, in particular, the perception of risks and threats since Russia's full-scale war against Ukraine and intensifying hybrid attacks against EU and NATO member states as well as competing external geopolitical influences in the candidate countries. Thus, the assessment of the current state of alignment with EU norms and their actual implementation in the EU member states and candidate countries should consider national context and factors, which influence how they actually regulate CI in practice.

For this purpose, the Chapter 3 develops an analytical framework based on the literature of policy implementation and compliance with EU norms. In addition to being attentive to the perception of threats, it proposes to focus on two sets of variables in the analysis of particular

countries' policies related to CI protection and resilience – incentives and capacities. They emphasized by the enforcement and management approaches used by scholars investigating divergent patterns of compliance with EU norms. These factors are discussed in more detail to provide an analytical basis for a systematic analysis of the state of affairs in this policy field in selected countries allowing to discover the main commonalities and differences and, thus, providing the ground for evidence-based policy proposals on aligning norms and practices.

Therefore, the Chapter 4 presents the systematic analysis of CI related policies and practices in selected EU member states and candidate countries. Those are EU members Finland, Latvia and Lithuania, which are "front-line" states in terms of their geography as well as intensity of hybrid attacks faced in recent years. Also three candidate countries are analysed – Montenegro, Ukraine and Georgia, which differ in terms of the perceived nature of threats, their state of integration with the EU and the state of transposition and implementation of EU norms. In terms of sectors, the analysis refers to the provision of vital services in two key sectors of CI – energy and communications including both physical and cyber domains and relevant policies of their protection and resilience. The sectors are chosen due to their relative importance in most countries covered here.

The report is based on the analysis of the relevant primary sources such as laws and other legal norms, security strategies (energy, cyber security, etc.), annual reports of relevant institutions, etc., and secondary sources such as available policy analyses and studies addressing those issues. They are supplemented by interviews with the key stakeholders in the ecosystem of CI protection and resilience such as policy-making and regulatory institutions, CI operators, relevant business associations, NGOs, experts.

This comparative analysis provides the basis for policy recommendations regarding existing discrepancies in terms of having a common EU wide framework, the explanatory factors behind them and suggestions on increasing convergence and interconnectivity. These recommendations are presented in the concluding chapter of the report.

2 Overview of the Evolution of EU-wide Framework

The Emergence of the EU-wide Framework on CI Protection

This chapter discusses the emergence of an EU-wide framework aimed at aligning policies of its Member States to protect and increase the resilience of CI both in physical and cyber domains. After presenting the initial legal norms adopted by the EU it then discusses the two most important recently adopted legal norms – the so-called CER Directive and NIS2 Directive, which had to be transposed by Member States by 17 October 2024.[1] They form the legal basis which should guide relevant policies of candidate countries as they align their legal norms in this policy area.

[1] At the time of writing, the dedicated EUR-LEX website showed that only 14 member states notified about the national legal norms which were adopted to transpose CER Directive (see https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32022L2557 (accessed 16.07.2025)) and 19 member states notified about national legal norms transposing NIS2 Directive (see https://eur-lex.europa.eu/legal-content/en/NIM/?uri=CELEX:32022L2555 (accessed 16.07.2025)).

The protection of critical entities and the infrastructure which they operate is considered to be one of the EU's most important security and resilience priorities.[2] These entities are considered important to the functioning of the internal market and its four freedoms as well as daily lives of European citizens through the provision of essential services. Disruptions to their functioning and provision of services can cause severe economic consequences, undermine public confidence, and impact the ordinary lives and security of citizens across the Union.

A formal EU-level approach on the protection of critical infrastructure can be traced back to the early 2000s, as a result of heightened security concerns following major terrorist attacks around the globe, such as those in the United States in 2001, Madrid in 2004, and London in 2005.[3] These attacks ended up highlighting the vulnerability of EU infrastructural systems, and the cross-border impacts they might present. For example, energy grids, transportation networks, financial systems, and digital communications infrastructure often cover multiple Member States. Therefore, a failure or disruption in one location could rapidly cascade, causing widespread disruption across the continent or a certain amount of Member States. This inherent cross-border character showed that, according to Article 5(3) of the Treaty on European Union (TEU) on the principle of subsidiarity, the EU could move forward with legislative proposals.

In 2004, the Commission published the Communication on "Critical Infrastructure Protection in the Fight against Terrorism"[4], and, in 2005, a Green Paper on a European programme for critical infrastructure protection[5], in which stakeholders were consulted on the choice of policy approach. The result was the proposal for a European Programme for Critical Infrastructure Protection (EPCIP), which aimed to create a common EU framework for identifying and protecting critical infrastructure.[6] Echoing the anxieties of the time, the initial proposal was largely focused on the prevention of terrorism. The EPCIP framework included several components: the legislative basis (which became the European Critical Infrastructures Directive), the establishment of a Critical Infrastructure Warning Information Network, the creation of specific expert groups, and dedicated funding mechanisms.[7]

Directive 2008/114/EC (ECI Directive)[8] was the first legislative step towards common European standards for the protection of European critical infrastructure. The overall objective of

[2] A 'critical entity' is an organisation designated by a Member State as essential for maintaining vital societal or economic functions, the disruption of which would have significant consequences.
[3] Anglmayer, Irmgard: European Critical infrastructure: Revision of Directive 2008/113/EC, European Parliamentary Research Service (EPRS), February 2021, p. 1, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf (accessed 10.10.2025).
[4] European Commission: Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism, COM/2004/0702, 2004.
[5] European Commission: Green Paper on a European programme for critical infrastructure protection, COM/2005/0576, 2005.
[6] European Commission: "The European Programme for Critical Infrastructure Protection", MEMO/06/477, 12 December 2006, available at: http://ec.europa.eu/commission/presscorner/detail/en/memo_06_477 (last accessed 05.09.2025)
[7] Ibid.
[8] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008., p. 75/82.

the ECI Directive, as laid down in the Article 1, was to establish a common procedure for the identification and designation of European Critical Infrastructures (ECIs) and to provide a common approach for assessing the need to improve their protection.

Article 2(a) of the ECI directive provides that, firstly, critical infrastructure is an "asset, system or part thereof located on EU territory, which is essential for the maintenance of vital societal functions, health, safety, security, economic or well-being of people, and the disruption or destruction of which would have a significant impact on at least two Member States, as result of the failure to maintain those functions." Meanwhile Article 2(b) defines an ECI as "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure". Therefore, the ECI Directive revolved around infrastructure with a cross-border element.

The ECI Directive also had a very narrow scope, limited to just two sectors: Energy and Transport.[9] Nuclear facilities were excluded, and while the potential future inclusion of the Information and Communication Technology (ICT) sector was mentioned in Article 3(3) and Recital (5) of the ECI Directive, it was not covered.

The Directive established specific mechanisms. For the identification and designation of ECIs, Articles 3 & 4 of the ECI Directive stated that Member States were responsible for identifying potential ECIs within their territory based on cross-cutting criteria (potential casualties, economic impact, public effects) and sector-specific criteria. Importantly, the formal designation of an infrastructure as an ECI involved a bilateral or multilateral process, where other potentially affected Member States would be notified and have opportunities to provide input.

After designation, the ECI Directive provided specific obligations for the operators of ECIs. Crucially, according to Article 5 of the ECI Directive, the owners or operators of ECIs had to develop an Operator Security Plan (OSP), which consisted of identifying assets, conducting risk assessments, and identifying security measures. Next to the OSP, each operator or owner of an ECI also had to designate a Security Liaison Officer (SLO) to act as a contact point between the ECI and the national authorities (Article 6 ECI Directive). Finally, Member States also had reporting obligations - providing the Commission with relevant information on risks, threats and vulnerabilities in the ECIs on the territory of the respective Member State (Article 7).

From the ECI Directive to CER Directive

During the 2010s multiple academic analyses, evaluations of the ECI Directive, and a Commission 2019 study on the ECI Directive identified that the impact of the ECI directive was limited and its implementation uneven.[10]

[9] Ibid. Annex I.

[10] European Commission: Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2 April 2019, available at: https://op.europa.eu/en/publication-detail/-/publication/118dcd3d-b041-11ea-bb7a-01aa75ed71a1/language-en (last accessed 05.09.2025).

The most significant failure of the ECI Directive was the extremely low number of infrastructures actually designated as ECIs across the EU. The requirement for bilateral agreement between Member States, while useful in theory, turned out to be cumbersome and politically sensitive, hindering the effective functioning of the designation process.[11] Furthermore, the restriction of the ECI Directive's applicability to only the Energy and Transport sectors became increasingly inadequate as threats evolved and the critical role of other sectors, particularly the ICT, become more apparent.[12]

As a result, the low number of designated ECIs meant that few new OSPs were developed, resulting in a low level of real improvement in security levels that could be actually attributed to the ECI Directive, begging the question of whether similar results could have been achieved with less intensive and binding means. Additionally, there were apparent gaps in the implementation of the ECI Directive, as practice varied significantly across Member States, undermining the idea of a 'common European approach'.

Finally, there was a fundamental shift in the approach towards critical infrastructure protection. 'Protection' was considered through the lens of traditional risk management in order to avoid and prevent unwanted events in certain critical infrastructure sectors.[13] Meanwhile, in academic debates, and also Horizon Europe research funding programmes, the debate moved away from just "protection" to the broader concept of "resilience", which observed the whole crisis management cycle.[14] This signalled the recognition that complete protection was not realistic and therefore in addition to protection measures have to be taken focusing on absorptive and adaptive capabilities in case of disruptions and recovery strategies.[15]

The necessity for reform can not only be attributed to the flaws in the ECI Directive, but also to a rapidly changing security and threat landscape. The nature, frequency and sophistication of threats continued to evolve beyond just terrorism. The 2010s saw a rapid increase in cyberattacks specifically targeting critical infrastructure, the frequency and impact of extreme weather events on critical infrastructure, and the emergence of hybrid threats. Furthermore, the ever-increasing level of digitalisation of all sectors, and the dependency on ICT services, meant that the ECI Directive essentially fell out of relevancy.

These reasons led to the European Commission drafting a Directive (EU) 2022/2557 on the Resilience of Critical Entities (CER Directive). The CER Directive entered into force on 1 January 2023, repealing the ECI Directive and currently constitutes the legal basis for aligning EU Member States' policies aimed at protecting and increasing the physical resilience of significantly expanded list of sectors assigned the status of CI.

---

[11] Ibid. p. 32 - 33.
[12] Ibid. p. 30.
[13] Christer Pursiainen/Eeero Kytömaa: From European critical infrastructure protection to the resilience of European critical entities: what does it mean?, in: *Sustainable and Resilient Infrastructure*, vol. 8 (sup1), 2022, p. 85-101; see also European Commission: Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2 April 2019, p. 28.
[14] See for a more extended discussion Ramūnas Vilpišauskas et al.: D.7.1 long policy report on the rules alignment of protecting critical infrastructure in interdependent states, 2025, available at: http://invigorat.eu/wp-content/uploads/2025/03/D7.1_InvigoratEU_long-policy-report_public.pdf (last accessed 05.09.2025).
[15] Ibid.

The CER Directive aims to reduce vulnerabilities and strengthen the physical resilience of 'critical entities' against a wide array of risks. The Directive has a much larger scope than the ECI Directive, applying to critical entities within eleven specified sectors: 1) energy; 2) transport; 3) banking; 4) financial market infrastructures; 5) health; 6) drinking water; 7) wastewater; 8) digital infrastructure; 9) public administration; 10) space; and 11) food.

The CER Directive takes a more holistic approach to critical entities' protection, requiring Member States to adopt a national strategy for enhancing critical entity resilience, and conduct regular risk assessments, covering relevant natural and man-made risks, including cross-border and cross-sectoral ones (the first strategy and risk assessments are due by 17 January 2026).

Following the national strategy and the risk assessments, Member States, within 6 months, need to identify critical entities, using relevant identification criteria. For example, whether the entity provides one or more essential services, operates critical infrastructure in the Member State, and whether an incident would have significant disruptive effects. The Commission in this regard has established a non-exhaustive list of essential services to aid the process of identification.

Once critical entities have been identified, Member States should: 1) designate one or more competent authorities responsible for supervising the Directive's application and ensure that the respective authorities have the necessary powers and resources, including, but not limited to the right to conduct inspections and the right to impose penalties for non-compliance; 2) provide support through guidance such as best practices, training and simulations or exercises; and 3) establish rules for critical entities to conduct background checks on personnel in sensitive positions.

Meanwhile, critical entities also have a set of obligations that have to be implemented within 10 months of being notified of their designation as a 'critical entity' by the respective Member State. Firstly, critical entities also have to conduct individual risk assessments at least once every four years. Secondly, on the basis of the risk assessment, critical entities have to take the appropriate and necessary technical, security, and organisational measures to ensure their resilience. All of the taken measures need to be documented in a resilience plan. Thirdly, in case of any incident that significantly disrupts or has the potential to significantly disrupt the provision of essential services, the critical entity must notify the competent authorities without undue delay.

Furthermore, critical entities can also be identified as being of 'particular European significance', where the respective critical entity provides essential services in or for six or more Member States. In this case, the entities may be subject to advisory missions organised by the Commission to assess their resilience plans and risk assessments.

In parallel to the obligations for Member States and critical entities, the CER Directive also establishes the Critical Entities Resilience Group (CERG), chaired by the Commission and composed of Member States representatives. CERG aims to facilitate cooperation, the exchange of information, and the development of best practices related to the resilience of critical entities. However, the effectiveness of such an institutional mechanism will largely depend on the degree of commitment and information-sharing by Member States. The CERG's advisory and

coordination mandate, unlike mechanisms in other EU policy areas – such as ENISA's operational role in cybersecurity – lacks counterbalance through formal enforcement or supervisory powers. This limits its ability to ensure consistency across Member States and to address persistent asymmetries in national capacities. Nonetheless, if effectively used as a platform for peer learning and joint risk assessment, the CERG could evolve into a central forum for building trust, enhancing transparency, and exchanging best practices between Member States.

Evolution of EU-wide Policies in Cyber Security – from NIS1 to NIS2

As previously mentioned, the 2010's saw a rapid increase in cyberattacks, which had a strong cross-border element, as evidenced by the interconnectedness and interdependence of EU systems, services and entities. The NIS1 Directive was the first EU level instrument aimed at the protection of network and information systems across the Union.[16] The NIS1 Directive set out minimum cybersecurity requirements for 'operators of essential services' (OES), digital service providers (DSP), and Member States. OES were essentially entities operating in critical sectors such as energy, transport, banking, financial market infrastructure, healthcare, drinking water supply, and digital infrastructure, while DSPs concerned online marketplaces, online search engines, and cloud computing services. The NIS1 Directive offered broadly two categories of obligations: 1) safeguarding obligations, which require organisations to put in place "appropriate and proportionate" security measures, and 2) information obligations, which require the sharing of disclosure of information.

Similarly to the ECI Directive, implementation proved to be difficult and resulted in a wide amount of fragmentation across Member States. However, there were plenty of other issues with the NIS1 Directive outlined in a Commission Staff Working Document attached to the NIS2 Directive proposal.[17] Essentially, the NIS1 Directive "fell short of ensuring a fully engaging, coherent and pro-active setting that could guarantee an effective take of shared responsibilities and trust among all relevant authorities and businesses [...] The NIS1 Directive revealed inherent weaknesses and gaps that make it incapable of addressing [..] cybersecurity challenges. These concern [..] a lack of clarity on the NIS1 scope, insufficient consideration of the increasing interconnectivity and interdependencies within EU economies and societies, the lack of alignment between security requirements and reporting obligations, a lack of effective incentives for information sharing or operational cooperation among relevant authorities and difference in treatment of comparable businesses across Member States and sectors."[18] Therefore, to alleviate those gaps in the scope of the NIS1 Directive, to remove discretionary Member State power, and to strengthen supervision and enforcement powers, the NIS2 Directive was proposed.

[16] Robert Mikac: Protection of the EU's Critical Infrastructures: Results and Challenges, in: Applied Cybersecurity & Internet Governance, vol. 2, no. 1, 2023.
[17] European Commission: Commission Staff Working Document – Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, SWD/2020/345 final – part 1/3, 2020.
[18] Ibid.

The NIS2 Directive,[19] which entered into force in January 2023, repeals and replaces the first NIS Directive (EU) 2016/1148.[20] The NIS2 Directive aims to achieve a high level of cybersecurity across the Union, and it achieves this through significantly expanding the scope of entities covered by the Directive, strengthening cybersecurity risk management requirements and incident reporting obligations.

The scope of the NIS2 Directive has a sectoral element and a size element. Firstly, according to Article 2 of the NIS2 Directive, entities covered by the aforementioned Directive generally include medium-size and large organisations. The NIS2 Directive defines medium-size and large organisations as 1) employing 50 or more people and having an annual turnover or balance sheet exceeding 10 million EUR; or 2) employing over 250 individuals regardless of financial considerations;[21] although smaller entities can also be included by Member States, where they identify a high-security risk profile. Furthermore, certain types of entities such as trust service providers, DNS providers and some other parts of the digital infrastructure sector are covered regardless of size.

Secondly, the NIS2 Directive categorizes entities into two main groups: 'essential entities' and 'important entities', reflecting the extent to which they are critical as regards their sector. Essential entities are covered by Annex I of the NIS2 Directive ('Sectors of high criticality') and include the following sectors: Energy; Transport; Banking; Financial market infrastructures; health; drinking water; waste water; digital infrastructure; ICT service management; public administration; space. Meanwhile 'Important entities' are covered by Annex II of the NIS2 Directive ('Other critical sectors') and include the following sectors: Postal and courier services; waste management; manufacture, production and distribution of chemicals; production, processing and distribution of food; manufacturing; digital providers; and research.

The requirements for Member States are by-and-large similar to the previous NIS1 Directive. Article 7 of the NIS2 Directive requires Member States to adopt and implement a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures with the aim of ensuring and maintaining a high level of cybersecurity. Furthermore, as required by Article 8 of the NIS2 Directive, Member States also have the responsibility to designate or establish one or more competent authorities responsible for cybersecurity and supervisory tasks and to establish a single point of contact, which would ensure cross-border cooperation. Article 9 of the NIS2 Directive requires Member States to designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises, while Article 10 of the aforementioned Directive requires that Member States also designate or establish one or more Computer security incident response teams (CSIRTs) that are responsible for risk and incident handling.

---

[19] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ L 333, 27.12.2022., p. 80. - 152.

[20] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016., p. 1. - 30.

[21] Article 2(1) of Annex I to the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-size enterprises OJ L 124, 20.5.2003, p. 34/41.

It should be noted that the competent authorities under Article 32 of the NIS2 Directive have had their supervisory and enforcement powers strengthened to, for example, conduct audits, on-site inspections, request information and perform security scans, as well as strengthening the administrative fines that can be imposed against 'essential' or 'important' entities in breach of the NIS2 Directive.

However, the obligations for entities covered by the scope of the NIS2 Directive are substantially different, when compared with the Directive's predecessor. Importantly, Article 21 of the NIS2 Directive requires that essential and important entities implement appropriate and proportionate technical, operational, and organisational measures to manage risks to their network and information systems. Article 21 of the NIS2 Directive also lists 10 baseline measures that all entities must implement, for example, incident handling procedures, basic cyber hygiene practices, human resources security, supply chain security, and more.

The NIS2 Directive continued to build on reporting obligations under the NIS1 Directive. Article 23 of the NIS2 Directive requires that entities notify the competent authority or the CSIRT of any 'significant incident' without undue delay through a multi-stage process: 1) an early warning (within 24 hours) when the entity becomes aware of an incident; 2) the incident notification (within 72 hours), providing an initial assessment of the incident; 3) an intermediate report, where requested by the national authority or the CSIRT; and, finally, 4) a final report (within one month), providing detailed information of the likely root cause, the necessary mitigation measures and the evaluated cross-border impact of the incident.

What is also important is that the NIS2 Directive creates a liability regime for the management bodies of the essential and important entities falling under the scope of the Directive, where they have not taken the necessary steps to approve and introduce cybersecurity risk management measures or failed to oversee the effective implementation of the aforementioned measures.

The Symbiotic Nature of the CER and NIS2 Directives and Potential Challenges to their Implementation

The CER Directive and NIS2 Directive, while tackling different types of threats, are complementary by their nature. Firstly, many entities operating critical infrastructure are very likely to be identified as both a 'critical entity' under the CER Directive and an 'essential' or 'important' entity under the NIS2 Directive. Secondly, The framework acknowledges that cyber risks covered by the NIS2 Directive and physical risks covered by the CER Directive are often linked. Cyberattacks can cause physical damage or disruption (e.g., manipulating industrial control systems), while physical events (e.g., power outages, natural disasters) can disable critical IT systems. The NIS2 Directive's requirement for an "all-hazards" approach to critical infrastructure related risk management implicitly requires entities to consider the potential physical consequences of cyber incidents. Meanwhile, CER's focus on overall resilience also requires ensuring the continuity of services even when supporting digital systems are impacted by physical events. Thirdly, both the CER and NIS2 Directives require cooperation and the regular exchange of information between the national competent authorities designated in the respective Member State under CER Directive and those designated under NIS2. Finally, there are what could be considered as 'external bridging measures' for the functioning of both directives. For example, the EU Critical Infrastructure Blueprint aims to provide a framework for

coordinating the EU-level response to significant cross-border disruptions to critical infrastructure, regardless of whether the trigger is physical or cyber. [22]

It should be noted that the implementation of NIS2 and CER Directives will present new challenges for the relevant industries in both EU Member States and candidate countries. Firstly, 'critical entities' under the CER Directive and 'essential' or 'important' entities under the NIS2 Directive that have been brought into the scope of the regulatory framework *will need to make large investments to strengthen both their physical security and cybersecurity*. While certain entities might be well-versed in some of those practices, they might lack the necessary know-how and experience in implementing cyber risk management systems and incident reporting protocols as well as expertise and resources to upgrade their physical security and resilience policies in the face of changing threats, for example, acts of sabotage or potential civilian drone attacks.

Second, the requirements set by new EU legislation might be particularly challenging *for companies operating in several EU Member States once they implement those common norms within their specific national legal and institutional context possibly leading to different requirements*. For example, under the NIS2 Directive a company operating in three different Member States might have to fulfil strict reporting obligations to be prepared for cyber incidents and attacks in those three Member States that might have differently implemented requirements. This could lead to operational inefficiencies.

Third, the NIS2 Directive, according to Articles 21(2)(d) and 21(3) requires 'essential' and 'important' entities to implement "a supply chain security policy which governs the relations with their direct suppliers and providers".[23] This requirement could prove to be very difficult to fulfil, especially for medium-sized companies, which *have not had experience in supply-chain monitoring*. Furthermore, this requirement could have spill-over effects, artificially extending the scope of the NIS2 Directive to SMEs, which do not directly fall under the scope, but are forced to implement extensive and heightened security measures to remain part of the supply chain with entities falling under the scope of the NIS2 Directive.

Meanwhile, it seems that the largest difficulty with the CER Directive will still concern *preventing the fragmentation of Member State and critical entity practices*. While Article 4 of the CER Directive requires Member States to develop national strategy plans and risk assessments, Member States might have different interpretations and standard systems to measure the resiliency of 'critical entities', as well as what falls under that definition.[24] Differing technical standards or lack thereof in the absence of clear rules could lead to gaps in implementation

[22] Council recommendation of 25 June 2024 on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance OJ C, C/2024/4371, 5.7.2024.
[23] ENISA: Implementing Guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures, October 2024, p. 57.
[24] Marcos J. Alexopoulos, Arto Niemi, Bartosz Skobiej, Frank Sill Torres: Examination of the Critical Infrastructure Resilience Directive from the Maritime Point of View, in: Journal of Common Market Studies, vol. 63, 2025, p. 667-678, https://doi.org/10.1111/jcms.1368.

of the CER Directive, leading to companies taking decisions on ensuring resiliency based on cost-efficiency rather than effectiveness.[25]

Finally, it should be noted that while the NIS2 Directive and the CER Directive are arguably the most notable and most directly concerned legislation on the protection and resilience of critical infrastructure, there are other legislative and non-legislative mechanisms within the EU that are connected to this policy field. One such example is Regulation 2019/941 on risk-preparedness in the electricity sector, which provides a system for Member States to assess risks and identify possible electricity crisis scenarios. [26] In that regard, the Directive requires Member States to prepare national risk-preparedness plans and strengthens cross-border cooperation.

Similarly, Regulation 2017/1938 on gas supply security[27] also requires Member States to conduct risk assessments and develop preventive action and emergency plans in crisis situations, as well as strengthening Member State solidarity and cooperation. Furthermore, the protection of critical infrastructure is not limited to legislative acts, but also strategy documents. For example, the EU Security Union Strategy 2020 – 2025, EU Preparedness Union Strategy and the EU Counter-Terrorism Agenda, as well as the EU Toolbox on 5G Security are all important frameworks, strategies and approaches that impact the protection of critical infrastructure in the European Union.

