InvigoratEU

Invigorating Enlargement And Neighbourhood Policy For A Resilient Europe

Long Policy Report on rules alignment of protecting critical infrastructure in interdependent states

Authors

Ramūnas Vilpišauskas, Sergejs Potapkins, Svitlana Chekunova, Danijela Jacimovic, Gocha Kardava, Marco Siddi, Nana Tabagua

Funded by the European Union

Executive summary

The report provides an extensive discussion of evolving landscape of threats to the CI in the EU and selected candidate countries in recent years and the challenges which, while varying depending on particular countries, also are common to all states affected by geopolitical tensions. The analysis of threats to energy, communications, transport and other CI in the Baltic States, Ukraine and the Baltic Sea region shows that hostile activities by authoritarian states, in particular, Russia, or actors linked to them have become increasingly frequent. Their proliferation especially intensified after Russia's full-scale war against Ukraine in 2022, as it also became a wider confrontation between the West and authoritarian powers. The analysis of CI-related policies in Montenegro, Ukraine and Georgia – three candidate countries, which differ in terms of their state of accession into the EU, their connectivity patterns and risks to their CI associated with them – allows to assess different challenges arising to their CI and provision of vital services to society and state and methods of coping with them in each of them. The report concludes with recommendations emphasising the importance of daily practices of partnership and exercises involving all stakeholders of CI ecosystems and cooperation with the EU and NATO partners, taking into account different patterns of interdependencies and existing threats.

Authors

Ramūnas Vilpišauskas
Professor
Department of International Relations
Vilnius University

Sergejs Potapkins
Research Associate
Agora Strategy Group A
Latvian Institute of International Affairs

Svitlana Chekunova
Research Associate
The Razumkov Centre

Danijela Jacimovic
Professor
Univerzitet Crne Gore

Gocha Kardava
Research Associate
PMCG - Research

Marco Siddi
Assistant Professor
Finnish Institute of International Affairs

Nana Tabagua
Lead Researcher
PMCG - Research

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.17340020

Funded by the European Union

Contents

1 Introduction

This policy report provides analysis of the debates on the protection and resilience of critical infrastructure in the EU Member States and selected candidate countries. It aims to provide the basis for the assessment of the most recent 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.

The focus on critical infrastructure (CI) – assets that are essential for the functioning of society and economy – is grounded in the understanding of its increasing relevance for the security and resilience of the EU and candidate countries. As explained in the next chapter, in recent decades for a number of technological, geopolitical, environmental and other reasons there has been a growing attention of analysts and policy-makers dedicated to the protection and resilience of CI such as energy, communications, transport and other which is considered vital for contemporary societies. Therefore, analysis of debates surrounding these issues is an important element in the holistic approach to strengthening Europe's resilience and invigorating enlargement and neighbourhood policy for a resilient future.

The report starts with the presentation of the scholarly debates and policy trends related to the protection and resilience of CI. First, the main concepts as well as trends, in particular the shift in focus from protection to resilience and adoption of all-hazard approach are discussed. Then it outlines the rationale for the cross-border cooperation in this field as well as other methods of increasing resilience of CI entities such as private and public partnerships, sharing of information and institutional roles.

After outlining the practices for enhancing CI resilience, the report investigates the most recent incidents and attacks on the CI of the EU Member States and candidate countries, including cyber-attacks in the Baltic States, cyber and kinetic attacks in Ukraine against energy, transport and communications infrastructure, and incidents and suspected sabotage against energy and telecommunications infrastructure under the Baltic Sea connecting the countries around it.

The purpose of these analyses is to show the evolving nature of the current challenges facing the EU, its Member States and candidate countries, the importance of protecting CI and the lessons learned with respect to enhancing protection and resilience of their CI. The Baltic States have been chosen due to their geographical position and recent experiences in diversifying away from aggressive authoritarian neighbours to increase their interdependencies in energy, transport and other sectors with EU/NATO partners and upgrading their CI-related policies. In response to cyber attacks attributed to Russia, the Baltic States have developed their cyber security policies which can be considered good practices having lessons for current candidate countries. Meanwhile, hybrid and kinetic attacks against CI in Ukraine illustrate both the challenges experienced by this candidate country and the methods of responding to them and (re)building capacity which can be useful to other European countries.

In addition, the report zooms into three candidate countries - Montenegro, Ukraine and Georgia - to assess the state of the debates on protection and resilience of CI there. The countries selected represent three different cases in terms of their state of integration into the EU, the patterns of interdependencies and the actual threats to their CI. On the basis of desk research and exploratory interviews, it presents the main trends in the current debates on CI related policy issues, the main challenges and actual practices compared to those which are considered good practices by the OECD and other international organisations. It also investigates policy conflicts between the EU's integration-driven demands and interdependencies with authoritarian countries and other factors which inhibit the enhancement of resilience of CI entities in line with best practices.