Conclusion

The emergence of the EU-wide framework for the protection of CI reflects a gradual evolution from fragmented national measures to a coordinated, harmonised European approach, which is based on shared security and resiliency objectives. The initial framework, born out of post-9/11 counter-terrorism concerns, laid the groundwork for identifying and protecting assets, which could affect multiple Member States, if they were to be disrupted. However, the ECI Directive was limited in scope both conceptually and regarding the covered sectors.

As the EU continued developing, the increasing interconnectedness of sectors, the evolving digital interdependencies, and the growing complexity of hybrid and cyber threats revealed the need for a broader and more adaptive policy framework. The development of the subsequent CER and NIS2 Directives marks a maturation of the common European approach, moving away from a focus on the protection of specific CI, to a more comprehensive system aimed at ensuring the resilience of CEs, not only against counter-terrorism and physical threats, but against all hazards, both physical and digital.

In essence, the EU framework for the resilience of CI has evolved from reactive, sector-specific measures to an integrated resilience-based strategy. This transformation underscores a shift

[25] Ibid.
[26] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, OJ L 158, 14.6.2019. p. 1 – 21.
[27] Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010. OJ L 280, 28.10.2017, p. 1 – 56.

in the Union's understanding of security. At the same time, as noted above, it also raises important challenges in terms of aligning CI policies among countries and their practical implementation.

3 The Analytical Framework for Assessing the Current State, Challenges and Ways for Improving the Alignment of CI related Policies in selected EU Member States and Candidate Countries

The Literature on Policy Implementation and EU Compliance

The evolution of the EU-wide norms on protection and resilience of CI shows that during the last 10-15 years the supranational norms were extended to cover more domains (physical and cyber) and increasingly more sectors (from two to six to eleven) in addition to shifting attention from protection to resilience. The expansion of the scope of CI regulatory policy has been presented by the European Commission as motivated by the growing interdependencies between Member States as well as different sectors and CI operators in the background of technological transformation and expanding landscape of threats.

According to scholars following these policy developments, they seem to fit three different, but compatible accounts of European integration: (neo)functionalist integration which takes place in response to the functional demands of economic entities and member states in response to growing cross-border interdependences, technological developments and changing external threats; European "multi-level governance" with different competencies being assigned to different levels of governance while member states guard their national security competencies and at the same time aim to increase protection and resilience of CI in a coordinated way; and "principle-agent approach" when member states decide to delegate certain functions to the European Commission because it has relevant expertise and better equipped to deal with information asymmetries.[28] Moreover, one could add that after the revival of the EU enlargement agenda by the Russia's unprovoked full-scale war in 2022, this functional spill-over is in the process of being supplemented by geographical spill-over as prospective members align their CI policies with above discussed EU norms.

However, the conclusion that this regulatory evolution "attests to increasing regulation of the CI sector, both deepening and widening the supranational tendencies in this field" has been so far based on the assessment of the regulatory norms adopted on the EU level.[29] In other words, as it is well know from the implementation studies in political science generally and from the compliance studies within the EU member states more concretely, the same EU norms can be transposed and implemented differently in different member states. This has also been

[28] Christer Pursiainen/Eero Kytomaa: From European critical infrastructure protection to the resilience of European critical entities: what does it mean? In *Sustainable and Resilient Infrastructure*, 8 (1), 2022, p. 95-96.
[29] Christer Pursiainen/Eero Kytomaa: From European critical infrastructure protection to the resilience of European critical entities: what does it mean? In *Sustainable and Resilient Infrastructure*, 8 (1), 2022, p. 97.

the case with the ECI Directive and NIS Directive, as noted above in the discussion of the arguments provided by the European Commission for the need to upgrade the EU legislative framework. Besides, as studies of the CI policies in the Baltic States (and Norway) illustrate, even countries with such a similar threat perception and recent history of institutional reforms as well as EU and NATO accession as Estonia, Latvia and Lithuania can have rather different approaches to protecting CI.[30]

All of the above-mentioned studies, however, do not systematically analyse the causes of the divergence of CI protection policies in the EU member states. This policy report aims to fill this gap in advancing the knowledge of CI policy implementation and coordination issues which so far have been mostly assessed from the technical and engineering perspectives.[31] Analyses of how threat perception is translated into CI protection and resilience policy, how it interacts with the adoption of the EU-wide framework and which factors affect the implementation of these policy measures within selected EU member states as well as candidate countries could provide useful academic and policy relevant insights into advancing our understanding of this policy area and the alignment of functional needs originating from interdependencies with national policies and politics. This could also shed more light on the differences between protecting and enhancing resilience of information (cyber) infrastructure compared to physical infrastructure.

There is a rich body of literature which has been developed during the recent decades on policy implementation and compliance with EU norms. Originating from the US in 1970s, the studies of policy implementation pointed to the importance of paying closer attention to what happens after policy decisions are made and legal norms are adopted, pointing to the ample evidence that implementation results, outputs and outcomes deviate from those initially intended.[32] The policy implementation studies focused on conditions of efficient and effective implementation pointing to the importance of clearly defined policy goals and objectives, and the agreement regarding them between participating institutions and stakeholders, proper causal theory to guide the choice of policy measures, proper institutional structure allowing to avoid overlaps of responsibilities, coordinate and communicate effectively as well as learn from implementation experience, adequate resources (personnel, funding, expertise, time) and taking into account external factors such as changing technological, political, economic and social circumstances.[33] These insights have been later used in studying implementation of the

[30] Maris Andžans/Andris Sprūds/Ulf Sverdrup (eds.): *Critical Infrastructure in the Baltic States and Norway: strategies and practices of protection and communication*, Latvian Institute of International Affairs, 2021.

[31] See, for example, Tim Prior: *Measuring Critical Infrastructure Resilience: Possible Indicators,* Risk and Resilience Report 9, Centre for Security Studies (CSS), ETH Zurich, 2014; Roberto Setola/Eric Luiijf/Marianthi Theocharidou: Critical Infrastructures, Protection and Resilience, in: Roberto Setola et al. (eds.) *Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach.* SpringerOpen, 2016; European Commission: European Reference Network for Critical Infrastructure Protection: ERNCIP Handbook 2018 edition, Joint Research Centre Technical report, 2018.

[32] In this respect the full title of the study which initiated policy implementation debates is very instructive – Jeffrey L. Pressman/Aaron Wildavsky: *Implementation. How great expectations in Washington are dashed in Oakland; or, why it's amazing that federal programs work at all, this being a saga of the economic development administration as told by two sympathetic observers who seek to build morals on a foundation.* University of California Press, 1973.

[33] See Brian W. Hogwood/Lewis A. Gunn: *Policy analysis for the real world.* Oxford University Press, 1984; Daniel A. Mazmanian/Paul A. Sabatier: *Implementation and Public Policy.* Bloomsbury Academic, 1989;

EU norms within the multi-level polity, especially since early 1990s as European integration advanced with the relaunching of the Single market project, Economic and monetary union and various regulatory policies aimed at dealing with externalities crossing borders and growing interdependencies.[34]

The EU compliance studies have focused on the implementation of EU norms, often pointing to the uneven record of transposition and investigating possible causes of the uneven practices. Some studies, representing state-based explanations, linked the difficulties in EU member states' compliance and implementation of EU norms to the lack of administrative capacities, for example, government inefficiency or corruption.[35] Other state-based explanations pointed to the importance of national public opinion and argued that higher support for European integration facilitates implementation of EU norms.[36] The non-compliance has also been explained by high institutional misfit between the EU-wide norms and national status quo as well as preferences or beliefs held by domestic, political, administrative and social actors.[37]

Other research found that non-compliance resulted from national preferences when they were ignored during the stage of negotiations of particular directive as an incentive to deviate from it during the process of implementation as well as the amount of discretion granted to member states.[38] Furthermore, examining large data sets of detected violations of EU legal norms authors assessed several dominant explanations proposed by enforcement, management and legitimacy approaches and concluded that powerful EU member states tend to violate EU law more often while best compliers are small countries with efficient bureaucracies.[39] The related stream of EU external governance studies found that the effectiveness of EU rules transfer to

---

Paul A. Sabatier: Top-Down and Bottom-Up Approaches to Implementation Research: a Critical Analysis and Suggested Synthesis, *In Journal of Public Policy*, 6(1), 1986, p. 21-48.

[34] For an example of the discussion of the factors of successful policy implementation inspired by implementation studies in the context of implementing EU norms see Dionyssis Dimitrakopolous/ Jeremy Richardson: Implementing EU public policy, In Jeremy Richardson (ed.) *European Union. Power and Policy-making*, Routledge, 2nd edition, 2001, p. 335-356.

[35] See Carmel Coyle: Administrative capacity and the implementation of EU environmental policy in Ireland, in *Regional Politics and Policy*, 4, 1994, p. p. 62-79; Geoffrey Pridham: National environmental policy-making in the European framework: Spain, Greece and Italy in comparison, in *Regional Politics and Policy*, 4, 1994, p. 80-101; Heather Mbaye: Why national states comply with supranational law: explaining implementation infringements in the European Union, 1973-1993, in *European Union Politics*, 2, 2001, p. 259-81.

[36] Peter Lampinen/Petri Uusikyla: Implementation deficit - why member states do not comply with EU directives, in *Scandinavian Political Studies*, 21, 1998, p. 231-251.

[37] See Christoph Knill/Andrea Lenschov: Coping with Europe: the impact of British and German administrations on the implementation of EU environmental policy, In *Journal of European Public Policy*, 5(4), 1998, p. 595-614; Christoph Knill/Dirk Lehmkuhl: The national impact of European Union regulatory policy, in *European Journal of Political Research*, 41(2), 2002, p. 255-280; Viktoria Brendler/Eva Thomann: Does institutional misfit trigger customisation instead of non-compliance? In *West European Politics*, 47(3), 2024, p. 515-542.

[38] See Robert Thomson/Rene Torenvlied/Javier Arregui: The Paradox of Compliance: Infringements and Delays in Transposing European Union Directives, in *British Journal of Political Science*, 37, 2007, p. 685-709.

[39] Tanja A. Borzel/Tobia Hofmann/Diana Panke/Carina Sprungk: Obstinate and inefficient: why member states do not comply with European law, in *Comparative Political Studies*, 43(11), 2010, p. 1363-1390.

candidate countries depended on the credibility of EU conditionality and the domestic costs of rule adoption.[40]

As the EU enlarged, in particular with the "big bang" enlargement into Central and Eastern Europe in 2004-2007, increasingly more attention has been devoted to the compliance with EU norms in "old" and "new" member states or extending existing classifications of EU member states on the basis of their record of compliance to Central and Eastern European countries. The main finding was that most "new" member states, especially Baltic countries, showed relatively positive record of compliance, generally far better than most "old" member states.[41] It was hypothesized that it might be explained by a greater susceptibility of new member states to naming and shaming by the European Commission and an institutional investment in legislative capacity (although in some Central European states such as Hungary or Poland the compliance with EU law, including the principle of the rule of law, has become a matter of controversy since 2010s-2015s highlighting the importance of shifting domestic political incentives).

Other scholars argued that surprisingly good compliance record of recently acceded EU member states might be an outcome of the difference between purely formal compliance and actual non-compliance in practice ("the world of dead letters"), which was, however, more difficult to assess.[42] Others came to the conclusion that neither this, nor other dominant approaches of enforcement, management and legitimacy could convincingly explain why Central and Eastern European countries showed better compliance record compared to other EU member states.[43] They hypothesized that pre-accession conditionality could explain why these new member states performed so well. However, this explanation could be linked back with factors emphasized by enforcement and management approaches, as pre-accession conditionality forms strong incentives for candidate countries to comply with EU norms in order to advance in their process of accession into the EU – of course, provided that there is a domestic political consensus on the goal of EU membership – and, at the same time, they benefit from EU technical and financial assistance measures aimed at improving their administrative capacities to comply with EU norms .

The Alignment of CI related National Policies – Guide for Analysis

This section presents the analytical framework for the qualitative analysis of implementing CI related policies, especially their alignment with EU-wide norms, in selected EU member states and candidate countries based on the above reviewed studies. It adopts the argument proposed by Jonas Tallberg that compliance with international regulatory agreements can be best achieved when two approaches of enforcement and management are combined to make

[40] Frank Schimmelfennig/Ulrich Sedelmeier: Governance by conditionality: EU rule transfer to the candidate countries of Central and Eastern Europe, in *Journal of European Public Policy*, 11(4), August 2004, p. 661-679.
[41] Ulrich Sedelmeier: After conditionality: post-accession compliance with EU law in East Central Europe, in *Journal of European Public Policy*, 15(6), September 2008, p. 806-825.
[42] Gerda Falkner/Oliver Treib: Three worlds of compliance or four? The EU-15 compared to new member states, in *Journal of Common Market Studies*, 46(2), 2008, p. 293-313.
[43] Tanja A. Borzel/Ulrich Sedelmeier: Larger and more law abiding? The impact of enlargement on compliance in the European Union, in *Journal of European Public Policy*, 24 (2), 2017, p. 197-215.

them more effective.[44] In other words, *enforcement, which focuses on the calculus of actors, whether it pays-off to comply with particular norms seeing it as a matter of incentives*, and *management, which sees compliance failures as originating from then lack of capacities (i.e. lack of information, expertise, funding)* are seen as complimentary rather than alternative approaches.

Although it is not the objective of this policy report to come up with comparative assessment of which countries comply with CI norms most, the analysis of the factors seen as relevant for the effective compliance can provide important material in advancing our understanding of the state of CI protection and resilience in the EU and candidate countries and the factors behind it.

First, however, drawing on the policy implementation literature which underlines the *agreement of the participating institutions and stakeholders on policy* as well as taking into account the importance of *threat (or risk) perception* for the implementation of CI related policy measures, it points to the need to be attentive to how they are outlined in the relevant national policy documents, strategies and other legal norms. The evidence of alignment of views regarding threats to CI – arguably a key precondition for the agreement on the goals such as CI protection and resilience – and policies aimed at mitigating or managing them among the key participants in the CI related policy subsystem on supranational, national and micro levels should signal conditions conducive to effective policy implementation.

Second, it is important to assess *the institutional context of CI related national policy formation and implementation*: how are the institutional roles and responsibilities defined, are there overlaps or gaps in terms of national coordination and communication processes, how learning takes place. These sets of *policy and institutional characteristics* should be outlined before moving to the discussion of incentives and capabilities to implement CI related policy measures as proposed by the enforcement and management approaches.

Third, the *factors stressed by the enforcement and management approaches* should provide a more nuanced discussion of the current state of CI policies in the selected countries, challenges they face and directions to increase their effectiveness. The enforcement approach, focused on *the structure of incentives,* stresses coercive strategy of *monitoring and sanctions* and should direct attention to the instruments that both European Commission and national regulatory authorities monitoring compliance with CI protection and resilience norms use with respect to operators/owners of critical infrastructure. It should be guided by the analysis of how monitoring procedures of risks assessments, designating responsible officers, reporting, conducting exercises, etc. are outlined and practically applied in particular country both with respect to physical CI and information CI (cyber), acknowledging that in practice both are interrelated. It should also assess the use of sanctions when non-compliance is detected – what types of sanctions are used by the EU and national institutions, are they consistently applied in practices, etc. It should be noted, that EU incentives and sanctions vary depending on whether the country is an EU member state or candidate country, as discussed by the literature on conditionality of EU accession.

[44] Jonas Tallberg: Paths to Compliance: Enforcement, Management and the European Union, in *International Organization*, 56 (3), summer 2002, p. 609-643.

Meanwhile management approach with its focus on *capabilities* stresses the importance of *capacity (administrative resources and expertise) building, rule interpretation and transparency*. This problem-solving approach focuses on technical assistance and advice with technical matters such as the methodologies of risk assessment, learning through joint exercises with partner countries, building trust between state and private actors. Again, the country analysis should allow to compare which types of problem-solving instruments are employed by the EU and national authorities, how they compare between different EU Member States as well as Member and candidate countries, how operators/owners assess the usefulness of those instruments and what do they lack.

The comparative analysis of factors outlined by each of those two approaches combined should allow to identify constraints and trade-offs faced by the authorities and operators/owners of critical entities and possible ways of improving the protection and resilience of CI from public policy perspective and coordination within the EU (and partner countries). Importantly, as noted above, the analysis should be based on the assessment of local (national) threat perceptions, including threats posed by Russia and other hostile actors, as well as corresponding measures to improve protection and resilience of CI and how these measures align with the relevant EU norms or are transformed during their transposition and practical implementation. The importance of external factors on the implementation of particular public policies has been stressed by implementation studies for a long time but it is even more relevant for the analysis of implementing CI policies since the latter explicitly aim at minimising the impact of potential threats.

The analysis based on the above presented framework should also allow to assess the challenges related to the practical implementation of CER and NIS2 directives discussed in the section 2.4 of this report. Attention to institutions and policies as well as incentives and capabilities should allow to provide a more nuanced picture of the need for additional resources and the trade-off between cost-efficiency and effectiveness of CI protection and resilience policies as well as persistence of fragmentation between national CI policies as applied by countries' authorities and CI operators.

To be sure, there are important constraints to such qualitative national analyses which should be outlined at the outset. One has to do with the fact that EU legal norms, which should refocus CI policies of EU member states from protection to resilience, have been only recently adopted and currently are being transposed. The CER and NIS2 Directives are only now being implemented and some of their provisions should be put into practice only in the coming years. This issue of the moving target is even more acute for candidate countries which, depending on their progress in adopting EU norms, are in the early stage of the CI policy alignment.

Even more complexity is added by another moving target – constantly evolving landscape of threats as illustrated by the debates focusing on the undersea incidents affecting electricity and communications cables in the Baltic Sea in winter 2024-2025 and in summer 2025 on the need for improved protection against drones in EU/NATO Eastern flank countries.

However, while these constraints are important, there is already a decade of experience with EU member states having in place national CI protection policies and a patchwork of measures which aim at protecting CI in all candidate countries. Therefore, analysis of primary and secondary sources (i.e. national security strategies, public statements, annual reports of respon-

sible authorities, etc.) as well as interviews with stakeholders from sectoral business associations and experts, who are easier accessed than officials, guided by the questions informed by the literature on policy implementation and compliance studies can provide original and policy relevant insights.

It should also be noted, that national policies of CI protection and resilience are often subject to confidentiality constraints and limits on information provided to the public and researchers due to national security concerns. This has indeed turned out to be an obstacle signalled by the authors of several country studies presented below, limiting their possibilities to conduct interviews with officials, regulators and operators of CI entities.

The comparative analysis of the CI protection and resilience policies in response to external threats and EU norms and their implementation will focus on three EU member states, i.e. Finland, Latvia and Lithuania as well as three candidate countries, which are all in different stages of their integration into the EU – Montenegro, Ukraine and Georgia. Although the limited length of the policy report does not allow to go deeper into analysis of particular CI sectors, the country studies will refer energy and communications sectors, allowing to assess CI policies with respect to both physical and informational/digital CI protection and resilience, taking into account national specificities.

Thus, each of the country case study presented below follows a common structure and analytical framework by, first, discussing the (perception of) threats in the respective country and their evolution in recent years, then, outlining the institutional and policy context, relevant from the point of view of CI protection and resilience, and, finally, assessing the changes and challenges related to incentives and capacities of further strengthening CI resilience .

4 The Analysis of CI related Policies in Selected EU Member States and Candidate Countries

Finland

Threat landscape

Finland is subject to low level of risks related to natural disasters, although its harsh climate does pose certain challenges to critical infrastructure objects, their surveillance and protection. Preparations for these well-known and long-standing 'natural' risks have existed for a long time; they have recently been complemented and adapted to the changing environmental situation, for instance by the National Climate Change Adaptation Plan 2030.[45]

Regarding the man-made hazards, the situation is somewhat different and in flux. Intentional actions targeting critical infrastructure – like sabotages, terrorism, or hybrid interference – are likely. Terrorist attacks targeting critical infrastructure are rare, but there have been waves of

[45] Ministry of Agriculture and Forestry of Finland: National Climate Change Adaptation Plan 2030, 2 April 2024, available at: https://mmm.fi/en/nature-and-climate/climate-change-adaptation/national-climate-change-adaptation-plan-2030 (last accessed 24.10.2025).

violent extremism in the recent past with attacks on railway networks and road logistics,[46] and it is not impossible that they could be repeated. Hybrid interference stemming from Russia is frequent and has taken many forms even prior to 2022 and Finnish accession to NATO. Between 2023 and 2025 there was a wave of incidents undersea damaging critical infrastructure, and the Finnish authorities have frequently reported suspicious surveillance activities in the proximity of drinking water and energy supply facilities. Whilst most of the incidents have not yielded evidence on possible state involvement, they are fully in line with Russian hybrid interference activities in Finland and elsewhere in the Russian neighbourhood.

Due to the strong political consensus in Finland that the threats to Finnish critical infrastructure are stemming from Russia, the events since 2022 have only fortified the understanding that preparedness to all-hazards is the key to enhancing resilience in Finland. Country's decision to become a member of NATO after 2022 Russia's full scale war against Ukraine also illustrates the widely shared perception of the escalation of threats posed by authoritarian Russia and the need for additional deterrence.

Policy and institutional context

Finnish critical infrastructure resilience and security of supply are in many ways distinct from most European countries, including the ones compared in this report. The closure of the Finnish-Russian border and the end of nearly all traffic across the Eastern border after the Russia's full-scale attack against Ukraine in February 2022 makes Finland almost an island. Consequently, nearly 80 per cent of the Finnish export and import of material goods are currently transported via maritime routes.[47] Moreover, Finland is highly dependent on the undersea energy and communication cables and pipelines that connect it to the European grids and networks.

Dependence on maritime routes has logically impacted on Finnish priority setting. Even though Finland is facing similar threats to its critical infrastructure as most of its peers, such as cyber-attacks and natural disasters, understandably much of the political focus in the critical infrastructure protection has been put on maritime logistics and undersea structures, and how to enhance the security of supply through alternative routes in the case that the main routes fail. This approach has only been fortified after four suspected sabotages occurred in the Baltic Sea in a relatively short period of time, between October 2023 and January 2025.[48] In all cases, undersea structures connecting Finland and Estonia, or Finland and Sweden were damaged by a ship dragging unnecessarily an anchor over the cables. Although none of the cases

[46] Tammikko, Teemu: Vihalla ja voimalla: poliittinen väkivalta Suomessa, Helsinki: Gaudeamus 2019.
[47] Merikuljetukset Suomessa: Logistiikan Maailma, 5 March 2025, available at: https://mmm.fi/en/nature-and-climate/climate-change-adaptation/national-climate-change-adaptation-plan-2030 (last accessed 24.10.2024).
[48] As discussed in deliverable D7.1, these sabotages began around a year after two major Russian gas pipelines meant for export to Germany and the EU, the Nord Stream pipelines, were sabotaged, conducted most likely by Ukrainian nationals.

made significant damage to the Finnish security of supply, the authorities enhanced their pursuing and surveillance capacities and leaned on international cooperation in the EU and NATO context.[49]

In Finland, discussions on resilience and preparedness – both in terms of physical infrastructure and of the functioning of society as a whole – have focused on the concept of comprehensive security. In this concept, the vital functions of society in a crisis are taken care of in collaboration between the authorities, business community, civil society organisations and citizens in all circumstances and at all levels of society.

This is an "all-hazard" approach. The crises may stem from human actions, technological developments, or natural causes, and are addressed through strategic tasks defined for different actors. Executing tasks requires preparedness, namely measures to respond to threats, information sharing and effective implementation among multiple actors in different sectors.[50] Such measures are meant to reduce the likelihood of threats realising and to promote society's readiness to face threats. Individuals are seen as key security actors, and mutual trust among people is considered a vital element in upholding society.[51] This is the discursive and conceptual context within which the transposition of the CER and NIS2 directives has occurred.

From an institutional standpoint, significant measures had been taken already during the 2010s. In 2013, a Security Committee was created to assist the government and ministries in broad matters pertaining to comprehensive security, including 20 members and 4 experts from administrative branches, authorities and the business community.

Recognising the value of the Finnish model for comprehensive security and national preparedness, where resilience is taken care of collaboratively by authorities, business community, organisations and citizens in all circumstances and at all levels of society, in March 2024 European Commission President Ursula von der Leyen tasked former Finnish President Sauli Niinistö with drafting a report on how the EU could enhance its civilian and military preparedness in the face of different crises.[52] The report argued for more extensive foresight capacities and intelligence sharing at the EU level, as well as more centralized decision-making mechanisms for crisis situations. Based on the Finnish model, the report also emphasized that preparedness is not the responsibility of government authorities alone but should be pursued in close cooperation with the private sector and relevant civil society actors. Niinistö's report was quickly transformed into three different papers from the Commission services: the White Paper

[49] On the incidents and responses to them, see for example Teemu Tammikko: The EU and NATO in pursuit of better deterrence: Baltic Sea sabotage prompts rethink of current practices, FIIA Briefing Paper 404, January 2025.

[50] For further details on the origins and articulation of the Finnish comprehensive security model, see Valtonen, Vesa/Minna Branders: Tracing the Finnish Comprehensive Security Model, in: Sebastian Larsson/Mark Rhinard (eds.): *Nordic Societal Security: Convergence and Divergence*, Routledge, 2020.

[51] Finland's Security Committee: Comprehensive Security, 23 June 2025, available at: https://turvallisuuskomitea.fi/en/comprehensive-security/ (last accessed 24.10.2025).

[52] The report, entitled 'Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness', is available at https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf (last accessed 24.10.2025). For an analysis, see Tuomas Iso-Markku/Niklas Helwig, The Niinistö report on preparedness: Finland's lessons for the EU and their limitations, FIIA Comment 9, 2024, https://fiia.fi/en/publication/the-niinisto-report-on-preparedness.

for European Defence – Readiness 2030,[53] the Preparedness Union Strategy,[54] and Protect EU: a European Internal Security Strategy.[55]

Nonetheless, it remains a matter of debate how well the recent EU legislation on the resilience of critical infrastructure and the Finnish comprehensive security model align with one another. The focus in the Finnish model has been to strengthen the communication and information exchange between the relevant actors at all levels, but much of the work has remained voluntary. This is the main change that must take place with the introduction of the CER and NIS2 directives. They force Finnish authorities to take new measures on organizing the work and on recognizing and supervising critical entities, because Finland has not yet defined the national critical infrastructure, the critical sectors, nor actors at the legislative level.[56]

Furthermore, recent research has suggested that the Finnish model is much broader and includes more actors and aspects of security; it emphasizes the pre-crisis phase over the other phases of crisis, but tends to be impervious to adaptation by learning (so it is rather a 'status quo' resilience management model).[57] However, while the resilience management is rather fixed due to the composition of the committee, the resilience itself is in the hands of the actors on the field and hence more flexible. Transposition of the CER and NIS2 directives should contribute to aligning Finnish and EU measures on critical infrastructure protection and resilience, while allowing for national specificities on how they are managed. Due to the above mentioned additional measures, Finland was late in transposing the two directives in its national law, but the work was concluded in July 2025 (CER) and April 2025 (NIS2) respectively.

The Act on the Protection of Infrastructure Critical to Society and on the Improvement of Resilience, transposing the CER directive, entered into force on 1 July 2025. It starts from the premise that the Russian invasion of Ukraine and changes in the security environment have increased the need to protect critical infrastructure and strengthen its resilience. The Act imposes duties on businesses and other entities that provide essential services and are thus deemed to be critical. The duties for critical entities involve: performing a risk assessment within nine months after being notified that they have been identified as critical entities; preparing a resilience plan within one year of their risk assessment; taking any measures to ensure resilience; and reporting any anomalies that significantly disrupt or have the potential to significantly disrupt the provision of essential services.

The Ministry of the Interior is responsible for general coordination, steering and developing operations, following a national plan on critical entities resilience that the Finnish government is due to approve in January 2026. Other ministries are responsible for statutory functions

[53] European Commission: ReArm Europe Plan/Readiness 2030, available at: https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en (last accessed 24.10.2025).
[54] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy: Preparedness Union Strategy, JOIN (2025) 130 final, 2025.
[55] European Commission: Communication from the Commission on Protect EU: a European Internal Security Strategy, no. COM (2025) 148 final, 2025.
[56] Finland's Ministry of the Interior: Kriittistä infrastruktuuria koskevan sääntelyn uudistaminen – Sisäministeriö, available at: https://intermin.fi/hankkeet/kriittinen-infrastruktuuri (last accessed 24.10.2025).
[57] Lauri Jauhiainen: Vital Meets Critical: Comparing the Finnish Comprehensive Security Model and the European Union's Resilience Legislation. Master's Thesis, National Defence University, 2025, available at: https://www.doria.fi/handle/10024/193001 (last accessed 24.10.2025).

within their respective fields. In particular, the other ministries are expected to identify and specify the critical entities in their sector by no later than 17 July 2026. The following authorities supervise jointly and with full respect of their respective mandates that critical entities comply with their obligations under the act: the Energy Authority; the Centre for Economic Development, Transport and the Environment for South Savo; the Finnish Transport and Communications Agency (Traficom); the Finnish Medicines Agency (Fimea); the Finnish Food Authority; the Finnish Safety and Chemicals Agency (Tukes); the National Supervisory Authority for Welfare and Health (Valvira) and the regional state administrative agencies.[58]

The Finnish Cybersecurity Act was adopted in April to implement the NIS2 directive. The competent authority and the single point of contact on the implementation of the Act is the National Cyber Security Centre within the Finnish Transport and Communication Agency. As laid down in the NIS2 Directive, Finland has a dedicated computer security incident response team (CSIRT). It operates within the National Cyber Security Centre, and it is responsible, amongst its dedicated tasks, also for mapping possible vulnerabilities in cyber security.

The supervising authorities on the NIS2 implementation are the same ones mentioned above in the context of the Act on the Protection of Infrastructure Critical to Society and on the Improvement of Resilience. Finland had developed a Cybersecurity Strategy already before the NIS2 directive, and amended it in 2024 to accommodate the requirements imposed by the directive. The Strategy was prepared under the leadership of the National Cyber Security Centre Director on an interministerial subcommittee of a project initiated by the Prime Minister's Office on 8 March 2024. Nearly 100 organisations from the public and private sectors, the scientific community and civil society participated in strategy preparation workshops.[59]

The Strategy is seen as part of the Finnish comprehensive security concept. It includes strategic objectives defined under four pillars (1) competence, technology and RDI; 2) preparedness; 3) cooperation; and 4) response and countermeasures, and common development measures for these objectives. The main focus and goals for the period up to 2035 lie in the preparation of a comprehensive plan on the management of crisis response capabilities and processes regarding the "measures that enable a digital society to prepare for, identify, combat and withstand incidents in electronic and networked systems and their impacts on vital functions and services of society, to recover from them, and to ensure the operating conditions for national security, national defence and security of supply".[60] This plan is currently under preparation in the Ministry of Transport and Communication, with the support of the supervising authorities, police, the security intelligence service, the defence forces, and the National Emergency Supply Agency. As a key challenge, the Strategy states that Finland currently spends nearly EUR 300 million annually to ensure cybersecurity in central government, and the sum spent by the business community is at least ten times larger. However, current basic funding levels are deemed insufficient to respond to the evolving operating environment.

[58] For an overview of the Act on the Protection of Infrastructure Critical to Society in English, see https://intermin.fi/en/frequently-asked-questions-about-the-cer-act (last accessed 24.10.2025).
[59] Finnish Government: Finland's Cyber Security Strategy 2024–2035, 25 October 2024, available at: https://julkaisut.valtioneuvosto.fi/handle/10024/165893 (last accessed 25.10.2025).
[60] Prime Minister's Office: Finland's Cyber Security Strategy 2024–2035, 25 October 2024, p. 10, available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf?sequence=1&isAllowed=y (last accessed 25.10.2025).

Incentives and capacities for implementing CI related measures

Thus, the need for an increase in fun ding to further increase protection and resilience of CI entities in Finland is one of the current challenges to further implementing comprehensive security concept. When it comes to strengthening capacities, Finland has had a Security Committee since 2013, assisting the government and ministries in broad matters pertaining to comprehensive security. Meeting approximately once a month, the Security Committee aims to stimulate discussion and collect information for the development of security in society, especially by arranging seminars and public discussions with various civil society organisations, the business community and other cooperation partners. It also prepares statements and recommendations on relevant matters, usually responding to a request of the responsible ministry.

While the concept of comprehensive security has long shaped Finnish thinking, incentives to review and adapt the system have come with the Russian attack on Ukraine in 2022 and the broader confrontation in Russia-West relations. Finland's NATO membership in 2023, and the consequent strengthened Russian perception of Finland as an adversary, have added further reasons for such a review. Following the adoption of the CER and NIS2 directives, the Ministry of the Interior has acquired further role by becoming responsible for general coordination, steering and developing operations, following a national plan on critical entities resilience that is expected to be approved in 2026. Also in terms of capacity, a computer security incident response team operating within the National Cyber Security Centre, which in its turn is based within the Finnish Transport and Communication Agency.

With the additional threats coming from the worsening geopolitical context, the Finnish Ministry of Transport and Communications has made 'sustained effort to strengthen security'. Already in 2021, Finnish legislation was reinforced based on the EU's recommendations for 5G networks, especially with the view of safeguarding national security and national defence; equipment endangering national security or national defence must not be used in the critical parts of the communications network. Furthermore, in January 2025 the Finnish Transport and Communications Agency Traficom issued a Regulation on critical parts of the communications network, updating legislation from 2021.[61]

The Transport and Communications Agency will regularly assess the updates to the regulation on the definition of the critical parts of communications networks and may, if necessary, also assess as critical a part of a communications network that is not specifically mentioned in the regulation. The Ministry also acknowledged that architecture of communications networks will become more complex in the future. In this regard, an Advisory Board for Network Security has been reviewing security issues related to 6G networks.[62]

Concluding comments

The Finnish case study highlighted the concept of comprehensive security, which can be taken as a potential model – indeed, this was the logic of the European Commission when it asked

[61] Traficom: Määräyshankepäätös: Määräys viestintäverkon kriittisistä osista, 24 January 2025, available at: https://traficom.fi/fi/ajankohtaista/maarayshankepaatos-maarays-viestintaverkon-kriittisista-osista-0 (last accessed 25.10.2025).

[62] https://valtioneuvosto.fi/en/-/1410829/finland-is-prepared-for-security-threats-against-communications-networks-and-is-making-sustained-effort-to-strengthen-security.

former Finnish president Sauli Niinistö to write a report on civil and military preparedness and readiness for the EU, which was eventually published in October 2024.

In this concept, the vital functions of society in a crisis are taken care of in collaboration between the authorities, business community, civil society organisations and citizens in all circumstances and at all levels of society, in an "all-hazard" approach. In this approach individuals are seen as key security actors, and mutual trust among people is considered a vital element in upholding society. The Niinistö report also argued for more extensive foresight capacities and intelligence sharing at the EU level, as well as more centralized decision-making mechanisms for crisis situations.

Finland has had to integrate the concept with the requirements coming from the EU level, notably the CER and NIS2 directive. Adding to its already existing Cybersecurity Strategy, Finland adopted the Act on the Protection of Infrastructure Critical to Society and the Cybersecurity Act, creating or adapting institutional structures to supervise and manage their implementation. Overall, the picture is that of an evolving scenario that responds to increasing and constantly mutating security threats. The consensus is that well-established frameworks and concepts must be flexible enough to deal with the new and future challenges .

Latvia

Threat landscape

Latvia's official assessments highlight Russia as the primary threat to national security and critical infrastructure. Russia's war of aggression, as well as hybrid threats have heightened concerns of targeted hybrid attacks at energy, communications and other networks.[63] The belief is that Russian intelligence and sabotage groups may target CI through espionage, subversion or physical destruction.

Meanwhile, in the cyber realm, state-sponsored attacks and cybercriminal disruptions are a major risk to ICT systems in energy, communications as well as other CI sectors.[64] While most state-sponsored cyberthreats can be attributed to Russia, there has also been an increase in Belarussian and Chinese cyberactivity.[65] CERT.LV noted that China overall has become a much more prominent threat actor in Latvian cyberspace in recent years.[66] In that regard, China's role has mostly been linked to cyber espionage and potential supply chain risks. However, the strategy since 2023 has not only emphasized protecting infrastructure from targeted physical harm and cyberattacks, but also ensuring the continuity of essential services under any crisis, such as natural hazards and technical failures. This is evidenced by the restructuring of the

[63] Latvian State Security Service: Annual Report on the Activities of the Latvian State Security Service (VDD) in 2024, February 2025, available at: https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf (last accessed 15 September, 2025) p. 12; See also Justina Budginaite-Froehly: Baltic States unplug from Russia's power grid – but Moscow still looms over critical infrastructure, in Atlantic Council, 05.02.2025.
[64] CERT.LV: CERT.LV Activity Report Q4 2024, 27.02.2025, available at: http://cert.lv/uploads/eng/CERT_Report_2024_Q4_ENG.pdf (last accessed 15.09.2025), p.7.
[65] Ibid.
[66] Interview with representative from CERT.LV.

crisis management system in Latvia, and the development of a new Crisis management centre, which has begun its work as of July 1, 2025.[67]

There is a broad political consensus in Latvia regarding these threats and the need to strengthen the resilience of CI objects and CEs. The Russian aggression, first in 2014, and then in 2022, were moments that unified Latvian policymakers on strengthening security of vital networks.

Policy and Institutional Context

Successive governments have treated alignment with NATO and EU security norms in the field of CI protection as existential, even when there were significant costs involved. For example, Latvia, together with Estonia and Lithuania, banned Russian energy imports,[68] and fast-tracked decoupling from the BRELL grid.[69] These moves were not controversial or disputed among political actors.

Furthermore, there is a strong consensus on excluding untrusted foreign actors from critical sectors, as evidenced by the amendments to the National Security law, banning Russian and Belarussian nationals from owning, managing, or working in CI companies.[70] In that regard, the Russian and Belarussian national ban was only introduced as late as 2025 due to the changing security landscape and necessity, rather than lack of political consensus on the matter.

Before 2022, arguments such as business interests, cheap energy and benefits of Chinese investments were still somewhat relevant in the public debate. However, the massive geopolitical shifts in recent years have largely seen these arguments disappear. As a result, these policy positions are strongly reflected in the relevant policy planning documents, such as the current National Security Concept, the Latvian Cybersecurity Strategy 2023 – 2026, and the National Defence Strategy 2023 – 2027. It should be highlighted that CI protection falls within Latvia's Comprehensive national defence (CND) policy or, rather policy framework, which envisions national defence as a "whole-of-society" approach to security, extending beyond military defence to include civil and economic resilience, as well as crisis-preparedness.[71] In practical terms, this means strengthening civil participation and preparedness at different levels of governance, fostering cross-sector cooperation between government, private sector, and citizens as well as promoting public awareness.

Latvia has developed a multi-layered institutional framework for the protection of CI objects and CEs. The National Security Law, adopted in 2000 establishes the basic framework for Latvia's national security system and sets out the responsibilities of the relevant institutions.[72]

---

[67] LV Portāls: The Regulatory Framework on the Functioning of the Crisis Management Centre Comes into Effect, 01.07.2025, available at: https://lvportals.lv/skaidrojumi/377945-stajas-speka-regulejums-krizes-vadibas-centra-darbibai-2025 (last accessed 16.09.2025).

[68] "Amendments to the Law on Energy" 14 July, 2022. Accessible on: https://likumi.lv/ta/id/334350-grozijumi-energetikas-likuma.

[69] Tom Bennett: Baltic states unplug from Russia and join EU power grid, in: BBC News (bbc.com), 09.02.2025.

[70] "Amendments to the Law on National Security" 12 June, 2025. Accessible on: https://likumi.lv/ta/id/361476-grozijumi-nacionalas-drosibas-likuma.

[71] Ministry of Defence of the Republic of Latvia: Comprehensive National Defence, available at: https://www.mod.gov.lv/lv/nozares-politika/visaptverosa-valsts-aizsardziba.

[72] "Law on National Security", 14 December, 2000. Accessible on: https://likumi.lv/doc.php?id=14011.

This legislative document defines national and European critical infrastructure, as well as critical financial services, and outlines the basic principles for their identification, protection and operation. Overall strategic coordination lies with the Cabinet of Ministers, which set CI policy and approve lists of critical infrastructure.[73] With regard to policy formulation, there is a split in competence between the Ministry of Interior (MoI) and the Ministry of Defence (MoD). The MoI is a key institution for the physical protection of CI objects and CEs, preparing the necessary amendments to the National Security Law in order to transpose the CER Directive,[74] while the MoD formulates policy with regard to the cyber security of CI objects and CEs, and, for example, has implemented the NIS2 Directive through the National Cybersecurity law.

At the operational level, sectoral regulators and ministries oversee day-to-day implementation in the respective fields. With regard to the energy sector, the Ministry of Climate and Energy as well as the Ministry of Economy alongside the Public Utilities Commission set requirements for supply continuity, grid reliability, and emergency preparedness by energy companies. In the communications sector, the Public Utilities Commission alongside the Ministry of Transport are the responsible institutions on telecommunications network continuity, reliability and resilience. These institutions frequently collaborate with the MoD or MoI to ensure that the necessary physical and cybersecurity standards have been met.

With regard to comprehensive security of CI objects and CEs, the security and intelligence agencies also play a critical role: the State Security Service (VDD) and the Defence Intelligence Service (MIDD) monitor threats, issue warnings, and coordinate protective measures for CI against threats such as espionage, sabotage or terrorism. Meanwhile the Constitution Protection Bureau (SAB), Latvia's intelligence agency, is tasked with overseeing cybersecurity of classified or particularly sensitive CI and CE systems.

The institutions cooperate through formal councils and information-sharing arrangements. For example, the National Security law establishes a National Security Council, that gathers the President, the Speaker of the Saeima, the chairs of the respective Standing committees of the Saeima, the Prime Minister, the Minister of Defence, the Minister of Foreign Affairs, and the Minister of Interior, as well as the Prosecutor-General, and on the basis of invitation - the heads of the national security agencies.[75] This Council essentially coordinates the implementation of a joint national security policy, and is a forum to discuss improvements, and resolve problems. With regard to cybersecurity, the National Cybersecurity Council, which gathers representatives of all ministries and national security agencies, the Central Bank, the Armed forces, the Parliament security bureau, the State Police, as well as the Latvian cyberincident prevention institution CERT.LV, coordinates the development of cybersecurity-related policy and the progress of implementing the goals and priorities set out in the Latvian Cyber Security Strategy, as well as the planning and implementation of relevant tasks and measures.[76] Furthermore, as a part of Latvia's CND policy private CI operators are brought into joint planning

[73] Ibid.
[74] Ministry of the Interior: Government strengthens critical infrastructure resilience and national security, 21.03.2025, available at: https://www.iem.gov.lv/en/article/government-strengthens-critical-infrastructure-resilience-and-national-security (last accessed 16.09.2025).
[75] "Law on National Security", 14 December, 2000. Accessible on: https://likumi.lv/doc.php?id=14011.
[76] Executive order of the Prime Minister No. 2024/1.2.1.-416 "On the National Cybersecurity Council", December 6, 2024. Accessible on: https://likumi.lv/ta/id/357025-par-nacionalo-kiberdrosibas-padomi.

sessions with both their sectoral ministry and the MoD. This way the government ensures that it is aware of civilian resources and plans, and can integrate them into national defense strategies.[77] In that regard, there is now a legal requirement that each critical infrastructure's continuity plan must be coordinated with the respective sectoral ministry and the MoD.[78]

With regard to EU legislation on CI protection and resilience, Latvia has transposed the CER Directive into national law. The MoI proposed amendments to the National Security law to bring into alignment with the CER Directive through introducing the concept of "critical entity resilience", updating criteria for identifying European-level "critical entities of particular importance", as well as adding amendments to empower the Cabinet of Ministers to set detailed rules on incident report, continuity measures, and resilience standards.[79] Although Latvia missed the original October 2024 EU deadline, it moved swiftly in 2025, having the amendments first be approved by the Cabinet of Ministers in March 2025, and then by the Saeima (Parliament) in June 2025.[80] With regard to the NIS2 Directive, Latvia has fully implemented its requirements through the new National Cyber Security Law,[81] which was adopted on June 20, 2024, and came into force on September 1, 2024. This law replaced the older 2018 Information Technology Security Law, significantly expanding the scope of regulated entities and strengthening obligations. Following the transposition of the NIS2, Latvia now designated "essential" and "important" service providers across a broad range of industries, who must adhere to cybersecurity risk-management and reporting rules, leading to an increase of both sectors and private actors, who now fall under the NIS2 directive's scope.

Incentives and capacities for implementing CI related policy measures

Latvia's primary incentive to strengthen CI protection is largely based on national survival and security. The risk of large-scale disruptions caused by an adversary has been made real by both historical events and the current war in Ukraine. This threat perception creates strong political incentives to implement protective measures. Additionally, the comprehensive approach of NIS2 and CER Directives aligns with the Latvian approach of CND. The expanded sectoral scope under CER resonates with authorities and CI operators on all levels – threats are becoming more widespread and interconnected.[82]

Furthermore, the CER and NIS2 directives have acted as an anchor for national policy measures in CI protection. The implementation of NIS2 directive through a new, restructured

[77] Interview with representative of "Latvijas Mobilais Telefons".
[78] Regulation of the Cabinet of Ministers No. 508, "Procedures for the identification, security measures and business continuity planning and implementation of critical infrastructure, including European critical infrastructure" July 6, 2021. Accessible on: https://likumi.lv/ta/id/324689-kritiskas-infrastrukturas-taja-skaita-eiropas-kritiskas-infrastrukturas-apzinasanas-drosibas-pasakumu-un-darbibas-nepartrauktibas-planosanas-un-istenosanas-kartiba.
[79] Ministry of the Interior: Government strengthens critical infrastructure resilience and national security, 21.03.2025, available at: https://www.iem.gov.lv/en/article/government-strengthens-critical-infrastructure-resilience-and-national-security (last accessed 16.09.2025).
[80] Ibid.
[81] "Law on National Cybersecurity" June 20, 2024. Accessible on: https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums.
[82] Mārcis Balodis/Marta Kepe: Lessons from Latvia's Efforts to Keep Essential Services Running During a Crisis, Atlantic Council – *New Atlanticist*, 07.05.2025, available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/lessons-from-latvias-efforts-to-keep-essential-services-running-during-a-crisis/ (last accessed 15.09.2025).

and reorganised Cybersecurity law has given both the authorities and operators of CIs a clear, up-to-date structure to address cyber threats. Rather than reinvent the wheel, Latvian policy makers implement EU directives faithfully, choosing to build additional national measures on top to address specific geopolitical concerns.

It would also be prudent to mention that EU infringement proceedings are also a major driver of compliance through their coercive effect. They are perceived as very costly, especially for smaller states. This is affirmed by the historical context of Latvia's track record with transposition of EU legislation, as Latvia did not have any infringement proceedings initiated against it by the EUCJ until 2024, when the Court delivered a judgment against Latvia for failing to transpose the European Electronic Communications code.

Finally, additional incentives such as attracting investment and increasing economic growth through providing reliable energy and communications services can also be identified.[83] Despite all of the incentives, Latvia along with most EU Member States failed to transpose the CER and the NIS2 Directives within the allotted time in 2024, pointing to the conclusion that the failure did not arise out of a faulty or inadequate incentive structure, but rather due to insufficient capabilities.

Therefore, Latvia has continuously invested expertise and resources in strengthening its capacity and capabilities, when it comes to implementing EU minimum standards on CI protection. To ensure compliance with CER and NIS2 Directives, as well as Latvian national requirements, the government has incrementally raised budgets for security and defence. As a result, institutions and authorities such as CERT.LV[84] under the umbrella of the MoD, the State Police and the National Guard have been able to expand their cybersecurity competences and expertise to meet the increasing administrative and substantive demand.[85] Cybersecurity authorities such as CERT.LV emphasise that Latvia is focusing on a data-driven cybersecurity approach to not only protect, but also to prevent cyberthreats proactively. A major aspect of this process, especially for smaller states, is qualitative analysis based on the data that is accessible.[86]

Operators of CIs and CEs have been closely engaged with Latvian institutions on the necessary steps to be taken for CI policy development. Leading CI operators in Latvia often have strong lines of communication with the relevant officials responsible for policy formulation, and frequently improvements and amendments are offered.[87] CI operators have highlighted that the joint Cabinet of Ministers Regulation No. 397 on Minimal cybersecurity standards, which among other things unifies security measures, continuity measures, resilience planning and incident notification under the NIS2 Directive and Directive 2018/1972 establishing the European Electronic Communications Code, came about through close cooperation between operators and policy formulating institutions (MoD in this instance).[88]

---

[83] Justina Budginaite-Froehly: Baltic States unplug from Russia's power grid – but Moscow still looms over critical infrastructure, in Atlantic Council, 05.02.2025.
[84] Interview with representative of CERT.LV.
[85] LSM+: Interview: Volunteers on the front line of Latvia's cyber defense capability, in: LSM (eng.lsm.lv), 24.07.2024.
[86] Interview with representative of CERT.LV
[87] Interview with representative of LMT.
[88] Ibid.

Furthermore, the MoD as the National Coordination Centre within the remit of the Regulation 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres maintains a community of cybersecurity experts, academics, NGOs and involved businesses. This cybersecurity community has the opportunity to separately or jointly apply for funding from the European Cybersecurity Competency Centre's funding instruments,[89] and strengthen expertise and competencies in the field of cybersecurity. Therefore, it is an opportunity for smaller CEs to not only apply for funding, but also exchange best practices, and ease implementation of EU standards. Furthermore, CERT.LV also heads a working group of security experts, creating a forum, where, for example, CEs can exchange best practices, and seek guidance on how to tackle existing security gaps.[90] Next to exchange of best practices and funding opportunities, it should be noted that the CER and NIS2 Directives also creates a negative system of compliance through fines and a liability system.