The report concludes with general observations on the key trends in terms of evolving threats to the CI of EU members and candidate countries, current challenges related to its protection and resilience as well as policy recommendations.

2 Literature review

The concept of critical infrastructure

The public attention to the infrastructure considered particularly important for the functioning of state and well-being of society could be traced back to the Ancient Roman times (i.e. protection of aqueducts and roads used for dual purpose). However, in modern times it was in the US that the public policy debate on the need to protect critical infrastructure initially emerged and soon expanded to other OECD countries.

In 1990s, the Clinton administration introduced regulation aimed at outlining the set of actions needed to protect critical infrastructure (CI) which was defined as "those physical and cyber-based systems essential to the minimum operations of the economy and government".[1] In the 2000s, the European Commission also took initiative to, first, present a Green Paper on a European Program for Critical Infrastructure Protection (17 November 2005), then followed by the Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

The Directive 2008/114/EC defined CI as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".[2] This legislation referred to CI of European dimension, but it also triggered increasingly more EU Member States to identify their national CI as well.[3]

[1] The US Presidential Decision Directive PDD-63 quoted in 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, p. 2.
[2] 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 (text with relevance to EEA), available at https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng (last accessed: 10.01.2025).
[3] Roberto Setola/Eric Luiijf/Marianthi Theocharidou: Critical Infrastructures, Protection and Resilience, 2016.

During the last two decades policy initiatives on both national and EU levels proliferated aiming at protecting CI and increasingly focusing on strengthening its resilience. The EU introduced new legislation that expanded the range of sectors, services and type of critical entities covered by supranational norms and replaced earlier directives.[4] Although initially EU legislation on CI applied to energy and transport sectors, gradually its scope was enlarged to include many other sectors and essential services such as information and elecommunications, financial services, health care, food and others. Meanwhile in addition to adopting supranational norms, EU Member States have been developing national policy measures, often linked to a changing landscape of perceived threats to national security.[5]

A number of factors explain the increasing importance of protecting CI and in turn higher levels attention paid by policy-makers and experts to developing measures aimed at protecting CI and enhancing its resilience. Initially those factors included: policy driven changes in regulatory environment, such as unbundling of power generation, transmission and distribution in the electrical power sector, liberalisation of telecommunications and other formerly state-owned monopolies; technological developments, in particular, spread of information and communication systems, advances in the use of internet and smart phones, etc.; economic factors such as growing cross-border exchanges and diffusion of ideas and policy paradigms such as smart grids, smart cities, cooperation between private and public actors and shifting focus on resilience in addition to or rather than protection (the latter trend is discussed in more detailed below).[6]

At the same time, the growing number of incidents due to malfunctioning of increasingly complex systems and extreme weather events, as well as malicious activities such as cyber-attacks, terrorism and other types of hybrid attacks, focused policy makers' attention on the search for methods of preventing and mitigating the disruptive effects on the functioning of CI. In particular, Europe became a playground of authoritarian powers, such as Russia, Belarus, China and North Korea, testing the functioning of CI in the EU Member States and candidate countries through cyber-attacks and sabotage in addition to disinformation, orchestrating illegal migration flows and other instruments of hybrid attacks. Following the full-scale Russian invasion of February 2022, Ukraine also experienced kinetic attacks on its CI, especially energy infrastructure.

Rising geopolitical tensions led many European democracies to introduce new rules and safeguards with respect to the ownership, foreign investment screening, restricting the use of foreign technologies, assigning institutional roles and upgrading routines aimed at regular exercises involving private actors and institutions from partner countries, performing risk management and assessing potential vulnerabilities.

---

[4] For the up-to-date list of EU's legal initiatives see the relevant site of the European Commission: Critical infrastructure resilience at EU-level, 23 September 2024, available at https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en (last accessed 10.01.2025).

[5] For the evolution of CI policies in the Baltic States see Māris 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.

[6] See Roberto Setola et al. (eds.) Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, 2016.

Finally, as a sign of acknowledging the importance of adapting CI policies to real world developments, national and EU funding for research related to protection of CI and enhancing its resilience, often also linked to the crises management analysis, has been on the rise.[7]

From protection to resilience of critical infrastructure

One of the most noted shifts in the paradigm of CI protection in recent decades among the OECD countries, led again by the US, was a growing focus on increasing resilience related to the acknowledgement that, due to the adverse and changing landscape of hazards and threats to CI and provision of vital services, complete protection – foreseeing, preventing, preparing or mitigating those events – is not realistic.