Finally, adjacent to the exchange of best practices and incentive systems, both private and public institutions involved in CI protection engage in regular exercises, simulations and trainings.[91] Here the annual military exercise "Namejs", which involves civil actors, municipalities, and CI operators, as well as the yearly cybersecurity training "Meduspods" organised by CERT.LV in collaboration with the MoD should be mentioned. Furthermore, CEs frequently engage in stress tests, penetration tests, and certain CEs in Latvia also participate in the NATO Cooperative Cyber Defence Centre of Excellence organised "Locked Shields" exercises among others.[92]

Concluding comments

The protection of CI is an integral part of Latvia's CND strategy, where attention is not only paid to cyberthreats and physical threats, but also to other aspects such as effective crisis management and the continuity of services, natural hazard preparedness and technical risk management among others. In that regard, a distinctive feature of the Latvian CND strategy is the close cooperation between the military and civilian sectors. This cooperation, and the arising expertise provided a strong foundation for implementing the NIS2 and CER Directives. In effect, Latvia's CND system reflected a high degree of cohesiveness with the EU minimum standards on CI protection, which could be considered an incentive itself.

Despite a strong incentive structure and institutional experience, Latvia's capacity and capabilities were initially insufficient to manage the transposition approach it had chosen, and the implementation of both Directives was delayed. However, continuous allocation of additional resources and funds aimed to remedy any potential gaps. Furthermore, Latvia chose a high degree of private sector involvement in the process of transposing and implementing both

[89] Cabinet of Ministers Regulation No. 139, "Implementing rules of the European Cybersecurity Competence Centre grant programme "Cybersecurity Transformation of Small and Medium-sized Enterprises" for the 2021-2027 programming period" February 27, 2024. Accessible on: https://likumi.lv/ta/id/350225-eiropas-kiberdrosibas-kompetencu-centra-20212027-gada-planosanas-perioda-grantu-programmas-mazo-un-videjo-saimnieciskas-darbibas-veiceju-kiberdrosibas-transformacija-istenosanas-noteikumi.

[90] Interview with representative from CERT.LV; Interview with representative from "Latvijas Mobilais Telefons".

[91] Ibid.

[92] Interview with representative from "Latvijas Mobilais Telefons".

Directives, leading to a longer period of coordination and planning, but a potentially more successful end 'product'. Here, the public-private cooperation – both in policy development and crisis management – stands out as one of Latvia's most valuable tools and is a positive model for other EU Member States.

Latvia's case also highlights other important aspects in the common framework of CI protection. Firstly, a strong institutional framework with both formal and informal coordination platforms is a strong necessity for cross-sectoral awareness and rapid response. Second, regular participation in both national and international exercises by private and public sectors has been vital for building expertise in a very specialized field such as CI protection. Third, Latvia has identified the necessity to streamline obligations and reporting mechanisms for CI operators arising out of different EU Directives.

To conclude, Latvia's experience points to several concrete lessons and recommendations. First, it is important to consolidate unified reporting mechanisms for CI operators to reduce fragmentation and ensure timely threat detection. Second, Latvia's model of sustained public-private cooperation in CI protection and crisis management can be seen as a good practice which might have useful lessons for other countries, in particular EU candidate states. Third, it is important to strengthen and formalize multisectoral coordination platforms, both of a formal and an informal nature.

Lithuania

Threat landscape

In Lithuania, the perception of threats has been mostly influenced by the recent memories of Soviet occupation, the use of economic blockade by Moscow in response to the declaration of the re-establishment of Lithuania's independence in Spring 1990, weaponisation of energy supplies and authoritarian turn of Russia in 2000s and later. As discussed below, the first measures aimed at protecting enterprises considered important for national security were foreseen back in late 1990s. Later they have been expanded with additional restrictions related to investment and technology transfers from China and other authoritarian countries.

Initially the decisions of country's authorities to protect CI by limiting ownership rights and investing into diversification of energy supplies have been domestically contentious. However, after Russia's aggression against Ukraine in 2014 and especially after full-scale war in 2022, the political and societal consensus on the importance of threat from authoritarian Russia became particularly strong. Before that in 2020-2021, Lithuania's relations with Belarus, fluctuating for a couple of decades between dialogue through engagement and sanctioning in response to violations of domestic political freedoms and human rights and its cooperation with Russia took a decisive turn towards growing restrictiveness. The latter followed massive repressions of Minsk against domestic protesters after rigged presidential elections in 2021, forced landing of Ryanair flight in May 2021 and especially the use of irregular migration by Belarus in summer 2021.

Similarly, in the sphere of cyber threats attribution of most important cyber attacks to authoritarian countries eventually led to the mobilisation of resources and institutional reforms, as

discussed below. It should also be noted, that extreme weather events, for example, storm in summer 2024 leaving many households without electricity and mobile communications, have also affected the public debates on the CI related policies, for example, on the need for stockpiling and purchases of electricity generators. Still, geopolitical threats related to authoritarian neighbours Russia and Belarus as well as China dominate political and expert debates.[93]

Policy and institutional context

In the case of Lithuania, it is important to place the recent developments in its CI protection and resilience policies in the context of the last 25 years, which includes developments in two partly overlapping policy subsystems each responding to different set of external factors.[94] In particular, the initial focus of Lithuania's authorities on energy security – first characterised by the gap between rhetoric and actual implementation but later accelerated by external shocks and resulting domestic political mobilisation – deserves more detailed presentation as it is currently used as a basis for country's efforts to mobilise EU resources to increase the resilience of the CI entities in this sector.

The first CI related policy subsystem was developed gradually since the adoption of the first law on the Basics of National Security in 1996 and the Law on the Protection of Objects of Importance to National Security in 2002 to regulate activities and transactions of economic entities considered important for national security, mostly from hostile activities of increasingly authoritarian Russia (and its satellite Belarus). Since early 2000s there has been an increase in political and media attention to the threats posed by Russia's influence in the energy sector via ownership or dominant position in terms of supply of oil, natural gas and electricity. Most of these interdependences in the energy sector – a legacy from the period of Soviet occupation – were increasingly perceived as the source of corrupt political influences aimed at obstructing country's efforts to reduce dependency on Russia and integrate into the EU and NATO.

These measures have been subsequently developed with the regular revisions of the National Security Strategies, adopted by the parliament, driven by wider security concerns, often in response to escalating aggressive actions of Russia in its neighbourhood. Initially they were focused mostly on energy sector, but later included information and communications and other sectors as well as threats associated with investments from China and technology transfers of its companies (since around 2018 when the US intelligence services started signalling to their European counterparts about the security risks related to China's presence in critical sectors, and Baltic States taking them particularly seriously due to the importance of the US as a strategic security partner and related need to align national policies with its).

---

[93] For assessments of threats to national security including CI, see annual reports of the State Security Department of Lithuania at https://www.vsd.lt/en/archive-national-threat-assessments/ (last accessed 27.10.2025). For assessment of cyber threats see the annual reports of the National Cyber Security Centre under the Ministry of Defence at https://www.nksc.lt/en/ (last accessed 27.10.2025).

[94] For a detailed discussion of the evolution of the legal norms and institutions responsible for CI protection in Lithuania see Ramūnas Vilpišauskas: Regulatory patchwork that evolved in response to external threats, legal approximation and domestic influences, in: Maris Andžans/Andris Sprūds/Ulf Sverdrup (eds.): Critical Infrastructure in the Baltic States and Norway: strategies and practices of protection and communication, Latvian Institute of International Affairs, 2021, p. 59-97.

Introduction of foreign direct investment screening and other business transactions by the Governmental Commission established for this purpose in 2018–2020, also influenced by country's accession into the OECD as well as relevant EU norms, constituted further important steps in trying to protect enterprises (also equipment, property, territory) considered important for country's national security in the sectors covering energy, transport, communications, financial and military. The most recent version of the National Security Strategy adopted in 2021 stressed the importance of the total defence model and, among other objectives, developing cyber security, also enhancing resilience and security of critical infrastructure (concretely mentioning transport, energy, finance and credit, information technology and communications, agriculture and food) and ensuring strategic reserve or the necessary production capacity.[95] Resilience of the state and society were described as the first line of defence with extensive list of objectives in the field of crisis and emergency management, cyber and information security and resilience, economic and energy security, migration management, resilience of the health system, etc. dedicated for this purpose.

In other words, evolution of the threat perception, usually in response to the weaponization of energy supplies by Russia (i.e. the termination of the oil supply via Druzhba pipeline in 2006 seen as a response to the decision of Lithuanian government to sell the only country's oil refinery to Polish company PKN Orlen instead of Russia's Lukoil) as well as external shocks such as cyberattacks, Russia's five days war against Georgia in 2008, hybrid aggression against Ukraine in 2014 and, COVID-19 pandemic, Belarus' instrumentalisation of irregular migration, and in particular, Russia's 2022 large-scale war against Ukraine have strengthened the political and societal consensus regarding the need to reduce vulnerabilities in sectors of CI and to strengthen country's resilience by integrating infrastructure with other EU member states.

Initially Lithuania's authorities focused their efforts at energy security which after initial delays led to diversification away from Russia and, as it will be argued below, to the current policy of trying to mobilise additional EU funds to reinforce energy CI protection and resilience. So, for example, when Estonia established NATO cybersecurity centre of excellence following the cyberattacks on country's state and private organisations in 2007, Lithuanian policy-makers started working on a similar initiative culminating in the opening of the NATO energy security centre of excellence in Vilnius in 2012. The Baltic Energy Market Interconnection Plan (BEMIP) to a large extent initiated by Lithuania when it had to close down the Ignalina nuclear power plant due to EU accession commitments, and adopted by the European Commission and most of the EU's Baltic Sea countries in 2009 played an important role in facilitating agreements of the Baltic States on regional energy projects which connected them to the Nordic states and Poland and supporting those projects with EU funding[96]. Lithuanian authorities were also among the first in the region to use EU rules, namely, EU's third electricity and natural gas package to restructure the ownership and management of energy companies.

These initiatives allowed Lithuania's government to declare in spring 2022, shortly after Russia's war, that it decided to completely stop buying all energy resources from Russia becoming

[95] For the last version of the Lithuania's National Security Strategy (which is being currently updated) see. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3ec6a2027a9a11ecb2fe9975f8a9e52e?jfwid=rivwzvpvg (last accessed 27.10.2025).

[96] See Jakub Godzimirski/Ramūnas Vilpišauskas/Romas Švedas: *Energy Security in the Baltic Sea Region: regional coordination and management of interdependence*, Vilnius University Press, 2015, available at: https://nupi.brage.unit.no/nupi-xmlui/handle/11250/296761.

the first EU member state to do so. The decoupling of energy sector from Russia (and Belarus) was completed in February 2025, when the Baltic States switched from Russia-controlled power grid BRELL (IPS/UPS) to synchronise with the Synchronous Grid of Continental Europe (UCTE) managed by European Network of Transmission System Operators for Electricity (ENTSO-E).

This synchronisation project of more than €2 billion benefited from EU funding through Connecting Europe Facility (CEF) contributing €1,2 billion. As Lithuania's Minister of Energy Žygimantas Vaičiūnas noted on that occasion "we are now removing Russia's ability to use the electricity system as a tool of geopolitical blackmail".[97] Lithuanian authorities saw this as a Baltic project driven mostly by Lithuania – a view supported by the official ceremony of the event taking place in Lithuania's capital Vilnius with the participation of the heads of Latvia and Estonia and the president of the European Commission Ursula von der Leyen. It should be noted, though, that a similar large long-term project in the transport sector Rail Baltica, aiming to integrate Baltic States into the EU railway network, important also as a dual-use corridor to facilitate military logistics, has been marred by numerous delays and growing costs.

The second (and related to the first) source of policy and institutional changes affecting the emergence of the CI protection and resilience policy was linked to the domestic political consensus to strengthen the protection of the critical information infrastructure with the legal basis introduced by the Government Resolution in 2016 (later amended in 2018). It provided the definition of the critical infrastructure as an institution or its unit, an enterprise, particular equipment, its properties or components, planned, built or already functioning, irrespective of whether private or state-owned, which provides services of special importance, the unavailability or interruption of which would cause serious harm to the national security, economy, interests of state and society.[98]

In other words, mobilisation of political attention to develop cybersecurity policy in the aftermath of growing number of cyberattacks and especially Russia's use of them as one of the tools of aggression against Ukraine in 2014 led to the explicit adoption of the CI protection policy in Lithuania. Initially protection of critical information infrastructure followed top-down approach by prescribing responsibilities, methodology, including the criteria (10 altogether) to conduct checks regarding the inclusion of the objects into the list of CI, extending them to 14 sectors – significantly more than included into the relevant EU legislation at the time.

Initially the responsibilities were dispersed among different Governmental institutions (in addition to Prime Minister's office and six different ministries including Communications Regulatory Authority, the State Data Protection Inspectorate and Police Department) with the Ministry of Interior acting as the main responsible policy-making and coordinating actor. However, dissatisfaction with institutional fragmentation and institutional turf-wars seen by the key policy-makers as the main obstacle for more effective cybersecurity policy led to the establishment

[97] Tom Bennett: 'Baltic States begin historic switch away from Russian power grid', BBC News, London, 8 February 2025, available at: https://www.bbc.com/news/articles/c627d55v07go.
[98] See Ramūnas Vilpišauskas: Regulatory patchwork that evolved in response to external threats, legal approximation and domestic influences, p. 59-60.

of the National Cyber Security Centre (NCSC) under the Ministry of Defence in 2015 and further consolidation of responsibilities within it in 2016-2017.[99] In 2018, the National Cybersecurity Strategy was approved by the Government.

These institutional reforms included the introduction of financial sanctions for the persons responsible for cybersecurity to incentivise them to take their duties seriously. At the same time, measures to strengthen capacities of CI operators to detect, respond and, if needed, recover from cyberattacks have been developed with the NCSC becoming as a centre of expertise, advice to CI operators, other state and private organisations, and capacity building through regular consultations and exercises, including EU and NATO partners as well as cooperation between private and state actors.

The mobilisation of political attention, centralisation of institutional responsibilities and intensification of capacity building efforts soon led to Lithuania improving its position in the World Cyber Security ranking to reach 4th place in 2019 from being 57th several years ago. These improvements were also accompanied by the initiatives of Lithuanian authorities to take leadership within the EU. At the end of 2017 the EU endorsed Lithuania-led initiative to create cyber rapid response teams within the Permanent Structured Defence Cooperation (PESCO) agreement. This Lithuania-coordinated initiative includes twelve EU member states and cooperates with NATO Rapid Reaction teams as well as partner countries such as Ukraine, especially after 2022 with more attention dedicated to the lesson-drawing from successful cyber defence performed by Ukraine. On the basis of their experience, Lithuanian officials also contributed with their proposals to the drafting of the NIS2 Directive.

These CI related policy developments in Lithuania, driven by domestic political initiatives in response to perceived external threats, often accompanied by the efforts to involve EU (and NATO) institutions with their expertise, financial resources and legal norms, form an important background to the recent adoption of CER and NIS2 Directives in Lithuania. Lithuania transposed them by amending a number of national legal norms. In the case of CER Directive, 15 laws and government resolutions have been amended, with the Law on Crisis Management and Civil Protection being the most important one. Important measures such as the risk assessment methodology, resilience strategy (guidelines) and the identification of the list of critical entities based on common criteria are expected to be adopted in the first half of 2026. In the case of the transposition of NIS2 Directive, 22 laws and government resolutions were amended.[100]

The process of transposing the CER Directive was led by the National Crisis Management Centre (NCMC) established under the Government Chancellery in 2023 to centralise the crisis-management in response to COVID-19 pandemic and other crises such as irregular migration orchestrated by Belarus since mid-2021, in cooperation with the Ministry of Interior. The NCMC is the competent authority representing the "whole-of-Government" approach to continuous

[99] For a detailed discussion of the evolution of Lithuania's cybersecurity policy see Ramūnas Vilpišauskas: Gradually and then suddenly: the effects of Russia's attacks on the evolution of cybersecurity policy in Lithuania, In *Policy Studies*, 45 (3-4), p. 467-488.

[100] See the relevant EU law web sites on national transposition measures communicated by the Member States concerning CER and NIS2 Directives - available at: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32022L2557 and available at: https://eur-lex.europa.eu/legal-content/en/NIM/?uri=CELEX:32022L2555.

monitoring, assessment and warning of risks and threats, receiving and sharing information on incidents, coordination of resilience-enhancing measures, management of crises and state level emergencies, coordinating national security communication, overseeing national stockpile system, organisation of exercises and coordination with NGOs. The NCSC and the Ministry of Defence took the lead in coordinating the transposition of the NIS2 Directive and its practical implementation benefitting from the expertise and working routines developed during the decade since its establishment.

In early 2025, it was agreed in the State Defence Council, bringing together key institutions and parties, that the defence expenditure should reach 5% of country's GDP from the next year – a commitment now also written in the program of the recently formed 20th Government – with a long-term aim of maintaining it at 5-6% level up to 2030. The allocation of more funding for the defence is also likely to benefit CI policy subsystem with some of those investments directed to improving its resilience. The revision of the National Security Strategy initiated this year by the Ministry of Defence is likely to provide a legal basis for such investments. The current version of the Strategy adopted in 2021 prioritised protection against hybrid threats and stressed comprehensive defence. The new strategy is likely to have a stronger focus on societal preparedness and defence, economic and energy security and resilience, including CI protection and resilience, for example, funding of dual-use infrastructure.[101]

Incentives and capacities for implementing CI related policy measures

As it has been underlined above, evolving (and escalating) external threats, mostly from authoritarian Russia and its allies, acted as the main incentive for developing CI related policies in Lithuania. It is also the main reason why during the period of more than two decades of EU membership Lithuania's authorities invested significant efforts aimed at establishing the country as the active and constructive partner in the fields related to security ranging from energy security to cybersecurity and cooperation with other like-minded partners within the EU and NATO as well as Eastern neighbours such as Ukraine, Moldova and (until recently) Georgia.

The widespread view within country's institutions that influencing EU policies requires credible domestic actions and policies consistent with articulated national preferences most likely also acts as an additional incentive to avoid being late with the transposition of EU norms, in particular such as CER and NIS2 Directives which relate to security concerns (according to the officials, Lithuanian was the fourth country among EU member states to transpose them – the fact that it was worth mentioning itself points to the importance of timely transposition).[102] At the same time, it should be noted that country's political processes are characterised by legalistic culture resulting in the proliferation of legal norms, thus increasing regulatory complexity and reducing flexibility in times crises – as noted numerously by the local experts and OECD.[103]

Thus, although the adoption of those EU norms required a number of changes to existing legal norms, those changes were incremental, for example, adding several new sectors such as

[101] Interview with the senior official of the Ministry of Defence, September 5, 2025, Vilnius.
[102] Interview with senior officials from the National Crisis Management Centre, August 26, 2025, Vilnius.
[103] OECD: *Mobilising Evidence at the Centre of Government in Lithuania*, OECD Publishing, 29 November 2021, available at: https://www.oecd.org/en/publications/mobilising-evidence-at-the-centre-of-government-in-lithuania_323e3500-en.html.

health care and public administration, while in many others similar or more demanding rules already existed in Lithuania. Besides, in the process of adopting NIS2 Directive responsible authorities such NCSC introduced additional measures considered the best practices such as foreseeing the position of cybersecurity chief or the possibilities to provide financial incentives for IT specialists which for many years had no possibility to get competitive salaries due to limits regarding pay for different categories of civil servants.[104]

Going to the level of CI operators and entities, incentives for designated persons responsible for the procedures aimed at protecting CI, in particular from cyber threats, have existed for some time. However, according the officials from the NCSC, there were only a few instances of issuing notifications to those responsible to take urgent actions but no cases of actual use of financial sanctions were reported.[105]

Officials from the authorities working with CI protection and resilience policies stress that their focus in working with CI operators and entities included into the relevant lists is on building capacities through regular advices, producing risk assessment manuals and training to use them, conducting awareness raising and training exercises, especially for senior management of CI operators, and similar activities. The National Crisis Management Centre, which is a designated institution responsible for the implementation of the CER Directive, uses also methods such as naming and shaming by comparing municipalities in terms of their preparedness for emergency situations (i.e. presence of shelters), collects and monitors information on variety of risks in real time, coordinates regular exercises and responses in emergency situations. The positive experience of cooperation with regulatory institutions has also been noted by the senior management of leading companies within the energy and telecommunications sectors.[106]

Interestingly, representatives of energy sector noted that the level of maturity in terms of organisational practices and risk assessment procedures regarding CI protection and resilience was higher in the cyber domain compared to physical infrastructure protection, the threats to which are relatively new and there is little experience in dealing with them (i.e. in the cyber domain the probability of attack is higher, the eventual damage is higher and the responsibility/sanctions are higher compared to attacks on physical infrastructure). In the case of the physical infrastructure protection and resilience, there is still significant uncertainty related to the risk assessment, its methodology and corresponding measures such as accumulation of redundancies (spare transformers, generators, cables, etc.) – eventually a matter of significant additional costs which have to be carefully assessed because they might eventually need to be reflected in the prices charged to electricity users.

Another issue complicating the timely actions to increase protection and preparedness of energy companies indicated by both CI operators and officials of the Ministry of Energy was public procurement procedures set by the relevant EU directive. More concretely, the complications arising when offers by companies with potentially high risk profile (i.e. Hungarian companies offering Chinese technologies and equipment) cannot be easily eliminated or procurement procedures cannot be accelerated. In general, the length of procurement procedures to

[104] Interview with senior officials from the National Cyber Security Centre, September 4, 2025, Vilnius.
[105] Interview with senior officials from the National Cyber Security Centre, September 4, 2025, Vilnius.
[106] Interview with the senior management of the energy company LITGRID, March 4, 2025, Vilnius; Interview with the senior management of telecommunications company TELIA, March 6, 2025, Vilnius.

buy new transformers or anti-drone systems has been underlined as the key challenge.[107] On this, the work is ongoing with the European Commission to adjust the public procurement procedures by including security and resilience criteria in addition to price, sustainability and others.[108] The telecommunications companies in their purchases of equipment have adopted due diligence procedures, which include geopolitical risks, also have been replacing Chinese equipment considered risky with similar measures considered by energy sector authorities with respect to solar panels made in China.

More generally, according to CI operators and officials from the state institutions, actions aimed at mobilising resources and expertise to strengthen the protection and resilience of CI, in particular in the energy sector, are actively coordinated with partners from the region, mostly other Baltic States, Poland and sometimes Finland, as well as working with the European Commission. For example, in 13 May, 2025, the ministers of energy of Estonia, Latvia, Lithuania and Poland in a joint letter to European Commissioner for Energy and Housing informed about the comprehensive package of immediate security measures developed by the Baltic and Polish Transmission System Operators (TSOs) and pointed to the joined determination "to establish a dedicated regional flagship model of excellence in energy infrastructure protection and resilience" which, by building on existing and future EU activities and complementing ongoing NATO activities, could in the future be applied to the entire EU – "from the EU's North to its South".[109]

Thus, Lithuanian authorities have been taking initiative to adopt joint regional security and resilience standards in the energy sector as well as cooperation procedures in case there is a need to share reserves. Joint applications for funding from the CEF to secure critical networks and energy infrastructure to supplement national measures focusing on prevention, detection, response, repair and deterrence by investing into anti-drone systems, monitoring systems for undersea cables, emergency reserve of transmission network equipment, protection of the electricity grids, transformers and other CI objects in the Baltic States ("to protect what has been installed with the EU co-funding") against potential threats have been prepared and the discussion with the European Commission on required funding totalling another €1,2 billion from the EU's next Multiannual Financial Framework (2028-2034) have been taking place (rather successfully).[110]

At the same time as expertise from other EU Member States and EU funding is being used to increase capacities of the Lithuanian CI entities and regulatory institutions, domestic policy measures have been implemented aimed at increasing preparedness of CI operators for sabotage acts, civilian drone attacks and potential military threats. These measures in recent years included the review of the rights of the responsible authorities such as the Public Security Service under the Ministry of Interior to use force against intruders into the territory of the

[107] Interview with the senior official of the Ministry of Energy, August 8, 2025, Vilnius.
[108] Interview with the senior official of the Ministry of Energy, July 31, 2025, Vilnius.
[109] Andres Sutt/Kaspars Melnmis/Žygimantas Vaičiūnas/Paulina Hennig-Kloska: Joint Letter of the Ministers for Energy of Estonia, Latvian, Lithuania and Poland to Dan Jorgensen, the European Commissioner for Energy and Housing, 13 May, 2025. The letter, which stressed the importance of EU's timely financial support from the current MFF via CEF an allocating sufficient resources in the next MFF (2028-2034) was accompanied by the non-paper setting out the details of the proposed flagship model of excellence in energy infrastructure protection and resilience.
[110] Interview with the senior official of the Ministry of Energy, July 31, 2025, Vilnius.

energy and other CI objects which it protects. The unidentified drone incursions into Lithuania's air space in summer 2025 led to intensified debates about revision of the mandates of the other authorities such as State Border Protection Service. Also, cooperation procedures between CI operators and military forces as well as civil society in the emergency situations threatening the provision of vital services are being upgraded.