This could be considered a reflection of the broader "resilience turn" and living under "the permanent state of adaptation".[8] More concretely, it has been argued that due to occurrence of environmental disasters, growing frequency of terror attacks and other hostile activities causing disruptions of vital services and threatening our way of living and our very existence, we "must learn to be more resilient in the face of an unknown and unpredictable future".[9]

In the EU's Global Strategy adopted in 2016, resilience has been defined as "the ability of states and societies to reform thus withstanding and recovering from internal and external crises".[10] Initially resilience referred to being able to bounce back from disruption and return to normality as quickly as possible, while more recently it was replaced by bouncing forward to a new normal and putting in place plans for coping with risks that cannot be accurately predicted in advance.[11]

Holistic approach to resilience situates it within the context of broader connectivity and market integration, and it includes societal and state resilience. The application of a resilience-focused approach to the functioning of CI and provision of vital services starts from stating the fact that different critical infrastructures are closely linked and dependent on each other and it is this interconnectedness, complexity and 'system of systems' networking which directs attention to its resilience. Increasing attention to complex and intertwined risks and the cascading effects of a breakdown in one system on other networked systems should lead to a proactive response in terms of risk management. This would allow assessing the ability of complex infrastructure systems to maintain function safely, adapt, and recover

[7] Roberto Setola/Eric Luiijf/Marianthi Theocharidou: Critical Infrastructures, Protection and Resilience, 2016. Also see European Commission: European Reference Network for Critical Infrastructure Protection: ERNCIP Handbook 2018 edition, Joint Research Centre Technical report, 2018, and European Commission activities on Critical Infrastructure Protection in the EU Science Hub, available at https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en (last accessed 10.01.2025).

[8] The origins of the resilience approach are often attributed to the book by German sociologist Ulrich Beck: Risk Society: Towards a New Modernity, published in German in 1986 and translated into English in 1992 by Sage Publications. For more recent studies see Jon Coaffee: Future Proof. How to Build Resilience in an Uncertain World, Yale University Press, 2019; Markus K. Brunnermeier: The Resilient Society, Endeavor Literary Press, 2021.

[9] Jon Coaffee: Future Proof. How to Build Resilience in an Uncertain World, 2019, p. 5.

[10] European External Action Service: European Union Global Strategy, 2016, p. 23.

[11] For a more extensive discussion of the concept of resilience and its use in the EU, its enlargement and neighbourhood policies see Hannah Brandt/Funda Tekin/ Pol Bargues, Ramūnas Vilpišauskas: Growing Resilient Together: Reshaping EU Enlargement and Neighbourhood Policy in a Geopolitical Era, InvigoratEU Conceptual Background Paper, 2024, available at https://invigorat.eu/invigorateu-publications/ (last accessed 11.01.2025).

from disruption as quickly as possible.[12] A resilience-based approach encompasses both elements of protection and adaptation deployed at various points during disruption or crisis.

Thus, "resilience is considered as the capacity of a critical infrastructure and its operative environment to combat in a preventive and adaptive manner adverse conditions resulting from a disruption or disaster, to mitigate possible impacts and to recover itself largely independently from the negative effects of the disturbance".[13]

In other words, resilience "refers to 'before, during and after' the unwanted event or disruption of the CI, thus covering the whole crisis management cycle".[14] As pointed by the authors who, while acknowledging the definitional ambiguity and theoretical nature of the concept, proposed methods to apply resilience in practice, four characteristics are often used to describe the nature of resilience in CI (the system as well as its components): robustness (resistance to a loss of function in the event of shock), redundancy (the level of substitutability to maintain the functional service), resourcefulness (the ability to direct resources for the increase in robustness in the event of shock), and rapidity (the restoration of functionality in a timely manner).[15]

Another way of approaching the issue of CI resilience is to use the 'resilience triangle' which refers to societal, organisational and technological domains.[16] Thus, societal resilience focuses on the effects of CI disruption on vital societal functions of affected community, organisational resilience refers to the crisis management on organisational and inter-organisational levels, including, preparedness, response capacity, communication, etc., and technological resilience is about the robustness, adaptability, redundancy, restoration and recovery capacity of the facility.[17] Studies exploring the CI disruptions as a crisis leadership challenge provide additional insights into the debates on organisational resilience of CI.[18]

Focus on resilience, flexibility and agility of CI operators leads to calls for advancing collaborative processes and practical efforts to foster cooperation between citizens, private actors and all levels of governance institutions as well as between allies within NATO/EU which have been noticeable, for example, in cyber security policies of many OECD countries. It also points to the importance of advancing the processes best suited to a particular context rather than modelled projections. This puts additional weight on the importance of timely information sharing between infrastructure operators, state institutions and other