Significant attention of the authorities and CI operators is focused on Ukraine and drawing lessons from its experience through regular meetings with Ukrainian counterparts. Several most important lessons have been indicated. One refers to the adoption of measures needed to ensure continuity of services in case of electricity blackouts and similar emergencies. These include additional measures to protect energy objects such as transformer and telecommunications stations by installing fences on the ground or nets against drones, hiding cables underground or aligning them with other infrastructure such as railways, installing "two-leg" cable links from the mobile communication towers to have one functioning in case of another is cut, having the option of "national roaming" in case the mobile connection is disabled. Yet another lesson includes accumulation of necessary redundancies (cables, generators and fuel to power them, etc.) and to copy data from the main state registers in the clouds in the reliable jurisdictions outside Lithuania. Also, having mobile protection forces as well as reliable personnel trained and committed to stay and provide required services in the case of emergency.

More long-term plans include the decentralisation of the management of electricity systems within Lithuania in case Vilnius or Kaunas is cut-off from the rest of the country, also the possibility to have alternative means of communications to the mobile such as satellite phones. As noted by many officials, most of these measures, especially related to increased resilience, imply significant costs which currently act as the main obstacle to their adoption. Also, when such investments are required in the communications sector where private companies operate, the state aid rules restrict possibilities for the state to support their investments.[111]

Concluding comments

In Lithuania, the concerns regarding external threats originating from authoritarian Russia (and Belarus) goes back to the late 1990s and 2000s. Initially they focused on energy security measures, including those relevant for the protection of CI objects important for national security through restrictions on ownership, business transactions, etc. Gradually with the proliferation of cyberattacks, escalation of aggressive policies by Russia and growing tensions between the US and China, more political attention and institutional changes were dedicated to cybersecurity and resilience policies, screening of investments and technology transfers from China.

There is a relatively wide consensus among the main political actors, business community, experts and civil activists regarding the need to invest into country's defence, including protection and resilience of its CI, to deter potential aggressors. This led to Lithuania becoming one of the first NATO members to announce in early 2025 its intension to allocate 5-6% of its GDP to defence-related funding in the coming years and maintain it up to 2030. Some of these additional funds will be used for upgrading the protection and resilience of CI, such a dual-

[111] Interview with the senior official of the Communications Regulatory Authority, September 3, 2025, Vilnius.

use infrastructure. It will be important to allocate and use those increasing sums in a transparent manner, maintaining trust and support of society for such policies.

At the same time, as noted by policy-makers, regulators and CI operators, additional EU funding for strengthening security and resilience of CI, often in coordination with other Baltic States and Poland, as well as the role of the European Commission and EU agencies such as ENISA in coordinating policies, exchanges of best practices and providing expertise is particularly important. There has also been active interest and cooperation with state authorities and private actors in Ukraine since 2014 and especially 2022 in lesson-drawing in protecting CI and making it more resilient as well as supporting Ukraine's resistance against Russia's aggression, often targeting energy and other CI objects and communication systems.

The multiplication of recent crises such as Russia's aggressive actions against neighbours, cyberattacks, COVID-19 pandemic, weaponization of trade in energy resources and irregular migration by authoritarian neighbours, also extreme weather events causing electricity blackouts and communication disturbances led to the centralisation of the institutional responsibilities, especially within the National Cyber Security Centre under the Ministry of Defence (established in 2015) and within the National Crisis Management Centre under the Government Chancellery (established in 2023). This facilitates coordination of activities aimed at detection, prevention and recovery measures, including those relevant to CI entities and the provision of essential services.

At the same time, existing regulatory complexity might constrain flexibility and agility of actors operating within CI ecosystem, especially in conducting public procurements. In this respect, growing cooperation between state and private actors in the background of the surge of civic activism during the COVID-19 pandemic, assisting refugees from Ukraine and raising support for Ukraine's defences can be noted. In the last several years, responsible ministries, regulatory institutions, in particular NCSC and NCMC, developed routines of coordination with CI entities, monitoring of potential threats 24/7, practices of responses and restoring organisational functions, although new situations such as incursions of unidentified drones and fast developments of technologies often expose new gaps and deficiencies of existing protective policies.

Montenegro

Threat landscape

Montenegro's critical infrastructure faces a combination of natural and man-made threats. Natural hazards include seismic activity, floods, wildfires, and extreme weather events, which pose risks to energy, transport, water, and telecommunications systems. The country's mountainous terrain and Adriatic coastline increase vulnerability to landslides and storm surges, while climate change intensifies frequency and severity of floods and wildfires, highlighting the need for adaptive risk management and resilience planning.

Man-made threats are increasingly prominent. Montenegro's digitalization and EU/NATO integration have made its CI a potential target for cyberattacks, espionage, and hybrid interference. Key sectors: energy (state-owned) and telecommunications (privately owned, foreign-controlled)face differing vulnerabilities. The 2022 cyberattack, attributed to Russian state-sponsored actors, disrupted government services in transportation, energy, and finance,

demonstrating the high impact of cyber operations on CI. Telecommunications operators' foreign ownership complicates oversight, potentially slowing incident response and creating dependencies on external priorities.

Suspicious surveillance and potential sabotage activities continue to be reported, reflecting a broader regional pattern of interference in Southeastern Europe. Terrorist or politically motivated attacks are possible but less frequent, though they remain a recognized risk.

Montenegro has strengthened CI resilience through legislative reforms (2024 Law on Information Security, NIS2 transposition) and institutional mechanisms (Gov-CIRT, planned Cybersecurity Agency), supported by EU, NATO, and regional cooperation. However, implementation gaps persist due to funding constraints, skills shortages, overlapping institutional mandates, and dependence on foreign investment, leaving certain sectors—particularly privately operated telecoms—exposed to both cyber and physical threats.

Policy and Institutional Context

Montenegro has strengthened CI resilience through legislative reforms (2024 Law on Information Security, NIS2 transposition) and institutional mechanisms (Gov-CIRT, planned Cybersecurity Agency), supported by EU, NATO, and regional cooperation. However, implementation gaps persist due to funding constraints, skills shortages, overlapping institutional mandates, and dependence on foreign investment, leaving certain sectors—particularly privately operated telecoms—exposed to both cyber and physical threats.

Montenegro has steadily advanced its digital agenda, in line with its accession process. Notable achievements in digital adoption include increasing internet access, promoting digital literacy and expanding e-Government services. Key aspects of the digital landscape are the following:

- Internet penetration reached 83 percent of the population at the beginning of 2022.[112]
- Digital literacy continues to improve, particularly among younger demographics.
- E-Government services now provide digital IDs and online portals for taxes, healthcare, and education.

While digitalization brings tremendous opportunities for economic growth,[113] it also exposes the country to new and evolving cyber threats.

Increased access to the internet and integration of digital skills into school curricula have equipped young people to navigate online platforms, use e-government services, and engage with digital tools for learning and communication. At the same time, expanded digitalization has led to a rise in cyber incidents, including phishing, ransomware, disinformation campaigns, and identity theft. Young users face heightened risks from exposure to harmful content, online harassment, and privacy breaches, with potential impacts on mental and physical health.

[112] European Union Cyber Direct: Montenegro, 2023, available at: https://eucyberdirect.eu/atlas/country/montenegro (last accessed 22.08.2025)

[113] Danijela Jaćimović/Milena Lipovina-Božović/Bojan Pejović/Suncica Vuković: The Impact of Infrastructure Development on the Economic Growth of the Countries in the Western Balkans and their EU Future. *Prague Economic Papers*, 34(1), 2025.

A stark example occurred in August 2022, when Montenegro experienced a mayor cyberattack which disrupted government IT systems, affecting services in transportation, energy, and finance, and causing significant economic losses.114 Authorities attributed the attack to Russian state-sponsored actors, was seen as a retaliation for Montenegro's alignment with NATO and EU sanctions against Russia.[115] The FBI and cybersecurity experts from France and the UK assisted in the investigation and in strengthening Montenegro's cyber defences.

The rapid expansion of digital infrastructure has not been matched by equivalent improvements in cybersecurity, leaving vulnerabilities that cybercriminals can exploit.[116] The 2022 cyberattack, which severely disrupted public administration systems, underscored the urgent need for clear procedures and institutional mechanisms for incident response," emphasized Dušan Polović, Director General of the Directorate for Infrastructure, Information Security, and Digitalization at the Ministry of Public Administration. [117]

To address these gaps, Montenegro adopted its Cybersecurity Strategy 2022-2026 in December 2021,[118] as part of its long-term commitment to digital resilience. The strategy focuses on risk management, threat prevention, and incident response, aiming to strengthen the national cybersecurity resilience.

However, the level of cyber resilience in Montenegro varies across sectors and ownership structures, according to recent research. The energy sector is considered the most mature and underwent relatively few changes with the adoption of the NIS2 and CER directives.[119] It is predominantly state-owned, with the Government of Montenegro holding a majority stake in key companies such as EPCG, CGES, and the Pljevlja Thermal Power Plant. Within this ownership ecosystem, the government retains full control over operations, infrastructure, and policies, enabling rapid implementation of safety, security, and resilience measures. State funding and planning can be directed entirely toward long-term national security and reliability, although this model may lack the speed and innovation associated with private foreign investment. Oversight and enforcement are more straightforward, as regulators or the government can directly implement policies without prolonged negotiations.

At the opposite end of the spectrum lies the telecommunications sector, where cybersecurity is partially outsourced to foreign operators. As of today, Montenegro's telecommunications industry is 100% privately owned, with all major operators controlled by foreign entities. The leading companies include T-Com Montenegro, with an approximate market share of 35%

[114] European External Action Service: Assessment of Cybersecurity Risks in Montenegro: Challenges and Recommendations'. EU Publications, 2 October, 2023, available at: https://www.eeas.europa.eu/sites/default/files/documents/2024/Montenegro%20Report%202024.pdf (last accessed 21.01.2025)

[115] Based on the interview with the Ministry of Interior's officials, October 17, 2024, via Zoom.

[116] Balkan Investigative Reporting Network: *Montenegro needs to bolster cyber security institutions, 26 June, 2024, available at:* https://balkaninsight.com/2024/06/24/montenegro-needs-to-bolster-cyber-security-institutions-birn-report (last accessed 21.08.2025)

[117] Based on interview with Mr. Dušan Polović, Director General of the Directorate for Infrastructure, Information Security, and Digitalization, Ministry of Public Administration, Podgorica, May 18, 2025.

[118] Government of Montenegro: *Cybersecurity Strategy of Montenegro 2022-2026*, 15 June 2022. Available at: https://www.gov.me/en/documents/85e2a9d0-0d3c-483a-9822-515d3b7798de (last accessed 21.08.2025)

[119] Based on the interview with experts in IT department Montenegro Electric Power Company on September 10, 2025, Podgorica.

(76.53% owned by Hrvatski Telekom, a subsidiary of Deutsche Telekom AG); One Montenegro, with about 23% of the market share (fully owned by the Hungarian technology company 4iG); and Mtel, with an estimated market share of 42% as of May 2025 (51% owned by Telekom Srbija and 49% by Telekom Srpske).

Foreign ownership provides Montenegro with modern telecom services but makes the regulatory oversight complicated, especially in areas such as cybersecurity, data sovereignty, and rapid incident response. The regulator must negotiate and enforce cybersecurity and operational standards with foreign entities, sometimes across borders. This creates risks of slower incident response, conflicting security protocols, and dependence on compliance by foreign shareholders whose priorities may not align with Montenegro's national interests.

As Kentera warned: "Our digital infrastructure depends on global platforms, whose decisions are made far away from Podgorica. If critical infrastructure falls into the hands of foreign capital driven by external interests, we lose the ability to decide our own future."[120]

For Montenegro cybersecurity is not only a technological objective but also a strategic necessity for safeguarding democratic processes, economic stability and national security. "Cyber resilience is a process that requires a strategic approach by each government, continuity in the specialization of experts in institutions, and sustained investment in the infrastructure and cyber ecosystem of Montenegro," stated Mr. Maraš Dukaj, Minister of Public Administration.[121]
.

Montenegro has initiated the process of aligning its cybersecurity and critical infrastructure legislation with EU norms.[122] Key steps include:

- ECI Directive (2008/114/EC): Fully adopted through the 2019 Law on Critical Infrastructure, which establishes procedures for identifying and protecting critical entities.
- NIS1 Directive (2016/1148): Incorporated into the Law on Information Security, introducing concepts such as operators of essential services (OES) and incident reporting obligations.
- GDPR: Data protection law enacted, though enforcement remains inconsistent.
- CER Directive (2022/2557): Montenegro is currently undergoing transition by shifting from a protection-focused CI law toward a resilience-oriented approach.
- NIS2 Directive (2022/2555):

[120] Based on the interview with Mr. Savo Kentera Savo Kentera expert in security and international relations, the President of the Atlantic Alliance of Montenegro, served as the Acting Director of the National Security Agency (ANB) of Montenegro in 2022, September 8, 2025, Podgorica.
[121] Vijesti: *Dukaj: Cyber resilience requires a strategic approach by every government, 20 November, 2023, available at:* https://en.vijesti.me/news-b/society/682595/dukaj-cyber-resilience-requires-a-strategic-approach-by-every-governmen (last accessed 21.08.2025).
[122] European Commission: *Montenegro report 2024,* 30 October, 2024, available at: https://enlargement.ec.europa.eu/document/download/a41cf419-5473-4659-a3f3-af4bc8ed243b_en (last accessed 21.08.2025).

- The transition to the CER Directive (2022/2557) should reflect a shift from protection-focused critical infrastructure legislation toward a resilience-oriented approach. However, Montenegro has not fully transposed CER into national law yet. NIS2 Directive (2022/2555) was introduced and subsequently transposed into the new Law on Information Security, adopted at the end of 2024[123].

The 2019 Law on Critical Infrastructure[124] defined critical sectors as energy, transport, water supply and healthcare, finance, electronic communications and ICT, environmental protection, functioning of state authorities, and other areas of public interest and Ministry of Interior as the responsible institution. The new sectors or subsectors were added in 2024, including space activities, ICT service management, food production, processing and distribution, manufacturing (covering medical devices, computers, electronics, machinery, vehicles, and other transport equipment), electronic service providers, and research entities focused on applied research and experimental development for commercial purposes. The 2024 Law shifts from a general sectoral approach toward a more comprehensive, detailed, and resilience-oriented framework, reflecting broader alignment with EU standards and the CER Directive.

The adoption of the *2024* Law on Information Security served two primary purposes: fulfilling Montenegro's EU obligations and establishing a secure cyberspace that protects critical infrastructure in line with EU best practices. As Dušan Polović noted, "The law has enabled the establishment of new and the strengthening of existing mechanisms for responding to cyber incidents and crisis situations." In addition, Mrs. Mišković emphasized: "This achievement reflects substantial alignment with EU standards in digital policy, media regulation, and electronic communications."

The law represents a significant step in strengthening administrative capacity and achieving legislative harmonization, reinforcing confidence in Montenegro's readiness for EU accession. Its adoption also enabled the provisional closure of Chapter 10 – Information Society and Media in December 2024. As Mrs. Mišković highlighted, "This marks a crucial milestone in the EU accession process."

The 2024 Law on Information Security also clearly defines the roles and responsibilities of institutions responsible for critical infrastructure and cybersecurity. Notably, it establishes the Ministry of Public Administration (MPA) as a central coordinating body in this process, providing strategic oversight and ensuring that institutional responsibilities are clearly delineated across the government.

The MPA's responsibilities include:

- Acts as the Single Point of Contact with the EU and regional partners.

[123] Ministry of Public Administration: Law on Information Security, 11 December, 2024, available at: https://www.gov.me/en/documents/23936380-482a-4784-bd94-be69413d7334 (last accessed 21.08.2025)

[124] Ministry of Interior: Law on the Identification and Protection of Critical Infrastructure, 30 January, 2020, available at: https://www.gov.me/en/documents/2585570a-cdff-420f-a7c4-0f67f19a6d8e (last accessed 21.08.2025)

- Coordinates national cybersecurity policy among ministries, agencies, and operators.
- Oversees the Cyber Security Agency and Gov-CIRT.
- Develops and maintains the national cybersecurity strategy and related action plans.
- Ensures proper categorization of essential and important entities.
- Coordinates regulatory oversight with sectoral regulators.

Operational Cybersecurity Units, function under the strategic guidance of the MPA. These units are responsible for:

- Gov-CIRT and G-SOC[125]: Provide 24/7 monitoring, incident detection, and coordinated response across government networks.
- Cyber Security Agency (planned): It will centralize oversight functions, ensure NIS2 compliance, facilitate cross-border cooperation and conduct audits and enforcement.

Agency for Electronic Communications and Postal Services complements this framework by

- Regulates telecoms and postal networks.
- Ensures network resilience and supervises the market.
- Oversees critical network obligations for private operators.

While Montenegro's institutional framework reflects formal compliance with EU norms, its functional capacity remains limited — a common challenge among smaller EU-harmonizing states. Overlapping jurisdictions, where the Ministry of Interior operates under the 2019 Law and the Ministry of Public Administration under the 2024 Law, limit Montenegro's functional capacity in critical infrastructure protection. This challenge is further compounded by weak enforcement and political influence. Structural fragmentation, skills gaps, and insufficient funding further reduce the effective implementation of CI-related measures. Multiple agencies are responsible for CI protection, with energy, telecom, and digital sectors each overseen by separate ministries. These overlapping or unclear mandates undermine efficiency, additionally.

Beyond domestic arrangements, Montenegro engages actively in regional and international cooperation:

- EU rapid response teams and ENISA initiatives supported the establishment of G-SOC.
- The Western Balkans Cyber Capacity Centre (WB3C)[126] provides training and capacity building for CI operators and institutional staff.
- The Energy Community monitors Montenegro's compliance with EU energy and cybersecurity standards.

[125] Ministry of Public Administration, *Directorate for Information Security and Gov-CIRT, 26 October, 2024,* available at: https://www.gov.me/clanak/drzavne-institucije-privrede-i-gradani-u-crnoj-gori-od-danas-bezbjedniji-u-internet-okruzenju (last accessed 22.08.2025)

[126] Ministry of Public Administration, Western Balkans Cyber Capacity Centre, 10 December, 2024, https://www.gov.me/clanak/otvoren-regionalni-centar-za-sajber-kapacitete-zapadnog-balkana-dan-za-pamcenje (last accessed 22.08.2025).

- NATO, EU, and U.S. partners provide practical support in incident recovery and infrastructure strengthening.

Incentives and capacities for implementing CI related policy measures

Montenegro's EU accession process provides a strong political and financial incentive to reform its critical infrastructure protection and resilience policies in line with EU norms. The negotiation process and provisional closure of Chapter 10 – Information Society and Media demonstrate the tangible benefits of alignment. Achieving this milestone signals progress in EU integration and reinforces Montenegro's commitment to modernizing its digital and cybersecurity frameworks.

Implementing EU legal norms for CI protection and resilience provides access to EU funding, technical expertise, and improved security standards, thereby strengthening the country's resilience.

Pre-accession conditionality and funding play a key role as practical incentives—aligning with EU standards is essential not only for smooth accession but also to access EU pre-accession funds and international grants. This combination of political milestones and financial support encourages Montenegro to adopt EU directives such as NIS2, strengthen infrastructure security measures, and enhance overall resilience, while simultaneously highlighting the risks of reliance on conditional or potentially unstable financing, which can affect the continuity of CI protection projects.[127]

The EU contributes to Montenegro's cyber resilience through multiple instruments, such as IPA programs and the Western Balkans Investment Framework (WBIF), by providing grants, technical assistance, and sector-specific cybersecurity training.128 The EU-financed Cybersecurity Rapid Response project (Phase 2.0) for Albania, Montenegro, and North Macedonia (April 2024–September 2025) provides €1.8 million to strengthen Gov-CSIRTs, SOCs, and cyber resilience in public institutions. Western Balkans Investment Framework (WBIF) provided Montenegro with over €3 billion in grants, mobilizing more than €24 billion in investments, though not cybersecurity-specific. Additionally, Montenegro joined the Digital Europe Programme (2021–2027) in June 2023, gaining access to €7.5 billion through competitive calls. Funding for the new Cybersecurity Agency and Government CIRT comes mainly from national budgets and EU cooperation. To address this, the EU supports Montenegro through IPA III and the Western Balkans Digital Agenda, offering financial aid, technical assistance, and training

However, the EU pre-accession incentives are necessary but insufficient: they encourage formal adoption of norms but cannot substitute for structural, financial, and technical capacity building. While conditionality has been effective in driving legislative alignment (for example, NIS2-based law adoption), it does not guarantee full implementation. Financial constraints

[127] Milena Mihailovic/Ruggero Tabosi: Reforming the EU's pre-accession funding instrument, Issue Paper, European Policy Centre and CEPS, September, 2023, available at: https://cep.org.rs/wp-content/uploads/2023/09/Reforming-the-EUs-pre-accession-funding-instrument.pdf (last accessed 21.08.2025).

[128] European Commission: *Montenegro report 2024*, 30 October, 2024, available at: https://enlargement.ec.europa.eu/document/download/a41cf419-5473-4659-a3f3-af4bc8ed243b_en (last accessed 21.08.2025).

also exacerbate technical gaps: outdated power grids, vulnerable telecom networks, and insufficient digital security frameworks cannot be upgraded without substantial capital.

In same time, Montenegro as a small economy, faces limited public and private funding for cybersecurity and critical infrastructure initiatives. Infrastructure operators often perceive EU norms as compliance burdens rather than strategic investments, particularly in regulated or low-profit sectors such as energy, where small market size, government price controls and high modernization costs constrain profitability.[129] The central challenge for Montenegro is closing the financial gap while ensuring both modernization, cyber resilience and sustainable growth. The country's economic development heavily depends on foreign investment. However, interest from EU businesses remains limited, and Montenegro faces strong competition from alternative sources of capital, including China and the United Arab Emirates. This could strongly increase the country's resilience to potential cyberattacks in the future.

In this context, FDI screening has become increasingly relevant, especially for sectors with national security implications. Montenegro has partially adopted frameworks influenced by the EU's FDI Screening Regulation - a specific FDI screening mechanism for the defence industry. However, no comprehensive FDI screening mechanisms have been in place for other sectors. Security concerns have also intensified around the procurement of Chinese telecom equipment—particularly from Huawei—which has led to stricter scrutiny under EU and NATO standards. Cybersecurity measures to address these risks include national strategies, the establishment of the CIRT, regular training for operators, and regional cyber exercises supported by both the EU and NATO.

As Kentera observed, "Control over strategic resources directly determines the degree of a state's independence—whoever controls the infrastructure, controls the state." Kentera[130] noted that while partnerships with private companies are possible, the State must retain authority over strategic sectors of critical infrastructure. In particular, Montenegro remains highly vulnerable in the energy and digital sectors.

These efforts are reinforced by reforms in public procurement, aligned with Chapter 5 of the EU accession negotiations, which was provisionally closed in June 2025. The reforms introduced electronic procurement, anti-corruption safeguards, and transparency measures—strengthening oversight of telecom-related procurements. As a result, contracts (involving Chinese suppliers) are now subject to fair, competitive, and EU-compliant screening.[131] Montenegro has also adopted EU-aligned legislation, developed centralized e-procurement systems, and professionalized its oversight institutions. Together, these tools embed early-warning

[129] Based on the interview with Mr. Ivan Bulatovic, General Manager of Elektroprivreda Crne Gore-EPCG the largest energy company, May 25, 2025, Podgorica.
[130] Based on the interview with Mr. Savo Kentera, an expert in security and international relations, the President of the Atlantic Alliance of Montenegro, served as the Acting Director of the National Security Agency (ANB) of Montenegro in 2022, September 8, 2025, Podgorica.
[131] EU ME, Chapter 5 - Public procurement, *June, 2025*. https://www.eu.me/en/poglavlje-5-javne-nabavke/ (last accessed 21.08.2025).

("red-flag") mechanisms to enhance scrutiny of foreign vendors and improve institutional capacity to detect and mitigate procurement-related security risks.[132]

Remaining challenges persist regarding CI protection and resilience. The adoption of laws under the NIS2 framework demonstrates Montenegro's formal alignment with EU standards. Political volatility further undermines resilience efforts. Despite strong political and popular consensus on fast EU accession, frequent government changes and limited public awareness of CI's importance reduce the motivation to invest in long-term security. Regulatory bodies and operators in the energy and telecommunications sectors face shortages of funding, personnel, and expertise, limiting their ability to enforce standards and manage risks. While the government has adopted EU-aligned legal frameworks, the implementation remains challenging. International support — particularly from the EU and the Energy Community — is therefore crucial to strengthening resilience.[133]

Domestic funds, both public and private actors, sometimes perceive EU cybersecurity norms as externally imposed obligations rather than strategic investments, thus weakening compliance. As Ivan Stanković of the private IT company Čikom observed, many companies will struggle to fully comply with CI-related regulations due to shortages of staff, expertise, and adequate technologies.[134]

Concluding comments

Montenegro's EU accession process has created strong political and financial incentives to reform its critical infrastructure protection and resilience policies, aligning them with EU norms. Achievements such as the provisional closure of Chapter 10 and the adoption of NIS2-aligned laws signal progress in integration and reinforce the country's commitment to modernizing digital and cybersecurity frameworks. EU support—including funding, technical assistance, and programs such as IPA, WBIF, and the Digital Europe Programme—strengthens national capacity and resilience, while pre-accession conditionality motivates formal compliance.

However, financial constraints, limited domestic resources, and dependence on foreign investment (telecommunications, banking, transportation...) pose significant challenges. Foreign ownership and competition for capital highlight the need for careful oversight, FDI screening, and strategic control over critical infrastructure. Reforms in procurement, regulation, and operational frameworks, together with EU-supported initiatives, have improved governance and early-warning capabilities in Montenegro. However, the country continues to face significant structural, technical, and human capacity gaps. Political volatility, limited public awareness, and perception of EU norms as compliance burdens further hinder full implementation.

[132] Vijesti, EC: Conditions for closing Chapter 5 fulfilled, implementation of agreement with UAE to be in line with European legislation, 3 June 2025. Available at: https://en.vijesti.me/news-b/politika/761159/EC-fulfilled-the-conditions-for-closing-Chapter-5--the-implementation-of-the-agreement-with-the-UAE-to-be-in-line-with-European-legislation (last accessed 21.08.2025).
[133] Based on the interview with expert for telecommunication in Ministry of Public Administration, September 5, 2025, Podgorica.
[134] Based on the interview with Mr. Ivan Stanković of the private IT company Čikom September 8, 2025, Podgorica.

Lessons learned from Montenegro's experience emphasize the importance of combining formal legal alignment with practical capacity building, sustainable financing, and robust institutional coordination.

Moving forward, Montenegro's resilience will depend on sustainable investment, institutional capacity building, skilled personnel, and integrated coordination across public and private actors. These measures are essential to ensure that legal alignment translates into practical protection and continuity of critical infrastructure in the face of evolving cyber threats .

Ukraine

Threat landscape

Since Russia's full -scale invasion, Ukraine has faced an unprecedented convergence of kinetic, cyber, and hybrid threats targeting its critical infrastructure. Now going through its fourth year, the war has placed enormous strain on the country's essential systems, yet the resilience and determination of the Ukrainian people and institutions remain a central factor in sustaining national functionality.

Critical Infrastructure has become both a direct target and an instrument in Russia's strategy to destabilise Ukraine. Disruptions in energy generation and transmission, damage to logistics networks, and interference with information and communication systems are designed to paralyse governance, reduce industrial output, and undermine public confidence. Alongside physical assaults, Ukraine continues to confront a wide range of coordinated cyber operations, disinformation campaigns, economic pressure tactics, environmental disasters, all aimed at amplifying the effects of kinetic warfare.

A UN Human Rights Monitoring Mission report[135] confirms that the destruction of vital infrastructure "violates the principles of international humanitarian law aimed at protecting civilians". This underscores both the severity of the threat and the urgency of building resilient, legally compliant systems of protection.

At the same time, Ukraine's EU accession process adds a crucial strategic dimension to its efforts in CI protection and resilience. Alignment with the EU acquis, not only strengthens Ukraine's institutional capacity, but also integrates its resilience framework into the broader European security architecture. Progress in this area is essential in both the country's reconstruction and its long-term integration with the EU.

In this context, the legislative and institutional framework of CI protection and resilience has acquired strategic importance. Ensuring the effective operation of vital systems under continued attack requires not only defensive capabilities but also coherent policies, regulatory mechanisms, and incentives that support both public and private operators of critical infrastructure.

[135] United Nations Ukraine: Attacks on Ukraine's energy infrastructure: harm to the civilian population, , available at: https://ukraine.un.org/en/278992-attacks-ukraine's-energy-infrastructure-harm-civilian-population (last accessed 16.10.25).

Policy and institutional context

Russia's aggression against Ukraine's critical infrastructure remains a central element of its military strategy, designed to inflict maximum operational, economic, and humanitarian damage. Its overarching objective is to destabilize the state and undermine national resilience.

This strategy involves the physical destruction of key assets and costly facilities, the replacement of which requires considerable time and resources, while their disruption critically affects energy supply to the population and essential infrastructure enterprises. These kinetic threats are further compounded by persistent and sophisticated cyberattacks, aimed at eroding economic stability, weakening public morale.

Cyberwar has become a full-fledged component of Russia's aggression against Ukraine. In 2022, the number of cyberattacks on Ukraine's information infrastructure nearly tripled compared to 2021. More than 1.5 million attempted attacks on the energy sector alone were recorded and blocked that year, with transmission and distribution system operators being the primary targets.

The most significant cyber threat to Ukraine's energy sector is the Industroyer malware[136], the first known malicious software specifically designed to disrupt electricity networks. Originally deployed in the 2016–2017 cyberattacks on Ukraine, it re-emerged in 2022 in an upgraded form known as Industroyer2, used by the Russian hacker group Sandworm.

This new variant, aimed at disabling electrical substations, was combined with a destructive malware tool called CaddyWiper, designed to erase data on infected systems. The attack was scheduled for April 8, 2022, but was successfully prevented through the joint efforts of Ukrainian cybersecurity specialists at CERT-UA and international partners, including ESET and Microsoft.

Attempts such as Industroyer2 are not isolated incidents but part of a broader, coordinated cyber strategy. Russian groups exploit cyber tools to infiltrate energy company networks, conduct reconnaissance, and prepare for both cyber and kinetic operations. According to a representative[137] of the Verkhovna Rada of Ukraine, cyberattacks can be synchronized with planned physical strikes, aiming to:

- Disrupt control systems: disable or confuse supervisory control and data acquisition (SCADA) systems and protective relays.
- Destroy data: deploy *wiper* malware to erase critical information, making rapid recovery through manual or automated processes far more difficult.

In the digital sector, Ukraine is in the process of adapting its national legislation to the NIS2 Directive (EU 2022/2555), which will facilitate integration into the EU digital single market[138]

[136] Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine , https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf (last accessed 15.09.2025).

[137] Communication with the Verkhovna Rada representative on CI protection in the written format (received on 19.09.2025).

[138] Ukraine: 3d Cyber Dialogue with the European Union takes place in Brussels, available at: https://digital-strategy.ec.europa.eu/en/news/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels (last accessed 17.04.25).

– an essential step toward Ukraine's accession to the European Union. Harmonization of cybersecurity standards and practices with EU norms is vital, especially in light of the increasing cyber threats and attacks emanating from the Russian Federation.

To this end, the State Service for Special Communications and Information Protection of Ukraine (SSSCIP) has established cooperative frameworks with European partners. Notably, collaboration has been initiated with the European Union Agency for Cybersecurity (ENISA), and a memorandum of understanding has been signed with CERT-EU. Ukraine has begun aligning its critical infrastructure sectors with the requirements outlined in NIS2 and has introduced procedures for incident response and information exchange concerning cyber incidents and attacks.

Pursuant to the EU Directive on Security of Network and Information Systems (NIS/NIS2), amendments to existing Ukrainian legislation are underway to establish criteria for designating critical infrastructure facilities and to define risk management and incident response requirements. The implementation of NIS2 standards in Ukraine is expected to enhance the resilience of national critical infrastructure against cyber threats, foster cybersecurity cooperation with European counterparts, and improve the protection of state information systems. Furthermore, Ukraine aims to establish a cybersecurity certification system aligned with the EU Cybersecurity Act[139], which will support the entry of Ukrainian IT products and services into the European market and improve their global competitiveness.

The Parliament of Ukraine has on 17 March 2025 adopted legislation concerning the protection of state information resources and critical information infrastructure. This law[140] strengthens Ukraine's cybersecurity defence capabilities and includes the following key provisions:

- Establishment and operation of national systems for responding to cybersecurity incidents, attacks, and threats, including the exchange of information concerning incidents that affect information, electronic communications, and ICT systems processing state or classified data.
- Development of national, sectoral, and regional response teams within the national cybersecurity response system, following the recommendations outlined in the NIS2 Directive.
- Delegation of responsibilities from the national CSIRT (CERT-UA) to sectoral and regional teams, with provisions for involving private response teams in the national cybersecurity framework.

An important characteristic of Ukraine's CI legislation is its two-fold nature. The law explicitly regulates activities in peacetime and under a state of emergency, while activities under martial law are governed by the other laws of Ukraine. This legal 'two-sidedness' reflects a strategic choice, enabling the state and its agencies to employ more flexible and operational protection tools during armed conflict.

[139] Cyber Resilience Act, European Commission, available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (last accessed 17.04.25).
[140] Law of Ukraine 4336-IX dated 27.03.25, On Amendments to Certain Laws of Ukraine on Information Protection and Cybersecurity of State Information Resources and Critical Information Infrastructure Facilities https://zakon.rada.gov.ua/laws/show/4336-IX#Text (last accessed 17.04.25).

Against the backdrop of ongoing threats, a key question is whether there exists a political consensus on the policy instruments used to address these risks, and whether this consensus is supported by regulatory authorities and by CI operators and owners. In general, there is mutual understanding between government bodies, regulators, and market actors about the importance and priority of effective responses. Discussions are ongoing concerning funding sources, the creation of reserve funds and stocks, and the securing of alternative supply routes[141].

Nonetheless, discrepancies between key stakeholders remain. The most systemic difference concerns the strategic architecture of Ukraine's power system. Current state policy continues to prioritize the protection of large, centralized facilities, consistent with the historical model of Ukraine's power grid, which has relied on several large nuclear, hydro, and thermal power plants. However, in the context of war with Russia, which deliberately targets these facilities, the effectiveness of this approach has been called into question. For example, the level of readiness of protective structures at Ukrainian Transmission System Operator (TSO) Ukrenergo National Power Company (NPC) facilities is currently estimated at over 85%. However, physical barriers such as gabions[142] and "big bags[143]" are not always effective against direct missile strikes. The construction of these fortifications is time consuming.

This centralized model has been sharply criticized by experts, many of whom argue instead for a strategy of decentralized generation. Ukraine War Environmental Consequences Work Group (UWEC)[144], among others, advocates for a model built around hundreds of smaller power plants, which would be significantly harder to disable through missile strikes. In their view, such a model offers greater sustainability. The issue of distributed generation in the energy sector is analysed in detail in report D.7.1[145].

In line with Ukraine's energy security strategy, the Cabinet of Ministers' Order No. 713-p of July 18, 2024, approved the Strategy for the Development of Distributed Generation until 2035 and its accompanying action plan for 2024-2026. This strategy aligns with Directive (EU) 2019/944 on common rules for the internal electricity market, as amended by Directive 2012/27/EU, which Ukraine is obliged to implement as part of its commitments to the Energy Community and its integration process with the EU. The plan also emphasizes the importance of guaranteed capacity and the modernization of transmission and distribution infrastructure.

[141] Communication with the former executives of Ukrainian TSO (Ukrenergo) on CI protection in the written format (received on 19.09.2025)

[142] Gabions are wire mesh with cages filled with stones, used for protection of the critical infrastructure by providing durable barriers against physical threats like blasts or vehicle impacts

[143] "Big bags" used for critical infrastructure protection are typically known as Giant Geotextile Bags (GGBs) or Megabags which are large containers made of high-resistance synthetic polymers and filled with soil (often sourced from surrounding area).

[144] Ukraine War Environmental Consequences Work Group (UWEC): Environmental consequences of the war in Ukraine: October-November 2024 Review, available at: https://uwecworkgroup.info/environmental-consequences-of-the-war-in-ukraine-october-november-2024-review/ (last accessed 19.09.25).

[145] Vilpišauskas, Ramūnas et al.: Long policy report on rules alignment of protecting critical infrastructure in interdependent states, available at: https://invigorat.eu/wp-content/uploads/2025/03/D7.1_InvigoratEU_long-policy-report_public.pdf (last accessed 19.09.25).

The obligations placed on energy CI operators and owners in Ukraine represent an important step forward and appear broadly adequate on paper, particularly in terms of alignment with EU standards. It reflects a shift from normative, state-driven approaches to the more comprehensive, risk-based frameworks required by the EU Critical Entities Resilience[146] (CER) and NIS2 Directives. However, their practical adequacy is constrained by limited resources, wartime disruptions, and gaps in detailed enforcement mechanisms.

At the facility level, CI operators are required to develop and implement physical and information protection plans. These plans are not autonomous, as their approval for facilities of categories I and II of criticality rests with the Security Service of Ukraine (SBU). This hierarchy reflects the state's approach to CI protection primarily through the prism of national security, with priority given to oversight by the security services.

Beyond the SBU, a wide range of state bodies are involved in the system, underscoring its nationwide scope. Depending on circumstances, the Armed Forces of Ukraine, the National Guard, the National Police, and the State Emergency Service may be engaged in security and protection measures. The State Service for Special Communications plays a central coordinating role in cybersecurity, including training on countering cyberattacks developed in cooperation with the US Cybersecurity and Infrastructure Security Agency (CISA). Even the NEURC, acting as regulator, has become involved in safeguarding CI-related information during martial law. This broad institutional coordination illustrates the existence of a coherent state policy framework.

Incentives and sanctions for implementing CI related policy measures

The main incentives for applying CI-related protection measures lie in ensuring the sustainability of state functions, particularly the continuity of vital government operations, the preservation of economic stability and citizen security, and the prevention of negative consequences arising from disruptions in infrastructure operations. These measures are also crucial for protecting against both external and internal threats. Further incentives on energy CI protection and resilience are linked to access to financing mechanisms for sensitive expenditures, which depend on compliance with established indicators.

As highlighted in the D.7.1 report, the obligations of CI operators and owners, including in the energy sector, have evolved significantly since the adoption of the Law of Ukraine "On Critical Infrastructure" (2021) and related regulations. Importantly, the law tasked the Authorized Body in the field of critical infrastructure protection – the State Service for Special Communications and Information Protection – with preparing amendments to the Law on Critical Infrastructure, the Code of Ukraine on Administrative Offenses, and the Criminal Code. These amendments were intended to establish forms and amounts of penalties for CI operators, define relevant offenses, and specify liability for violations, within one year of the law's entry into force. To date, however, these requirements remain unimplemented. The reason of non-implementation is a combination of war-related disruptions, limited institutional capacity, political sensitivities, and the need to synchronise with evolving EU legislation.

[146] The CER Directive has not been transposed into Ukrainian legislation.

According to a representative[147] of the National Energy and Utilities Regulatory Commission (NEURC), within the framework of state oversight, the regulator monitors compliance by licensees, including CI operators, with licensing conditions and imposes penalties where necessary. These include sanctions for failing to implement protection measures for critical infrastructure facilities provided for in tariffs, investment programs, or as required by law.

As highlighted in the D.7.1 report, Ukraine is receiving substantial technical and financial support from the EU during the pre-accession period. The EU-Ukraine Facility (2024–2027) is a comprehensive programme providing up to €50 billion in grants and soft loans to help Ukraine address the consequences of the ongoing war and align with EU-standards on its path to accession. The programme is structured around three pillars:

- Ukraine Plan — support for reforms linked to EU accession and urgent financial needs.
- Investment Facility for Ukraine — guarantees and blended finance to attract public and private investment, restore and grow Ukraine's economy, and manage risks for investors in a high-risk environment.
- Macro-financial assistance — stabilisation instruments to sustain Ukraine's fiscal capacity.

Payments under the programme are conditional on Ukraine's adherence to democratic governance, the rule of law, and human rights protections. Beyond financial stabilisation, this assistance serves as a direct instrument of Ukraine's recovery strategy: it enables the purchase of new equipment, funds modernization projects, and supports the integration of Ukraine's energy system into the European one. It also illustrates the strong international consensus that underpins Ukraine's recovery efforts.

In this context it is important to note that the EU integration framework goes beyond financial assistance: it provides a structures pathway for institutional and regulatory transformation based on EU bast practices, standards, and mechanisms for protecting critical infrastructure. This approach helps ensure that Ukraine's resilience is not solely dependent on external aid, but is embedded in sustainable, EU-aligned governance and risk management systems.

At the same time, Ukraine's CI protection strategy remains heavily dependent on international financial and technical assistance. This reliance creates vulnerability to shifts in the geopolitical priorities of partner states. A striking example is the termination by the United States Agency for International Development (USAID) of a $75 million grant agreement for the Ukraine Energy Support Fund. Such developments pose a strategic challenge for Ukrainian policymakers: how to design a protection system resilient to unpredictable political decisions by partners. While U.S. assistance – particularly under the Biden administration – has indeed played a significant role in supporting Ukraine's immediate CI protection needs, the more sustainable and structural path toward resilience is needed, rather than just donor-driven support. Addressing this challenge underscores the importance not only of attracting but also of diversifying funding sources, in particular by fostering conditions for domestic and foreign private investment that are less susceptible to geopolitical fluctuations.

[147] Communication with the NEURC representative on CI protection in the written format (received on 11.09.2025).

The protection of energy critical infrastructure (CI) in Ukraine is based on close cooperation between the public and private sectors. This includes the establishment of joint cybersecurity centres, the development of unified security standards and information-sharing protocols on cyber threats, as well as cost-sharing mechanisms for system modernization and staff training[148]. Such measures enhance the overall resilience of energy CI entities.

While there is broad consensus on the need for robust physical protection, practical implementation faces substantial financial and logistical obstacles, which create strategic vulnerabilities. Restoring and strengthening energy infrastructure requires significant investment. For example, NPC Ukrenergo has received a €100 million EU grant[149], channelled through the German State Development Bank, for substation modernization and physical protection, while the European Investment Bank (EIB) has allocated an additional €86 million for similar purposes. These contributions illustrate the scale of international efforts to support Ukraine's power system.

However, the pace of implementation remains a serious challenge. The construction of passive protection structures (such as reinforced concrete shelters for substations) is a lengthy and multi-stage process. Although the first stage has already been completed, full completion of the second stage is expected only in the first quarter of 2026. Delays are largely due to the need to deenergize[150] equipment during construction, as well as ongoing military risks in frontline regions.

This situation highlights a critical gap between political priority, which demands an immediate strengthening of protection, and the practical feasibility of implementation under wartime conditions. While political and public consensus on the need for protection is absolute, the slow and costly construction of protective structures creates a strategic vulnerability that cannot be resolved overnight. This discrepancy between urgent needs and slow implementation also fuels broader debates about the future direction of Ukraine's protection strategy.

The economic dimension represents another significant area of disagreement. While there is broad consensus on the need to restore the sector and attract investment, specific regulatory instruments have provoked sharp criticism. The private sector, represented in particular by the Federation of Employers of Ukraine (FUE), opposes steep increases in electricity distribution prices for businesses[151], arguing that such measures threaten the survival of industrial enterprises amid widespread infrastructure destruction. Given that FUE represents around 8,000 enterprises accounting for 70% of the country's GDP, its position carries substantial weight.

---

[148] EGA: Boost in cyber resilience of Ukrainian critical infrastructure, Estonia, available at: https://ega.ee/ukrainian-critical-infrastructure/ (last accessed 15.09.2025).

[149] Ukraine to receive €100 million from EU for the reconstruction of electricity transmission system, available at: https://euneighbourseast.eu/news/latest-news/ukraine-to-receive-e100-million-from-eu-for-reconstruction-of-electricity-transmission-system/ (last accessed 15.09.2025).

[150] Isolate the equipment from all hazardous energy sources, which may involve shutting off power and removing fuses or unplugging devices. Performing lockout/tagout (LOTO) procedures by applying locks and tags to the equipment or prevent accidental re-energization etc. Verify that the equipment is de-energized and free from any stored or trapped energy using testing equipment.

[151] Publication by The Federation of employers of Ukraine, available at: https://www.facebook.com/story.php?story_fbid=1401645161443436&id=100047938970171&mibextid=wwXIfr&rdid=jj9ItvGj0ku4XevN# (last accessed 15.09.25).

The Federation of Employers of Ukraine stresses that, under current conditions, tariff policy must take into account not only the cost balance of energy companies but also the sustainability of businesses and the economy as a whole. Otherwise, instead of fostering development and recovery, the country risks facing a new wave of production shutdowns and job losses, particularly in regions most affected by the war.

Other experts contend that the main factor deterring private investment in the Ukrainian energy sector is not the war itself, but rather excessive state interference and regulation. Studies[152] highlight that those frequent changes to market rules, together with state control over electricity prices and sales volumes, make it difficult for investors to assess the profitability of projects. This creates a fundamental contradiction: while the state seeks to attract private capital for recovery, its regulatory policies remain a key obstacle.

For example, regulatory changes to a "green tariff" by National Energy and Utilities Regulatory Commission (NEURC) led to a loss of investor confidence[153], as outlined by analysts and public petition. These changes, which involved altering the tariff's rules and lowering its rates, created an unstable and unpredictable investment environment for renewable energy projects in Ukraine.

This problem is particularly acute in the development of decentralized renewable ("green") generation. Analysts emphasize that resolutions adopted by the National Energy and Utilities Regulatory Commission (NEURC) – altering the rules of the "green tariff" and reducing tariff rates – have undermined investor confidence. As a result, policies intended to stabilize the market in practice deteriorate the investment climate and constrain the growth of one of the most sustainable energy sectors.

It is important to emphasize the cooperation between the state and private sectors. The most striking example of such cooperation is the field of cybersecurity. NPC Ukrenergo and PrJSC Ukrhydroenergo were among the first in Ukraine to join the SBU MISP-UA (Malware Information Sharing Platform – Ukrainian Advantage) platform. This platform allows for real-time information on cyber threats, which is critical for preventing attacks. Ukrenergo NPC was noted that having operational information about existing or potential cyber threats, Ukrenergo will be able to take timely measures to protect energy infrastructure. This statement confirms that operators not only comply with regulatory requirements, but are also actively interested in such cooperation tools, as they directly increase their resilience.

Concluding comments

Russia's aggression has clearly demonstrated that energy and communications infrastructure is a key target in modern hybrid warfare. The enemy uses attacks against energy infrastructure to destabilize the state and undermine national economy. Ukraine, in turn, has demonstrated

[152] White Book of Reforms 2025. Chapter 7. Energy sector reforms in Ukraine, VoxUkraine Team Reforms, available at: https://voxukraine.org/en/white-book-of-reforms-2025-energy-sector-reforms-in-ukraine (last accessed 15.09.2025).
[153] Competition Market Study of Ukraine's Electricity Sector, available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/competition-market-study-of-ukraine-s-electricity-sector_045239a1/f28f98ed-en.pdf (last accessed 15.09.25).

extraordinary resilience, the ability to quickly adapt and strategically transform. Ukraine's response is not just to repair, but to fundamentally restructure its energy and communications system to become more resilient against such future threats of disruption.

There exists a gap between the political priority to urgently strengthen defences and the practical feasibility of implementation under real conditions. Although there is broad political and public consensus on the need for stronger protection, the slow and costly construction of defensive structures creates a strategic vulnerability that cannot be resolved overnight. This mismatch between urgent needs and the pace of implementation has become a key source of disagreement over the defence strategy itself.

Current state policy continues to prioritize the protection of large, centralized facilities, consistent with the historical model of Ukraine's power grid while the experts' community[154] advocates for a model built around hundreds of smaller power plants, which would offer greater sustainability. The main incentives for applying CI-related protection measures lie in ensuring the sustainability of state functions, particularly the continuity of vital government operations, the preservation of economic stability and citizen security, and the prevention of negative consequences arising from disruptions in infrastructure operations.

More broadly, the most effective incentive for investing in CI protection would be the introduction of preferential taxation and special lending conditions, opportunities for participation in joint financing programs, cost-sharing mechanisms, the creation of reserve funds and warehouses, and a procedure for compensating CI facilities for damage, including reimbursement for lost property and funds invested in restoration and protection.

The financial assistance from the international partners is a direct tool for implementing the state recovery policy. It allows for the purchase of new equipment and financing of modernization projects, integrating the Ukrainian energy system into the European one. This is a vivid example of the consensus that exists at the international level, which the Ukrainian government is actively using.

At the same time, Ukraine's CI protection strategy remains heavily dependent on international financial and technical assistance. This reliance creates vulnerability to shifts in the geopolitical priorities of partner states. Addressing this challenge underscores the importance not only of attracting but also of diversifying funding sources, in particular by fostering conditions for domestic and foreign private investment that are less susceptible to geopolitical fluctuations.

Diversification of support is not only about funding sources, but also about broadening the foundation of Ukraine's resilience – from donor-funded initiatives to systemic alignment with the EU *acquis* and long-term integration into European CI protection networks.

Harmonization of cybersecurity standards and practices with EU norms is vital, especially in light of the increasing cyber threats and attacks emanating from the Russian Federation. Since 2014 Ukraine's experience shows that resisting hybrid attacks requires robust cyber and infrastructure defences, effective counter -disinformation services.