[12] Jon Coaffee: Future Proof. How to Build Resilience in an Uncertain World, 2019, p. 95-97.
[13] Jon Coaffee: Future Proof. How to Build Resilience in an Uncertain World, 2019, p. 110.
[14] Christer Pursiainen: The Crisis Management Cycle, Routledge, 2017, cited in 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. 87.
[15] Tim Prior: Measuring Critical Infrastructure Resilience: Possible Indicators, Risk and Resilience Report 9, Centre for Security Studies (CSS), ETH Zurich, 2014, p. 5.
[16] Michel Bruneua at el.: A Framework to quantitatively assess and enhance the seismic resilience of communities, 2003, cited in 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. 88.
[17] 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. 88.
[18] Eric Stern/Brian Nussbaum: Critical Infrastructure Disruption and Crisis Management, Oxford Research Encyclopedia of Politics, 2022.

actors, being flexible in changing established practices, even when doing so might lead to redundances, bigger costs or reduced productivity.

It should be noted, that on the EU level the focus was initially on protection of CI rather than enhancing its resilience. The emphasis on resilience first emerged in the scholarly research funded by EU Horizon 2020 and Horizon Europe research funding programs. Only in 2020 the European Commission proposed a directive on the resilience of critical entities, acknowledging that it is necessary to fundamentally switch the current approach from protecting specific assets towards reinforcing the resilience of the critical entities that operate them.[19]

Besides, in addition to the focus on resilience there was a shift from CI sectors to critical entities, i.e. operators of vital societal functions or economic activities in the EU single market. According to Pursiainen and Kytomaa, this narrowed down the level of analysis and action on operators and at the same time extended it to the EU Single market.[20]

A similar shift towards resilience has also been observed to take place in NATO around the same time.[21] On 11 January 2023, "in light of growing assertiveness of strategic competitors and the increasing complexity of security threats", the President of the European Commission and NATO Secretary General announced the establishment of a dedicated NATO-EU Task Force on the resilience of critical infrastructure.[22]

Cross-border threats to critical infrastructure and the role of the EU and international organisations

It is often repeated that global crises such as environmental disasters, extreme weather events and hostile activities cross national borders and affect more than one country. Economic, technological and societal interdependencies imply that there exists a functional need for the states to coordinate their policies in order to respond more effectively to cross-border threats, provide vital services and maintain resilience of critical infrastructure and its entities. In other words, "infrastructure often crosses borders or provides services that do so. Therefore, cooperation at regional and international level, including through international organisations, is indispensable".[23]

As it has been noted back in 2010, "[T]he increasing interdependence between infrastructures and between countries, as well as the inter-links between physical infrastructure and the information infrastructure create a compelling argument for the coordination of CIP [critical infrastructure protection] policy at international level".[24] This study was among those which, in addition to advocating increased policy and operational focus on resilience and preparedness, also called for coordination of CI protection policy at EU level, by

[19] Christer Pursiainen/Eero Kytomaa: From European critical infrastructure protection to the resilience of European critical entities: what does it mean? 2022, p. 88.
[20] Christer Pursiainen/Eero Kytomaa: From European critical infrastructure protection to the resilience of European critical entities: what does it mean? 2022, p. 89.
[21] Christer Pursiainen/Eero Kytomaa: From European critical infrastructure protection to the resilience of European critical entities: what does it mean? 2022, p. 88.
[22] NATO-EU Task Force on the Resilience of Critical Infrastructure: Final Assessment Report, June 2023.
[23] NATO-EU Task Force on the Resilience of Critical Infrastructure: Final Assessment Report, June 2023, p. 3.
[24] Bernhard Hammerli/Andrea Renda: Protecting Critical Infrastructure in the EU, CEPS Task Force Report, Centre for European Policy Studies, 2010, p. 1.

performing a subsidiarity test for each sector and adopting an all-hazards approach by empowering a single EU level agency to coordinate emergency management.

However, the more noticeable shift in the EU's approach to focus on European interdependences and extend the list of sectors, or rather vital societal functions provided by critical entities took place around early 2020s. Possibly based on the functional needs of interdependent societies and economies of EU Member States, the most recent initiatives of the EU extend the scope of policy areas and reflect the broadening of the risk landscape, treating physical and digital risks as more interconnected and including hybrid threats which intensified in recent years, especially after Russia's full-scale war against Ukraine.[25]

The OECD has also been recently working in the field of CI resilience by assessing practices of its members and providing policy recommendations. Noting that the "interconnectedness of supply chains and technological and financial systems in the global economy increase the exposure and vulnerability of critical infrastructure" and that the "negative impacts of shocks and disruptions can cut cross sectors and borders", it proposed a Policy Toolkit for Governance of Critical Infrastructure Resilience. [26] It argued that instead of focusing on asset protection alone, a systems resilience approach allows governments and infrastructure operators to address asset interdependencies and prioritise resilience measures for critical hubs and nodes whose failure would cause the most damage.

Similarly to the scholarly studies examining concrete cases of CI resilience and building on the experience and good practices of OECD countries such as Finland, the OECD study discusses the proper role of governments in strengthening CI resilience, including by engaging CI operators, the most appropriate mechanisms of sharing sensitive information about risks, vulnerabilities and resilience measures between governments and operators and the sharing of costs and benefits of investing in resilience between governments, operators and end-users.[27]

This condensed review of the debates on protection and resilience of CI shows that it has become increasingly important and merits more in depth analysis in the context of EU enlargement. The cross-border nature of the threats to CI in the EU and candidate countries points to the need for a coordinated and coherent system-based approach both nationally, involving multiple stakeholders, and on a regional or international level (EU/NATO).

At the same time, the consistent coordination in the field of protection and resilience of CI and its entities is challenging due to the policy area being considered both a matter of national security and performing important economic and societal functions. Moreover, as studies of the evolution of CI policies in selected EU member states illustrate, even such countries like Estonia, Latvia and Lithuania which are EU and NATO member states, have very similar threat perceptions and recent history of economic and social development, still differ in their practical approaches to protection and resilience of CI.[28] It is even more

[25] On critical assessment of EU's Hybrid Toolbox see Kenneth Lasoen: Realising the EU Hybrid Toolbox: opportunities and pitfalls, Clingendael Policy Brief, December 2022.
[26] OECD: Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies, OECD Publishing, 2019, p. 3.
[27] OECD: Good Governance for Critical Infrastructure Resilience. 2019, p. 101-114.
[28] See Māris 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.

likely that those CI-related policies will differ in candidate countries, taking into account their patterns of interdependencies and divergence of challenges faced by them ranging from kinetic attacks by Russia against CI entities in Ukraine to cyber-attacks and domestic cleavages regarding threat perceptions in other candidate countries.

The analysis provided below aims to assess the debates on CI-related issues and policy trends in both EU member states, in particular, related to cyber-attacks in the Baltic States, recent incidents in the Baltic Sea, and developments in three candidate countries of Ukraine, Montenegro and Georgia. The focus of those cases studies is on the current threats to their CI and how they respond to them by protecting their CI and strengthening its resilience in the context of their connectedness and having in mind the need for public and private partnerships as well as functional needs of cross-border cooperation to adapt, learn by doing and rebound from the shocks. In depth analysis of differences should allow to later investigate the potential for more aligned CI-related policies between the EU and candidate countries, having in mind similar external threats which will be an object of the next policy report D.7.2.

3 Analysis of recent incidents and attacks on critical infrastructure

Cyber-attacks on critical infrastructure in the Baltic States

Objects and targets of cyber-attacks

Cyber groups operated by foreign intelligence services pursue different objectives. Most often they compromise computer systems, i.e., they unauthorizedly penetrate them to instantly obtain classified intelligence information, sabotage the operation of computer systems, or destroy the data they contain. Very often, however, groups controlled by hostile states hack into computer systems to gain and establish a prolonged covert presence on those systems.

These are complex attacks that are carried out to penetrate and carry out malicious actions either on a large number of computer systems simultaneously or on individual well-protected systems. In such cases, cybercriminals attack a potential target through one member of its supply chain. For example, computer systems, software, or updates may be infected with malware before being delivered to a potential target. According to the Latvian State Security Service, a significant portion of cyber-attacks still succeed because of mistakes made by information technology managers and users. Cyber attackers take advantage of poorly configured computer networks and low levels of cyber hygiene. [29]

Ideologically or politically motivated cyberattacks mainly target government authorities, critical infrastructure, including financial, transportation and communications institutions, the media, and various businesses. So called Distributed Denial of Service (DDoS) attacks do not compromise information security, but they do impede or halt the operation of online services. DDoS campaigns by Russian hacktivists are aimed at intimidation, demonstration of power, and publicity. For this reason, they are accompanied by informational activity, often exaggerating the success of the attacks, and are aimed primarily at the internal

[29] Latvijas Republikas Valsts Drošības Dienests: VDD Publiskais Pārskats 2023, January 2024, available at: https://vdd.gov.lv/uploads/materials/34/lv/vdd-publiskaisparskats-2023-web.pdf (last accessed 10.02.2025)

Russian audience, emphasizing Russia's strength and capabilities and the weakness of the West.