[154] Lessons of war: Ukraine's energy infrastructure damage, resilience, and future opportunities, Saulius Rimutis, Eastern Europe Studies Centre, available at: https://www.gssc.lt/wp-content/uploads/2024/05/v04_Rimutis_Ukrainos-energetikos-sektoriaus-zala_EN_A4.pdf (last accessed 15.09.2025).

It is important to emphasize the cooperation between the state and private sectors. This interaction is based on a common need to respond promptly to threats and ensure stable operation of systems. This includes the establishment of joint cybersecurity centres, the development of unified security standards and information-sharing protocols on cyber threats, as well as cost-sharing mechanisms for system modernization and staff training. Such measures enhance the overall resilience of energy CI entities.

Georgia

Threat landscape

Georgia's threat landscape is defined by a broad spectrum of threats that encompass both conventional military risks and complex hybrid challenges. More than 20 percent of Georgia's territory remains under Russian occupation, creating a persistent source of instability. creating a persistent source of instability. The presence of occupying forces is accompanied by ongoing unlawful activities, including arbitrary detentions, abductions, killings of Georgian citizens, and the gradual "borderization" of administrative boundary lines.[155]

In addition to threats originating from the occupied territories, Georgia's security environment is affected by broader regional and global dynamics. The ongoing war in Ukraine and the continuing conflicts in the Middle East have contributed to heightened instability across the wider region. These external pressures intersect with internal challenges, including domestic unrest stemming from disputed elections and a foreign policy shift away from EU integration, as well as deepening political polarization and institutional fragility, which further erode national resilience and weaken Georgia's ability to respond effectively to security threats.[156]

The global escalation in the frequency and sophistication of cyberattacks[157] is reflected in Georgia, which has persistently been a target of Russian state-sponsored actors.[158] In 2024, based on the annual report of State Security Service of Georgia,[159] the Operational-Technical Agency responded to 173 cyber incidents of medium and high criticality that were carried out against 32 first-category Critical Information System Subjects (CISSs). This represents an increase of nearly 25 percent compared to the same period in the previous year and reflects only incidents of medium and high severity, indicating that the overall volume of hostile cyber activity is likely much higher.

Policy and Institutional Context

Despite the persistently volatile security environment, Georgia's security policy framework remains fragmented and outdated.[160] Progress in this field appears to have been hindered by democratic backsliding and ongoing political tensions,[161] which have weakened institutional

[155] Seskuria, N.: Russia's 'Hybrid Aggression' against Georgia, 2021.
[156] Gvineria, Sh.: 'The Roots of Georgia's Political Crisis', 2025.
[157] The European Union Agency for Cybersecurity (ENISA) Threat Landscape 2024.
[158] Civil Georgia: Bloomberg: Russia Hacked Entire Georgia Between 2017-2020, 2024.
[159] State Security Service of Georgia, Annual report, 2024.
[160] The National Security Concept was approved in 2011, while the publicly available section of the National Threat Assessment covered the years 2010-2013.
[161] Statement by the Parliamentary Assembly of the Council of Europe (PACE), April 10, 2025

continuity, reduced policy prioritization, and diverted resources away from long-term capacity building.[162] Moreover, Georgia's recent departure from its EU integration trajectory has considerably hindered efforts to align national legislation with European standards. Particularly concerning is the absence of a regulatory framework for CI. This gap leaves country's essential sectors exposed to physical, cyber and hybrid threats, while limiting the state's ability to coordinate responses and build institutional resilience.

As outlined in the previous long policy report,[163] Georgia continues to lack both a legal framework and an institutional architecture dedicated to CI. In September 2025, the National Security Council, formally tasked in 2020 with leading and coordinating the CI reform, was abolished.[164] This institutional vacuum has left the already stalled reform process without clear authority, responsibility, or implementation structure. In this context, when the reform has progressed no further than the development of an initial draft of the law on CI protection, which has remained dormant for more than three years, assessing alignment with the EU Critical Entities Resilience (CER) Directive is premature. By contrast, as described in the previous report, Georgia has achieved some progress in cyber governance and legislation. This chapter therefore focuses on these developments and their alignment with the NIS2 Directive.

To contextualize the analysis, this section first examines the policy framework within the cyber domain. Although Georgia has prior experience in developing cyber policy documents, it currently lacks a national cyber strategy following the expiration of the previous strategy in 2024,[165] representing a setback in the country's alignment with NIS2 requirements. According to field experts,[166] democratic backsliding and ongoing political tensions,[167] together with institutional weakening, particularly the abolition of the National Security Council which previously served as a coordinating and policy-shaping body within the national cyber ecosystem, have further disrupted policy continuity in this domain.

As highlighted in the previous long policy report, the 2021 reform led to substantial amendments in Georgian cyber legislation, notably the Law of Georgia on Information Security,[168] which although is not formally based on ISO/IEC 27000-series standards,[169] it incorporates similar requirements, including governance, risk management, security controls, incident management, and information classification. In essence, the law is framework-agnostic, allowing organizations to adopt internationally recognized standards developed by Information Systems Audit and Control Association (ISACA) or National Institute of Standards and Technology (NIST), to achieve compliance with international best practices in information security.

---

[162] Interview with the former government official, Security Policy Expert, September 4, Tbilisi.
[163] Aho et al.: Long policy report on rules alignment of protecting critical infrastructure in interdependent states (InvigoratEU Report D7.1), 2025.
[164] Civil Georgia: Georgian Dream to Abolish National Security Council, 2025.
[165] Government of Georgia: Decree N482, 2021.
[166] Interview with the founder of a Georgian cyber security civil society organisation, September 1, 2025, Tbilisi.
[167] Council of Europe Parliamentary Assembly Resolution 2585, 2025.
[168] For a detailed description of the reform, the established supervisory system, and the categorization of CISSs, see the previous long policy report.
[169] ISO/IEC 27000-series standards on information security management systems, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

It should be noted that during the 2021–2025 period, steps were undertaken to clarify and regulate some key aspects of cyber supervision over CISSs and to operationalize the 2021 amendments. A series of by-laws were issued by the Head of the LEPL Georgian Operational-Technical Agency (OTA) under the State Security Service of Georgia (SSSG) for First- and Second-Category CISSs, and by the Head of the Digital Governance Agency (DGA) under the Ministry of Justice for Third-Category systems. These by-laws addressed minimum information security requirements, minimum standards for information security managers, rules for managing information assets, procedures for conducting information security audits, rules for configuring network sensors, and requirements for the conduct and frequency of penetration tests.[170]

Despite these advancements, significant challenges remain in further developing the legal framework to achieve closer alignment with EU standards. One of the most critical shortcomings in Georgia's legal framework concerns the process for designating entities as CISSs, as it provides only a general framework and lists several designation factors, while also mandating the development of detailed regulations and methodologies. However, by 2025 such instruments have not yet been adopted, and the designation process remains state-driven, non-inclusive, and opaque. For example, in the absence of clear regulations and a systematic approach, private healthcare service providers are entirely excluded from supervision. According to insights obtained from cyber experts with professional ties to CISSs,[171] private companies are not meaningfully involved in the process and are often informed of their designation only retrospectively. Simultaneously, the introduction of a risk-based classification system for CISSs, distinguishing between "essential" and "important" categories as set out by the NIS2 Directive, is currently absent in Georgia, which is widely regarded as a critical priority for strengthening the supervisory framework and ensuring more effective oversight. Exploring the underlying reasons for these delays requires further research, however, possible factors include limited institutional capacity, weak policy leadership, and the relatively low prioritization of cybersecurity on the political agenda, all of which appear to have been further exacerbated by political instability.

Incentives and capacities for implementing CI related policy measures

At the outset of any discussion on incentives for advancing CI policy, it should be emphasized that broader political turbulence has undermined the coherence of policy development across all sectors in the country. The uncertain prospects of Georgia's EU accession have further constrained the prioritization of aligning national legislation with EU norms, including the CER Directive and the NIS2 Directive. Rather than fostering long-term strategic planning, institutional dynamics have become increasingly oriented toward regime preservation, often at the expense of democratic consolidation.[172]

Prior to the government's decision in December 2024 to delay EU accession negotiations until 2028, Georgia's Euro-Atlantic aspirations consistently guided efforts to align national legisla-

[170] All by-laws are accessible at: https://matsne.gov.ge/.
[171] Interview with the director of the private cyber security consulting company, September 10, 2025, Tbilisi.
[172] European Parliament Press Release, 4 July 2025, available at: https://www.europarl.europa.eu/news/en/press-room/20250704IPR29451/parliament-deplores-the-democratic-backsliding-and-repression-in-georgia.

tion with EU norms. Nonetheless, reform initiated in 2018 to establish a comprehensive framework for CI protection, which at the time would have aligned Georgian legislation with the ECI Directive[173] and laid the groundwork for transposing the CER Directive, remains stalled. This stagnation reflects not only recent political turbulence but also a lack of strategic leadership and a coherent, long-term policy vision. Consequently, limited prioritization has weakened incentives and motivation, and deficiencies in the policymaking process are directly reflected in the private sector's limited awareness and underdeveloped capacities.[174]

As noted earlier, the highly digitalized nature of Georgia's financial sector, combined with the persistent threat of cyberattacks from Russia, has intensified the government's focus on developing the national cybersecurity domain. Although the NIS Directive has never been formally binding, the country's pro-European orientation was evident in its cyber policy, with the most recent National Cybersecurity Strategy and Action Plan (2021–2024) explicitly identifying alignment with the NIS Directive as a strategic objective. While the strategy implementation report was never made publicly available, leaving the extent of progress toward this objective unclear, the commitment at the national policy level nonetheless served as a significant incentive and clearly articulated strategic goal.

However, Georgia's cyber ecosystem exhibits significant gaps in incentives and state support mechanisms for CISSs. Field experts note,[175] that rather than prioritizing trust-based cooperation and ecosystem strengthening, the government has adopted a predominantly supervisory approach, integrating the security service into the cyber domain. This has made the system more insular and focused primarily on formal legal compliance. The public-private partnerships, widely recognized as critical for developing a coherent policy vision and establishing incentives, have largely remained ineffective in practice, despite their prioritization in the national cybersecurity strategy and backing from international donors.

Available open-source information indicates only occasional mentions of state supervisors conducting free capacity building trainings for CISSs. While such trainings could be considered a form of incentive, their fragmented and unsystematic nature limits their overall significance.

While lacking a systemic approach to incentives and state support mechanisms, the 2021 reform introduced administrative sanctions for violations of information security requirements, thereby establishing a form of legal accountability previously absent. Prior to this reform, the absence of such mechanisms and the predominantly recommendatory nature of the law hindered effective enforcement of cybersecurity legislation across both the public and private sectors. Interviewed field expert[176] contends that, due to insufficient political will, potentially stemming from ongoing political turmoil in the country, state regulators often fail to enforce sanctions rigorously, opting instead for more lenient approaches, which undermines overall compliance.

[173] Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures (ECI Directive).
[174] Interview with the former government official, Security Policy Expert, September 4, 2025, Tbilisi.
[175] Interview with former senior official within Georgia's cyber governance framework, September 1, 2025, Tbilisi.
[176] Interview with the founder of a Georgian cyber security civil society organisation, September 1, 2025, Tbilisi.

All interviews conducted with field experts highlight that the capacity of state supervisory agencies is limited, both in terms of human resources and technical capabilities. In addition, deficiencies and ambiguities within the regulatory framework and legislation further undermine the effectiveness and overall capability of supervisory functions.

The absence of formal coordination mechanisms among state stakeholders constitutes one of the most significant deficiencies. Each supervisory body maintains its own Computer Emergency Response Team (CERT), aligned with the CISSs under its jurisdiction. However, the law neither designates a single national CERT nor establishes a formal framework for coordination among existing teams during cyber incidents. This represents a significant gap, not only in terms of alignment with EU norms, but also in creating a fragmented operational landscape that may limit the effectiveness of incident response and undermine the overall resilience of Georgia's CISSs. Furthermore, the absence of an integrated approach leaves the national crisis management framework inadequate, representing one of the key shortcomings in Georgia's alignment with the NIS2 Directive.

Among the key shortcomings undermining the overall capacity of the supervisory system is the absence of a sector-specific approach. The telecommunications sector remains the only domain distinctly categorized within the supervisory framework. However, this formal distinction has not resulted in the establishment of sector-specific supervisory practices. The decision to place the sector under the oversight of the OTA SSSG was initially met with considerable criticism from civil society organizations and expert community, particularly regarding concerns over supervision of telecom operators and the potential access to sensitive data.[177] However, in the four years following the reform's implementation, experts have questioned[178] the extent to which the OTA SSSG has actively fulfilled its supervisory responsibilities in this sector. In the context of political tensions, the agency may have limited its oversight to avoid conflicts with major private entities that hold substantial economic and political influence within the telecommunications field.

Unlike the telecommunications sector, the energy sector is not categorized separately, and the approach applied here appears even less systematic. State-owned energy companies are designated as first-category CISSs and fall under the supervision of the OTA SSSG, whereas private energy companies are classified as third-category CISSs and are overseen by the DGA. The division of supervisory responsibilities between different authorities raises concerns regarding regulatory coherence and the potential for uneven treatment within the energy sector.

When assessing capacities within private critical sectors, all interviewed experts highlight a general lack of capability and awareness, an exception being banks, which, due to their high level of digitalization, have invested substantially in cybersecurity. One of the pressing issues identified during the interviews is the insufficient level of cyber awareness among the top management of CISSs. This lack of strategic understanding directly contributes to the underdevelopment of institutional cyber capabilities, a concern particularly relevant given that leadership engagement and awareness are core requirements under the NIS2 Directive. An evident

[177] IDFI: "Georgian Parliament should not support Draft Amendments to the Law of Georgia on Information Security", 2020.
178 Interview with the founder of a Georgian cyber security civil society organisation, September 1, 2025, Tbilisi.
Interview with the former government official, Security Policy Expert, September 4, 2025, Tbilisi.

reflection of these capacity gaps is the repeatedly extended compliance period for CISSs to meet minimum information security standard. Initially set at two years at the outset of the 2021 reform, the deadline has since been doubled to four years. This pattern suggests both limited capacity among CISSs to meet regulatory requirements and a weak enforcement approach by the state, which has favored deadline extensions over the application of sanctions.

It should be noted, that during the implementation period of the previous strategy, international donors launched numerous initiatives aimed not only at strengthening the capacity of state cyber agencies but also at enhancing the resilience of CISSs. However, the enactment of the so-called 'foreign agents law'[179] in 2024 substantially reduced the scope of this assistance.

Concluding comments

Georgia has long been regarded as a frontrunner among the association trio. On many technical benchmarks, the country remains more closely aligned with the European Union than Moldova or Ukraine. However, the recent erosion of democratic standards and the broader departure from the EU integration path have significantly slowed progress.[180] As a result, numerous internal reforms, including those related to the harmonization of CI regulations with EU-wide norms have stalled, leaving the process marked by stagnation and uncertainty, with no clear prospects or timelines for advancement.

The preceding analysis highlights both persistent gaps and incremental advancements in Georgia's CI policy alignment with EU standards. As noted above, the absence of a comprehensive legal and institutional framework governing CI suggests, that current cybersecurity efforts may be insufficient to address broader systemic risks. Progress in transposing the CER Directive into national legislation remains highly limited, as CI reform in Georgia is stalled, lacking a clear roadmap or political commitment.

Notably, efforts to strengthen national cyber resilience lay the groundwork for potential alignment with the NIS2 Directive. This is reflected in the European Cyber Security Organisation's (ECSO) NIS2 Transposition Tracker, which indicates that transposition of the directive has commenced and has already reached a partial stage.[181] Nevertheless, the continuity of legislative harmonization and the resolution of critical gaps remain uncertain, particularly in light of current strains in EU-Georgia relations.[182]

[179]OSCE Office for Democratic Institutions and Human Rights: "*Georgia's foreign agents legislation raises concerns over negative impact on civil society*", 2025.
[180] De Waal, T.: The Orbanizing of Georgia, 2023.
[181] ECSO NIS2 Directive Transposition Tracker, available at: https://ecs-org.eu/activities/nis2-directive-transposition-tracker/.
[182] EU NEIGHBOURS east: "Georgia accession process de facto halted as EU calls on government to change course", 2024.

5 Conclusions and Recommendations

The changing threat landscape is the key driver behind CI related policies

The CI protection and resilience policies in European countries have been evolving in response to the changing landscape of threats – from natural disasters and extreme weather events to terrorist acts, sabotage and, most recently, a range of potential and actual attacks attributed to Russia amidst Russia's large-scale war against Ukraine, targeting directly its energy and other critical infrastructure. The escalation of the threats to CI represents a key challenge and at the same time a major incentive for European countries, especially 'front-line' states to continuously review and adapt their policies, institutional routines and practices in order to improve their agility and preparedness in the face of the high uncertainty and flux.

The national context is important…

The analysis of the CI related policies in six European countries provided in this report leads to several conclusions. To start with, the national situations in terms of threats perceptions and existing policy and institutional templates aiming to increase protection and resilience of CI differ. Even countries as similar in their threat perception and recent political, institutional and other reforms as Latvia and Lithuania adopted somewhat different institutional roles and priorities in responding to the changes in external threats and evolving legal framework as well as learning from experience, including experience of Ukraine.

These national differences, often originating from path dependency of past decisions, also affect how EU norms such as CER and NIS2 Directives are being implemented with different institutional responsibilities assigned and different adjustments needed compared to previously existing norms. This is particularly visible in the case of Finland where EU norms are seen to some extent as diverging from the established traditional voluntary mode of collaboration between state, private and societal actors in dealing with risks and threats to CI and maintaining societal resilience.

The national differences in their CI related policies and institutional approaches are also visible among the three candidate countries, originating first of all from general consensus regarding the goal of EU accession or lack of it, as in the case of Georgia. Another reason for those divergent legal and policy templates is related to different geopolitical situation, in particular, threats perception and actual state of experiencing daily kinetic and cyberattacks on the country's CI as in the case of Ukraine. However, Ukraine's experience has also become a testing ground for new practical resilience measures in restoring the provision of essential services such as electricity, communications and other, thus providing important lessons not only for Ukrainian authorities, private and civil actors, but also for its partners in the EU and other candidate countries. In this respect, European Commission and EU's agencies acting in this field would also benefit from closely monitoring experience of Ukraine from developing anti-drone systems to findings ways how to deal with interruptions of communications and other disturbances by hostile actors.

… but there are important similarities and alignments

At the same time, those national differences should not be exaggerated and should be seen in a broader temporal perspective. The analysis shows that in recent years threat perceptions of EU Member States, especially 'front-line states', became more similar. This is reflected in

comprehensive security (or defence) approaches adopted by Finland, Latvia and Lithuania. Also, dealing with the threats associated with cyberattacks in particular seems to be a common policy priority in all countries analysed originating from their frequency, potential for damage and cross-border nature. In this respect, EU's norms such as NIS2 Directive provide useful template for improving the protection and resilience of CI entities, while leaving sufficient flexibility to take into account national institutional characteristics and technological evolution.

More systematic use of the known best practices is important

The analysis of selected country cases and their approaches to CI protection and resilience confirms the importance of state and private actor cooperation as well as cross-border cooperation, especially among neighbouring countries facing similar risks and threats and through institutions such as the EU and NATO. Flexibility and agility allowing to respond to the changing nature of threats and technological advances is particularly important and needs to coexist with the tendencies of centralisation and the need for transparency in decision-making, for example, while conducting public procurements. European Commission and EU's relevant agencies would be advised to cooperate with Member States and candidate countries in the continuous search for the adequate balance, facilitating learning from each other's experience.

Similarly, country studies once again confirm that important trade-offs exist in the search for the best methods of increasing resilience of CI entities, especially in the times of hybrid and kinetic war. The key among those is the trade-off between cost-efficiency and effectiveness and more generally the acknowledgement that strengthening resilience often requires massive investments and regional coordination mechanisms. Finland, Latvia and Lithuania are examples of countries which have significantly increased their defence-related spending (and provide relatively high support for Ukraine), some of which is being used also for CI protection and resilience purposes.

However, here the role of EU funding and coordinator role of the European Commission seem particularly important. As the negotiations on the new MFF (2028-2034) gather pace in the EU, it is a very appropriate time to decide on allocating money for Ci related investments which would be adequate compared to the current challenges experienced by European countries. The geopolitical outlook signals that those challenges are not going to disappear – rather on the contrary. The new MMF should also provide certainty to the candidate countries, which are on the path of EU accession related reforms, that they will also be able to benefit from EU funding and other capacity building measures. As the analysis in this report shows, EU's contribution to capacity building in terms of additional funding, providing of policy templates and expertise as well as platforms for sharing best practices and conducting joint exercises is extremely valuable and should be continued.

Bibliography

Alexopoulos, Marcos J., Arto Niemi, Bartosz Skobiej, Frank Sill Torres: Examination of the Critical Infrastructure Resilience Directive from the Maritime Point of View, in: *Journal of Common Market Studies*, vol. 63, 2025, p. 667–678, https://doi.org/10.1111/jcms.1368.

Andžans, Maris /Andris Sprūds/Ulf Sverdrup (eds.): *Critical Infrastructure in the Baltic States and Norway: strategies and practices of protection and communication*, Latvian Institute of International Affairs, 2021.

Anglmayer, Irmgard: European Critical infrastructure: Revision of Directive 2008/113/EC, European Parliamentary Research Service (EPRS), February 2021, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf (accessed 10.10.2025).

"Amendments to the Law on National Security" 12 June, 2025. Accessible on: https://likumi.lv/ta/id/361476-grozijumi-nacionalas-drosibas-likuma.

"Amendments to the Law on Energy" 14 July, 2022. Accessible on: https://likumi.lv/ta/id/334350-grozijumi-energetikas-likuma.

Balkan Investigative Reporting Network: *Montenegro needs to bolster cyber security institutions, June 2024, available at:* https://balkaninsight.com/2024/06/24/montenegro-needs-to-bolster-cyber-security-institutions-birn-report.

Balodis, Marcis/ Marta Kepe: Lessons from Latvia's Efforts to Keep Essential Services Running During a Crisis, Atlantic Council – *New Atlanticist*, 07.05.2025, available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/lessons-from-latvias-efforts-to-keep-essential-services-running-during-a-crisis/ (last accessed 15.09.2025).

Bennett, Tom.: Baltic states unplug from Russia and join EU power grid, in: BBC News (bbc.com), 09.02.2025.

Boost in cyber resilience of Ukrainian critical infrastructure, EGA, Estonia, https://ega.ee/ukrainian-critical-infrastructure/.

Borzel, Tanja A. /Tobia Hofmann/Diana Panke/Carina Sprungk: Obstinate and inefficient: why member states do not comply with European law, in *Comparative Political Studies*, 43(11), 2010, p. 1363–1390.

Borzel, Tanja A. /Ulrich Sedelmeier: Larger and more law abiding? The impact of enlargement on compliance in the European Union, in *Journal of European Public Policy*, 24 (2), 2017, p. 197–215.

Brendler, Viktoria /Eva Thomann: Does institutional misfit trigger customisation instead of non-compliance? In *West European Politics*, 47(3), 2024, p. 515–542.

Budginaite-Froehly, Justina.: Baltic States unplug from Russia's power grid – but Moscow still looms over critical infrastructure, in Atlantic Council, 05.02.2025.

Cabinet of Ministers Regulation No. 139, "Implementing rules of the European Cybersecurity Competence Centre grant programme "Cybersecurity Transformation of Small and Medium-sized Enterprises" for the 2021-2027 programming period" February 27, 2024. Accessible on: https://likumi.lv/ta/id/350225-eiropas-kiberdrosibas-kompetencu-centra-20212027-gada-planosanas-perioda-grantu-programmas-mazo-un-videjo-saimnieciskas-darbibas-veiceju-kiberdrosibas-transformacija-istenosanas-noteikumi.

CEP, *Reforming the EU's pre-accession funding instrument*, September 2023, available at: https://cep.org.rs/wp-content/uploads/2023/09/Reforming-the-EUs-pre-accession-funding-instrument.pdf.

CER Directive (see https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32022L2557 (accessed 16.07.2025).

CERT.LV Activity Report Q4 2024, 27.02.2025, available at: http://cert.lv/uploads/eng/CERT_Report_2024_Q4_ENG.pdf (last accessed 15.09.2025).
Civil Georgia: Bloomberg: *Russia Hacked Entire Georgia Between 2017-2020,* October 21, 2024, available at: https://civil.ge/archives/629367.

Civil Georgia: *Georgian Dream to Abolish National Security Council*, June 16, 2025, available at: https://civil.ge/archives/687308.

Competition Market Study of Ukraine's Electricity Sector, https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/competition-market-study-of-ukraine-s-electricity-sector_045239a1/f28f98ed-en.pdf.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008.

Council of Europe Parliamentary Assembly Resolution 2585, January 29, 2025, available at: https://pace.coe.int/en/files/34147.

Council recommendation of 25 June 2024 on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance OJ C, C/2024/4371, 5.7.2024.