Another type of cyber-attack is vulnerability hunting and digital penetration, which aims to obtain military, political, or economic information, as well as to gather information and prepare for future cyber operations. Targeted email attacks also remain a widespread form of cyber-attack. Phishing attacks are also frequently used by cyber units of Russian intelligence agencies to gain access to government email and computer networks.

Recently, cyber-attacks using so-called "supply chains" have become more frequent. In this case, to gain access to the target's information systems, attackers first try to gain access to computer networks that have access to the target's computer network The covert, persistent presence in infected networks can be used by foreign intelligence services through cyber groups under their control both to obtain information and to carry out malicious actions, if necessary, on the victim's computer system. Similarly, cyber groups controlled by Russian intelligence agencies attempted to carry out so-called supply chain attacks, which are now considered one of the most dangerous and difficult-to-identify cybersecurity threats.

There have also been cases of fraudsters approaching Latvian media and state institutions, posing, for example, as politicians or popular civil society figures, offering phone calls and interviews that could later be used to discredit them.[50] Attackers have tried to contact high-ranking government officials; in 2023, such a scheme was realized to the Latvian Prime Minister.[51] Such manipulations occur regularly and are not directed against any particular country, but against European countries in general. In this way Russia expands its foreign policy activities, discrediting representatives of other countries aiming to reduce public trust in authorities. Manipulative measures are most often of high quality and targeted, and for this reason, the fraudsters succeed.

Cyber-attacks are transnational in nature, with simultaneous attacks targeting the digital resources of several Baltic States, utilizing digital resources from other EU countries as well. Data exchange and cooperation between EU member states are therefore crucial for effective counteraction. Similarly, in the realm of information warfare, waves of disinformation and information campaigns are not directed at a single country, but at the entire region, the EU and NATO. They can aim at disrupting the processes of integration of energy and transport infrastructure of the Baltic states, which aims to reduce dependencies on Russia and diversify through connectivity to other EU members. An example of a disinformation campaign was the disconnection of the Baltic States from the Russian power supply network, BRELL. In the days leading up to the disconnection from the BRELL network on 9 February, 2025, attempts to sow panic were observed, spreading images and messages in messengers and social media groups about the need to turn off various electrical appliances on weekends, although there was no rational basis for such actions.[52]

---

[50] Latvijas Republikas Satversmes Aizsardzības Birojs: SAB 2022 Pārskats, January 2023, available at: https://www.sab.gov.lv/files/uploads/2023/07/2022_parskats.pdf (last accessed 10.02.2025)
[51] LSM: Krisjanis Kariņš fell for a ruse of Russian pranksters, 14 November 2023, available at: https://rus.lsm.lv/statja/novosti/politika/14.11.2023-krisyanis-karins-popalsya-na-ulovku-prankerov-iz-rf.a531622/ (last accessed 10.02.2025)
[52] Latvija Avīze: Dezinformatori Igaunijā rada paniku par atslēgšanos no Krievijas energotīkla; kritiskā infrastruktūra tiek apsargāta, 06 February 2025, available at: https://www.la.lv/dezinformatori-igaunija-

Additional example of the transnational nature of cyberattacks on digital infrastructure can be seen in the disruption of GPS systems, which the Baltic and European countries are increasingly facing. According to the Latvian Air Navigation Agency, GPS interference still occurs in the region. By the end of 2024, these disturbances had become more frequent and intense, reaching record highs in December 2024, with 179 instances of interference recorded by December 18. In total, there were 830 disruptions to the Global Navigation Satellite System (GNSS) in 2024, compared to 342 in 2023.[33]

At the individual level, the most common are various financial schemes, attacks on users' social media accounts to gain control over them, and fraud attempts by sending emails or SMS inviting them to open links or attachments to obtain users' private information or access their accounts. [34] Malware, threats to command and control (C&C) centres, and phishing continue to be among the most common cyberattacks that can cause major damage to both computers and cell phones and tablets. The goal of scammers is to enable further use of devices for other criminal purposes, including generating cryptocurrencies and extracting sensitive information from users.[35]

The recent trends of cyber-attacks against CI in the Baltic States

Cyber-attacks, often linked to geopolitical tensions and state-sponsored actors, have targeted CI, government agencies, and private organizations in Estonia, Latvia and Lithuania. Existing data based on reports from national Computer Emergency Response Teams (CERTs), national telecommunications carriers, government security agencies, and the media demonstrate the changing nature of cyber threats, which are increasing in number and intensity.[36] They underscore the importance of robust cybersecurity systems and effective, continuously updated policies of protecting CI and strengthening its resilience.