Coyle, Carmel: Administrative capacity and the implementation of EU environmental policy in Ireland, in *Regional Politics and Policy*, 4, 1994, p. p. 62-79.

Cyber Resilience Act, European Commission, available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine , https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf.

Dimitrakopolous, Dionyssis/Jeremy Richardson: Implementing EU public policy, In Jeremy Richardson (ed.) European Union. Power and Policy-making, Routledge, 2nd edition, 2001, p. 335-356.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ L 333, 27.12.2022.

EGA: Boost in cyber resilience of Ukrainian critical infrastructure, Estonia, available at: https://ega.ee/ukrainian-critical-infrastructure/ (last accessed 15.09.2025).

ENISA: Implementing Guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures, October 2024.

EU ME, *Chapter 5 - Public procurement, June 2025.* https://www.eu.me/en/poglavlje-5-javne-nabavke/.

European Commission: *Montenegro report 2024,* October 2024, available at: https://enlargement.ec.europa.eu/document/download/a41cf419-5473-4659-a3f3-af4bc8ed243b_en

European Commission: Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism, COM/2004/0702, 2004.

European Commission: Green Paper on a European programme for critical infrastructure protection, COM/2005/0576, 2005.

European Commission: European Reference Network for Critical Infrastructure Protection: ERNCIP Handbook 2018 edition, Joint Research Centre Technical report, 2018.

European Commission: "The European Programme for Critical Infrastructure Protection", MEMO/06/477, 12 December 2006, available at: http://ec.europa.eu/commission/presscorner/detail/en/memo_06_477 (last accessed 05.09.2025).

European Commission: Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2 April 2019, available at: https://op.europa.eu/en/publication-detail/-/publication/118dcd3d-b041-11ea-bb7a-01aa75ed71a1/language-en (last accessed 05.09.2025).

European Commission: Commission Staff Working Document - Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, SWD/2020/345 final - part 1/3, 2020.

European Commission: ReArm Europe Plan/Readiness 2030, available at: https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en (last accessed 24.10.2025).

European Commission and the High Representative of the Union for Foreign Affairs and Security Policy: Preparedness Union Strategy, JOIN(2025) 130 final, 2025.

European Commission: Communication from the Commission on Protect EU: a European Internal Security Strategy, no. COM (2025) 148 final, 2025.

European Union: *Cyber Direct Montenegro, 2023, available at:* https://eucyberdirect.eu/atlas/country/montenegro.

EU NEIGHBOURS east, *Georgia accession process de facto halted as EU calls on government to change course*, October 30, 2024, available at: https://euneighbourseast.eu/news/latest-news/georgia-accession-process-de-facto-halted-as-eu-calls-on-government-to-change-course/.

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

European Parliament, "*Parliament Deplores the Democratic Backsliding and Repression in Georgia.*" Press release, 4 July 2025. Available at: https://www.europarl.europa.eu/news/en/press-room/20250704IPR29451/parliament-deplores-the-democratic-backsliding-and-repression-in-georgia.

European External Action Service: Assessment of Cybersecurity Risks in Montenegro: Challenges and Recommendations'. EU Publications, 2 October, 2023, available at: https://www.eeas.europa.eu/sites/default/files/documents/2024/Montenegro%20Report%202024.pdf (last accessed 21.01.2025).

European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024*, September, 2024, available at: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf.

Executive order of the Prime Minister No. 2024/1.2.1.-416 "On the National Cybersecurity Council", December 6, 2024. Accessible on: https://likumi.lv/ta/id/357025-par-nacionalo-kiberdrosibas-padomi.

Falkner, Gerda /Oliver Treib: Three worlds of compliance or four? The EU-15 compared to new member states, in *Journal of Common Market Studies*, 46(2), 2008, p. 293-313.

Federation of employers of Ukraine, available at: https://www.facebook.com/story.php?story_fbid=1401645161443436&id=100047938970171&mibextid=wwXIfr&rdid=jj9ltvGj0ku4XevN# (last accessed 15.09.25).

Finland's Prime Minister's Office: Finland's Cyber Security Strategy 2024-2035, 25 October 2024, available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf?sequence=1&isAllowed=y (last accessed 25.10.2025).

Finland's Ministry of the Interior: Kriittistä infrastruktuuria koskevan sääntelyn uudistaminen – Sisäministeriö, available at: https://intermin.fi/hankkeet/kriittinen-infrastruktuuri (last accessed 24.10.2025).

Finland's Security Committee: Comprehensive Security, 23 June 2025, available at: https://turvallisuuskomitea.fi/en/comprehensive-security/ (last accessed 24.10.2025).

Godzimirski, Jakub/Ramūnas Vilpišauskas/Romas Švedas: *Energy Security in the Baltic Sea Region: regional coordination and management of interdependence*, Vilnius University Press, 2015, available at: https://nupi.brage.unit.no/nupi-xmlui/handle/11250/296761.

Government of Georgia, Decree №482 on the approval of the National Cyber Strategy and Action Plan. September 30, 2021, available at: https://matsne.gov.ge/document/view/5263611?publication=0.

Government of Montenegro: *Cybersecurity Strategy of Montenegro 2022-2026*, June 2022. Available at: https://www.gov.me/en/documents/85e2a9d0-0d3c-483a-9822-515d3b7798de.

Gvineria, Sh.: *'The Roots of Georgia's Political Crisis'*, February 8, 2025, Available at: https://politicsgeo.com/the-roots-of-georgias-political-crisis/
Hogwood, Brian W. /Lewis A. Gunn: Policy analysis for the real world. Oxford University Press, 1984.

Institute for Development of Freedom of Information (IDFI), *Georgian Parliament should not support Draft Amendments to the Law of Georgia on Information Security,* May 29, 2020, Available at: https://idfi.ge/en/law-on-information-security.

Iso-Markku, Tuomas and Niklas Helwig: The Niinistö report on preparedness: Finland's lessons for the EU and their limitations, FIIA Comment 9, 2024, https://fiia.fi/en/publication/the-niinisto-report-on-preparedness.

Jaćimović, Danijela /Milena Lipovina-Božović/Bojan Pejović/Suncica Vuković: The Impact of Infrastructure Development on the Economic Growth of the Countries in the Western Balkans and their EU Future. *Prague Economic Papers*, 34(1), 2025.

Jauhiainen, Lauri. 2025. Vital Meets Critical: Comparing the Finnish Comprehensive Security Model and the European Union's Resilience Legislation. Master's Thesis, National Defence University. https://www.doria.fi/handle/10024/193001.

Knill, Christoph /Andrea Lenschov: Coping with Europe: the impact of British and German administrations on the implementation of EU environmental policy, In *Journal of European Public Policy*, 5(4), 1998, p. 595-614.

Knill, Christoph /Dirk Lehmkuhl: The national impact of European Union regulatory policy, in *European Journal of Political Research*, 41(2), 2002, p. 255-280.

Lampinen, Peter /Petri Uusikyla: Implementation deficit – why member states do not comply with EU directives, in *Scandinavian Political Studies*, 21, 1998, p. 231-251.

Latvian State Security Service: Annual Report on the Activities of the Latvian State Security Service (VDD) in 2024, 02.2025, available at: https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf (last accessed 15.09.2025).

Law of Ukraine 4336-IX dated 27.03.25, On Amendments to Certain Laws of Ukraine on Information Protection and Cybersecurity of State Information Resources and Critical Information Infrastructure Facilities https://zakon.rada.gov.ua/laws/show/4336-IX#Text.

"Law on National Cybersecurity" June 20, 2024. Accessible on: https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums.

"Law on National Security", 14 December, 2000. Accessible on: https://likumi.lv/doc.php?id=14011.

Lithuania's National Security Strategy, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3ec6a2027a9a11ecb2fe9975f8a9e52e?jfwid=rivwzvpvg (last accessed 27.10.2025).

LSM+: Interview: Volunteers on the front line of Latvia's cyber defense capability, in: LSM (eng.lsm.lv), 24.07.2024.

LV Portāls: The Regulatory Framework on the Functioning of the Crisis Management Centre Comes into Effect, 01.07.2025, available at: https://lvportals.lv/skaidrojumi/377945-stajas-speka-regulejums-krizes-vadibas-centra-darbibai-2025 (last accessed 16.09.2025).

Mazmanian, Daniel A. /Paul A. Sabatier: Implementation and Public Policy. Bloomsbury Academic, 1989.

Mbaye, Heather: Why national states comply with supranational law: explaining implementation infringements in the European Union, 1973-1993, in European Union Politics, 2, 2001, p. 259-81.

Merikuljetukset Suomessa: Logistiikan Maailma, 5 March 2025, available at: https://mmm.fi/en/nature-and-climate/climate-change-adaptation/national-climate-change-adaptation-plan-2030 (last accessed 24.10.2024).

Mikac, Robert: Protection of the EU's Critical Infrastructures: Results and Challenges, in: Applied Cybersecurity & Internet Governance, vol. 2, no. 1, 2023.

Ministry of Agriculture and Forestry of Finland: National Climate Change Adaptation Plan 2030, 2 April 2024, available at: https://mmm.fi/en/nature-and-climate/climate-change-adaptation/national-climate-change-adaptation-plan-2030 (last accessed 24.10.2025).

Ministry of Defence of the Republic of Latvia: "Comprehensive National Defence", available at: https://www.mod.gov.lv/lv/nozares-politika/visaptverosa-valsts-aizsardziba.

Ministry of the Interior of the Republic of Latvia: Government strengthens critical infrastructure resilience and national security, 21.03.2025, available at: https://www.iem.gov.lv/en/article/government-strengthens-critical-infrastructure-resilience-and-national-security (last accessed 16.09.2025).

Ministry of Interior: *Zakon o odredjivanju i zaštiti kritične infrastructure*, January 2020,available at: https://www.gov.me/en/documents/2585570a-cdff-420f-a7c4-0f67f19a6d8e.

Ministry of Public Administration, *Directorate for Information Security and Gov-CIRT, 26 October 2024,* available at: https://www.gov.me/clanak/drzavne-institucije-privrede-i-gradani-u-crnoj-gori-od-danas-bezbjedniji-u-internet-okruzenju.

Ministry of Public Administration, *Western Balkans Cyber Capacity Centre*, December 2024, https://www.gov.me/clanak/otvoren-regionalni-centar-za-sajber-kapacitete-zapadnog-balkana-dan-za-pamcenje.

Ministry of Public Administration: *Zakon o informacionoj bezbjednosti*, December 2024, available at: https://www.gov.me/en/documents/23936380-482a-4784-bd94-be69413d7334
National Cyber Security Centre under the Ministry of Defence of Lithuania, https://www.nksc.lt/en/ (last accessed 27.10.2025).

National Security Concept of Georgia, December 23, 2011, available at: https://matsne.gov.ge/document/view/1555410?publication=0.

Niinistö, Sauli. 2024. 'Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness', can be accessed at https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf.

NIS2 Directive (see https://eur-lex.europa.eu/legal-content/en/NIM/?uri=CELEX:32022L2555 (accessed 16.07.2025).

OECD: *Mobilising Evidence at the Centre of Government in Lithuania*, OECD Publishing, 29 November 2021, available at: https://www.oecd.org/en/publications/mobilising-evidence-at-the-centre-of-government-in-lithuania_323e3500-en.html.

OSCE Office for Democratic Institutions and Human Rights: *Georgia's foreign agents legislation raises concerns over negative impact on civil society,* April 2, 2025, available at: https://www.osce.org/odihr/588667.

Parliament of Georgia, Criminal Code of Georgia, July, 1999, available at: https://matsne.gov.ge/document/view/16426?publication=284.

Parliament of Georgia, Law of Georgia on Information Security, July, 2012, available at: https://matsne.gov.ge/document/view/1679424?publication=8.

President of Georgia, Decree №707, Georgia's Threat Assessment Document, September 2, 2010, available at: https://matsne.gov.ge/document/view/1032959?publication=0.

Pressman, Jeffrey L. /Aaron Wildavsky: Implementation. How great expectations in Washington are dashed in Oakland; or, why it's amazing that federal programs work at all, this being a saga of the economic development administration as told by two sympathetic observers who seek to build morals on a foundation. University of California Press, 1973.

Pridham, Geoffrey: National environmental policy-making in the European framework: Spain, Greece and Italy in comparison, in *Regional Politics and Policy*, 4, 1994, p. 80-101.

Prior, Tim: *Measuring Critical Infrastructure Resilience: Possible Indicators*, Risk and Resilience Report 9, Centre for Security Studies (CSS), ETH Zurich, 2014.

Pursiainen, Chirster /Eeero Kytömaa: From European critical infrastructure protection to the resilience of European critical entities: what does it mean?, in: *Sustainable and Resilient Infrastructure*, vol. 8 (sup1), 2022, pp. 85-101.

Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010. OJ L 280, 28.10.2017.

Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, OJ L 158, 14.6.2019.

Regulation of the Cabinet of Ministers No. 508, "Procedures for the identification, security measures and business continuity planning and implementation of critical infrastructure, including European critical infrastructure" July 6, 2021. Accessible on: https://likumi.lv/ta/id/324689-kritiskas-infrastrukturas-taja-skaita-eiropas-kritiskas-infrastrukturas-apzinasanas-drosibas-pasakumu-un-darbibas-nepartrauktibas-planosanas-un-istenosanas-kartiba.

Rimutis, Saulius: Lessons of war: Ukraine's energy infrastructure damage, resilience, and future opportunities, Eastern Europe Studies Centre, https://www.gssc.lt/wp-content/uploads/2024/05/v04_Rimutis_Ukrainos-energetikos-sektoriaus-zala_EN_A4.pdf
Sabatier, Paul A.: Top-Down and Bottom-Up Approaches to Implementation Research: a Critical Analysis and Suggested Synthesis, *In Journal of Public Policy*, 6(1), 1986, p. 21-48.

Schimmelfennig, Frank /Ulrich Sedelmeier: Governance by conditionality: EU rule transfer to the candidate countries of Central and Eastern Europe, in *Journal of European Public Policy*, 11(4), August 2004, p. 661-679.

Security Service of Georgia: *2024 Annual Report*, available at: https://ssg.gov.ge/page/info/reports.

Sedelmeier, Ulrich: After conditionality: post-accession compliance with EU law in East Central Europe, in *Journal of European Public Policy*, 15(6), September 2008, p. 806-825.

Seskuria, N.: *Russia's 'Hybrid Aggression' against Georgia: The Use of Local and External Tools,* Center for Strategic and International Studies, September 21, 2021, available at: https://www.csis.org/analysis/russias-hybrid-aggression-against-georgia-use-local-and-external-tools.

Setola, Roberto /Eric Luiijf/Marianthi Theocharidou: Critical Infrastructures, Protection and Resilience, in: Roberto Setola et al. (eds.) *Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach*. SpringerOpen, 2016.

State Security Department of Lithuania at https://www.vsd.lt/en/archive-national-threat-assessments/ (last accessed 27.10.2025).

Statement, Parliamentary Assembly of the Council of Europe, "As Situation in Georgia Continues to Deteriorate, Assembly Sets Out Additional Demands to Reverse Democratic Backsliding," April 10, 2025, Available at: https://www.coe.int/en/web/portal/-/as-situation-in-georgia-continues-to-deteriorate-assembly-sets-out-additional-demands-to-reverse-democratic-backsliding.

Sutt, Andres/Kaspars Melnmis/Žygimantas Vaičiūnas/Paulina Hennig-Kloska: Joint Letter of the Ministers for Energy of Estonia, Latvian, Lithuania and Poland to Dan Jorgensen, the European Commissioner for Energy and Housing, 13 May, 2025.

Tallberg, Jonas: Paths to Compliance: Enforcement, Management and the European Union, in *International Organization*, 56 (3), summer 2002, p. 609-643.

Tammikko, Teemu: The EU and NATO in pursuit of better deterrence: Baltic Sea sabotage prompts rethink of current practices, FIIA Briefing Paper 404, January 2025.
Tammikko, Teemu: 2019. Vihalla ja voimalla: poliittinen väkivalta Suomessa. Helsinki: Gaudeamus.

Thomas de Waal, "The Orbanizing of Georgia," *Carnegie Endowment for International Peace: Strategic Europe*, August 31, 2023, Available at:https://carnegieendowment.org/europe/strategic-europe/2023/08/the-orbanizing-of-georgia?lang=en.

Thomson, Robert /Rene Torenvlied/Javier Arregui: The Paradox of Compliance: Infringements and Delays in Transposing European Union Directives, in *British Journal of Political Science*, 37, 2007, p. 685-709.

Traficom: Määräyshankepäätös: Määräys viestintäverkon kriittisistä osista, 24 January 2025, available at: https://traficom.fi/fi/ajankohtaista/maarayshankepaatos-maarays-viestintaverkon-kriittisista-osista-0 (last accessed 25.10.2025).

Ukraine: 3d Cyber Dialogue with the European Union takes place in Brussels, available at: https://digital-strategy.ec.europa.eu/en/news/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels.

Ukraine to receive €100 million from EU for the reconstruction of electricity transmission system, https://euneighbourseast.eu/news/latest-news/ukraine-to-receive-e100-million-from-eu-for-reconstruction-of-electricity-transmission-system/.

Ukraine War Environmental Consequences Work Group (UWEC): Environmental consequences of the war in Ukraine: October-November 2024 Review, available at: https://uwecworkgroup.info/environmental-consequences-of-the-war-in-ukraine-october-november-2024-review/ (last accessed 19.09.25).

United Nations Ukraine: Attacks on Ukraine's energy infrastructure: harm to the civilian population, , available at: https://ukraine.un.org/en/278992-attacks-ukraine's-energy-infrastructure-harm-civilian-population (last accessed 16.10.25).

Valtonen, Vesa & Minna Branders: Tracing the Finnish Comprehensive Security Model. In: Larsson, S., & Rhinard, M (eds.). *Nordic Societal Security: Convergence and Divergence* (1st ed.). Routledge, 2020.

Vijesti, *EC: Conditions for closing Chapter 5 fulfilled...* June 2025. Available at: https://en.vijesti.me/news-b/politika/761159/EC-fulfilled-the-conditions-for-closing-Chapter-5--the-implementation-of-the-agreement-with-the-UAE-to-be-in-line-with-European-legislation.

Vijesti: *Dukaj: Cyber resilience requires a strategic approach by every government, November 2023, available at:* https://en.vijesti.me/news-b/society/682595/dukaj-cyber-resilience-requires-a-strategic-approach-by-every-governmen.

Vilpišauskas, Ramūnas: Regulatory patchwork that evolved in response to external threats, legal approximation and domestic influences, in: Maris Andžans/Andris Sprūds/Ulf Sverdrup (eds.): Critical Infrastructure in the Baltic States and Norway: strategies and practices of protection and communication, Latvian Institute of International Affairs, 2021, p. 59-97.

Ramūnas Vilpišauskas: Gradually and then suddenly: the effects of Russia's attacks on the evolution of cybersecurity policy in Lithuania, In *Policy Studies*, 45 (3-4), p. 467-488.

Vilpišauskas, Ramūnas, et al: *Invigorating enlargement and neighbourhood policy for a resilient Europe: Long policy report on rules alignment of protecting critical infrastructure in interdependent states* (InvigoratEU Report D7.1), 2025, available at: https://invigorat.eu/wp-content/uploads/2025/03/D7.1_InvigoratEU_long-policy-report_public.pdf.

White Book of Reforms 2025. Chapter 7. Energy sector reforms in Ukraine, VoxUkraine Team Reforms, https://voxukraine.org/en/white-book-of-reforms-2025-energy-sector-reforms-in-ukraine.

Interviews conducted and personal communication:

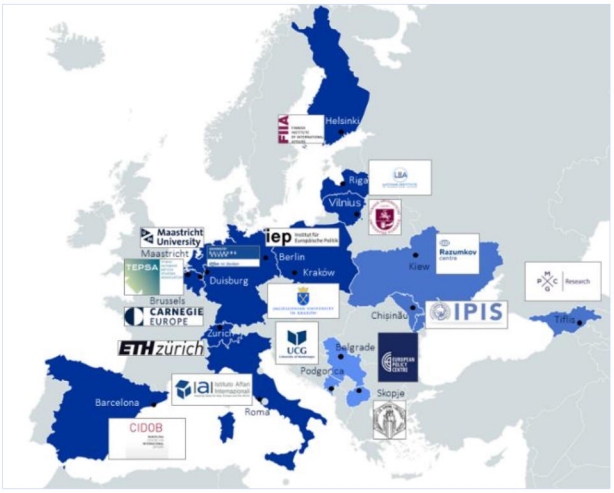
1. Interview with representative from CERT.LV, 2 September 2025, Riga.
2. Interview with representative of "Latvijas Mobilais Telefons", September 17, 2025, Riga.
3. Interview with the senior official of the Ministry of Defence of Lithuania, September 5, 2025, Vilnius.
4. Interview with senior officials from the National Crisis Management Centre of Lithuanian Government, August 26, 2025, Vilnius.
5. Interview with senior officials from the National Cyber Security Centre under the Ministryf of Defence of Lithuania, September 4, 2025, Vilnius.
6. Interview with the senior management of the Lithuania's energy company LITGRID, March 4, 2025, Vilnius.
7. Interview with the senior management of telecommunications company TELIA, March 6, 2025, Vilnius.
8. Interview with the senior official of the Ministry of Energy of Lithuania, August 8, 2025, Vilnius.
9. Interview with the senior official of the Ministry of Energy of Lithuania, July 31, 2025, Vilnius.
10. Interview with the senior official of the Communications Regulatory Authority of Lithuania, September 3, 2025, Vilnius.

11. Interview with the Montenegro Ministry of Interior's officials, October 17, 2024, via Zoom.
12. Interview with Dušan Polović, Director General of the Directorate for Infrastructure, Information Security, and Digitalization, Ministry of Public Administration, May 18, 2025, Podgorica.
13. Interview with Ivan Bulatovic, General Manager of Elektroprivreda Crne Gore-EPCG the largest energy company, May 25, 2025, Podgorica.
14. Interview with experts in IT department Montenegro Electric Power Company on September 10, 2025, Podgorica.
15. Interview with Savo Kentera, expert in security and international relations, the President of the Atlantic Alliance of Montenegro, September 8, 2025, Podgorica.
16. Interview with Ivan Stanković of the private IT company Čikom September 8, 2025, Podgorica.
17. Interview with former high official of a state cyber security agency of Georgia, September 1, 2025, Tbilisi.
18. Interview with the founder of a Georgian cyber security civil society organisation, September 1, 2025, Tbilisi.
19. Interview with the former Georgian government official, Security Policy Expert, September 4, 2025, Tbilisi.
20. Interview with the director private cyber security consulting company, September 10, 2025, Tbilisi.
21. Communication with the Verkhovna Rada of Ukraine representative on CI protection in the written format (received on 19.09.2025).
22. Communication with the former executives of Ukrainian TSO (Ukrenergo) on CI protection in the written format (received on 19.09.2025).
23. Communication with the NEURC representative on CI protection in Ukraine in the written format (received on 11.09.2025).

About InvigoratEU

InvigoratEU is a Horizon Europe-funded project, coordinated by the EU-Chair at the University of Duisburg-Essen (UDE) together with the Institut für Europäische Politik (IEP) in Berlin. The project, with a duration of 3 years from January 2024 until December 2026, examines how the EU can structure its future relations with its Eastern neighbours and the countries of the Western Balkans. The consortium has received around three million euros for this endeavour.

How can the EU invigorate its enlargement and neighbourhood policy to enhance Europe's resilience?



Our first goal is to investigate how to reform the EU's enlargement strategy in a new geopolitical phase, HOW TO RESPOND to other actors' geopolitical ambitions in the Eastern Neighbourhood and Western Balkans, and HOW TO REBUILD the EU's foreign policy arsenal in view of a new era of military threats (triple "R" approach) combining the modernisation and geopolitical logics of EU enlargement, leading to new data – e.g. a public opinion survey in Ukraine, a set of scenarios, an external influence index (Russia, China, Turkey), and a social policy compliance and cohesion scoreboard.

Our second goal is to elaborate an evidence-based, forward-looking vision for the EU's political agenda and institutional frameworks for co-designing a multidimensional toolbox (i.e. two tailor-made toolkits), together with InvigoratEU's Expert Hub, Civil Society (CS) Network, Youth Labs, Workshops for Young Professionals and Policy Debates in a gaming set up, which will result in context-sensitive and actionable policy recommendations for European and national political stakeholders and (young) European citizens in particular.

Our third goal is to deploy a CDE (communication, dissemination and exploitation) strategy aiming at recommendations from Day 1 to maximize our scientific, policy and societal impact in invigorating the EU's enlargement and neighbourhood policies to enhance Europe's resilience. Ultimately, InvigoratEU is a deliberately large consortium respecting the diversity of Europe and political perspectives; 7 out of 18 are from Georgia, Moldova, Ukraine, and the western Balkans (North Macedonia, Montenegro, Serbia), complemented by our Civil Society Network of 9 representatives from all Western Balkan countries, Georgia, Moldova and Ukraine.

InvigoratEU is funded by the European Union.