One of the earliest and most notable examples of cyber-attacks was the massive attack on Estonia in April and May, 2007. Over three weeks, government and parliamentary portals, ministries, news outlets, internet service providers, major banks, and small businesses were all targeted, predominantly by DDoS. The cyber-attack coincided with the Estonian government's decision to relocate the 'Bronze Soldier Memorial' in Tallinn, which led to significant civil disturbance in both Estonia and Russia. Most of the malicious network traffic was Russian-language and showed signs of political motivation. The Russian government has denied involvement, but the cyber-attacks were accompanied by hostile political

radijusi-tik-lielu-paniku-par-atslegsanos-no-krievijas-energotikla-ka-cilveki-izperk-generatorus (last accessed 10.02.2025)

[33] DELFI.LV: Количество помех в работе спутниковой системы навигации в воздушном пространстве Латвии увеличилось в пять раз, 06 February 2025, available at: https://rus.delfi.lv/57860/latvia/120060243/kolichestvo-pomeh-v-rabote-sputnikovoy-sistemy-navigacii-v-vozdushnom-prostranstve-latvii-uvelichilos-v-pyat-raz (last accessed 10.02.2025)

[34] Latvijas Republikas Valsts Drošības Dienests: VDD Publiskais Pārskats 2023, January 2024, available at: https://vdd.gov.lv/uploads/materials/34/lv/vdd-publiskaisparskats-2023-web.pdf (last accessed 10.02.2025)

[35] LMT: Kiberapdraudējumu līmenis pieaug - uzbrukts vairāk nekā pusei LMT tīklā esošo ierīču, 21 October 2024, available at: https://lmt.lmt.lv/jaunumi/kiberapdraudejumu-limenis-pieaug (last accessed 10.02.2025)

[36] CBAP: The Changing Face of Cybersecurity in the Baltics and Finland, 03 May 2023, available at https://cbap.cz/archiv/5299 (last accessed 09.02.2025)

rhetoric by Russian officials, economic measures, and a refusal to cooperate with investigations in Estonia.[57]

After these attacks, the Estonian government began purposefully formulating cybersecurity policy, and in May 2008, the NATO Cyber Defence Centre of Excellence was established in Tallinn. The centre has become an important source of knowledge in the field of cyber defence, both for NATO and member states. The centre brings together experts from 29 countries.[58]

This incident demonstrated the threat potential of cyber-attacks and became a global benchmark for cyberspace warfare, serving, among other things, to intensify efforts by the Baltic States, the European Union, and NATO to develop legislation, strategies, and institutional mechanisms to counter cyber threats and increase resilience of CI.

Subsequently, cyber-attacks on the Baltic States have often been linked to political events and deteriorating relations between, on the one hand, Latvia, Lithuania, Estonia, and, on the other hand, Russia. Thus, at the end of June 2008, when the websites of different state institutions, organizations, and companies in Lithuania were attacked, it attracted more public attention. During these cyberattacks, more than 300 web pages were marked with symbols of the Soviet Union. Before that, information about possible cyber-attacks on the Baltic States and Ukraine appeared on Russian Internet forums. The Lithuanian minister of national defence did not exclude the possibility that the attacks were retaliation for amendments to the law recently adopted by the Seimas, which equated the symbols of the former USSR with Nazi symbols and prohibited their use in public gatherings. In the media, this was described as "one of the biggest incidents in the Lithuanian internet space", while recalling the cyberattacks in Estonia a year ago.[59]

Later cyber-attacks have been reported in growing numbers and eventually led to significant policy and institutional reforms aimed at improving cyber security in Lithuania and coordination of efforts aimed at increasing resilience of CI domestically between public and private actors as well as with NATO and EU partners.[60] Russia's hybrid war against Ukraine in 2014, which included the use of cyber-attacks against CI in Ukraine acted as another important trigger leading to more attention being devoted to cyber security in the Baltic States.

Latvia was no exception, and against the backdrop of strained relations with Russia, was also regularly subjected to cyber-attacks. During Latvia's presidency of the EU Council in the second half of 2015, a large number of state institutions fell victim to targeted cyber-attacks. DDoS attacks, vulnerability scans, and malware campaigns were widespread. The technical information obtained during the investigation was passed to law enforcement

[57] NATO Strategic Communications Centre of Excellence: 2007 cyber-attacks on Estonia, May 2007, available at https://stratcomcoe.org/publications/download/cyber_attacks_estonia.pdf (last access 09.02.2025)
[58] Ministry of Foreign Affairs of the Republic of Estonia: Regional activities, Last updated: 13.01.2022, available at: https://www.vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/regional-activities (last accessed 10.02.2025)
[59] BNS 2008. "Internet Invaders Paralyzed more than 300 Lithuanian Websites," June 30.
[60] 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.

authorities.[41] CERT.LV also investigated the activities of Russian Internet trolls in the comment sections of Latvian news portals, where they used provocative comments to spread links that were used to infect users' computers.[42]

Shortly after the start of Russia's full-scale war in February, 2022, several groups of pro-Kremlin hacktivists became active. Their target was not only Ukraine but also many countries supporting Ukraine, including Estonia, Finland, Latvia, Czech Republic, Romania, Poland, and others. The range of targets of DDoS attacks in different countries has been generally the same: ministries, government agencies, critical electronic services, the transportation sector, banks, and the media. Often waves of DDoS attacks were caused by a country making a political decision in support of Ukraine, for example, declaring Russia a state sponsor of terrorism.[43]

After Russia attacked Ukraine, the number and intensity of cyberattacks in the Baltics increased significantly. In its public report for 2022, the Latvian Constitution Protection Bureau (SAB) indicated that 2022 saw the most intense cyber-attacks in Latvian cyberspace. The number of cyber-attacks tended to increase and had a wave-like character. In the public administration sector, the search for vulnerabilities in IT systems increased 7 times, and the total volume of attacks increased 4 times. According to SAB, Russia was the source of most cyber threats. According to data collected by CERT.LV, increased cyberattack activity was observed even before Russia invaded Ukraine in February. The number of attempts to invade Latvian infrastructure has increased significantly since February. The cyberattacks came in waves, peaking in May and August, which was associated with Latvia's political decisions to support Ukraine in various ways.[44]

In response to public and political calls to dismantle the Soviet monument in Victory Park, hacktivist groups such as "Killnet", which support the aggressive Russian regime, conducted intensive DDoS attacks on Latvian infrastructure. Although these attacks were large-scale, they were characterized as hooliganism and mostly had no tangible consequences. The exception was organizations that are not usually the target of DDoS attacks and have low levels of preparedness and protection, such as the charity organization Ziedot.lv, which helped raise funds for the demolition of a monument in Victory Park and support of Ukraine.[45]

Similar trends have been observed in Estonia. In its 2022 report, CERT Estonia stated: "The volumes of the attacks were sometimes more than a hundred times higher than in 2007, when, after the removal of the Bronze Soldier monument, our eastern neighbour disrupted

[41] CERT.LV: Publiskais pārskats par CERT.LV uzdevumu izpildi, January 2016, p.11,available at: https://www.cert.lv/uploads/parskati/CERT.LV_gada_parskats_2015.publ.pdf (last accessed 10.05.2025)
[42] CERT.LV: Publiskais pārskats par CERT.LV uzdevumu izpildi, p.13, January 2016, available at: https://www.cert.lv/uploads/parskati/CERT.LV_gada_parskats_2015.publ.pdf (last accessed 10.02.2025)
[43] RAI EE: Cyber Security in Estonia 2023, January 2024, available at https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf (last accessed 10.02.2025)
[44] Latvijas Republikas Satversmes Aizsardzības Birojs: SAB 2022.GADA DARBĪBAS PĀRSKATS, p.32, 2023, available at: https://www.sab.gov.lv/files/uploads/2023/07/2022_parskats.pdf (last accessed 10.02.2025)
[45] CERT.LV: 2022. gads Latvijas kibertelpā, January 2023, available at: https://www.cert.lv/lv/2023/01/2022-gads-latvijas-kibertelpa (last accessed 09.02.2025)

the work of our e-services and thereby our daily life with mass requests."[46] One of the largest and most noticeable side effects of the full-scale invasion of Ukraine was a fourfold increase in DDoS attacks. Back in 2022, activity on this front seemed frequent and rapid, but in 2023 broke the previous record. 484 DDoS attacks were recorded, which was 60% more than in 2022. More DDoS attacks were reported in just one month than in the entire year before Russia launched its offensive on Ukraine. Only 139 attacks – less than a third – had consequences. Typically, the damage was limited to a short period of downtime or a slow response time of a website or service, but in some cases were more serious. The most notable was an attack that interrupted online sales of train tickets and the operation of payment terminals on trains for a day.[47]

In November 2022, the electronic channels of Eesti Energia, including the Elektrilevi network company, were attacked. The website and mobile application of Eesti Energia and the website and mobile application of Elektrilevi MARU were affected. According to the State Infosystems Department, attacks by pro-Kremlin criminals targeted also companies and agencies in Latvia, Poland and Ukraine. The Ministry of Economy, the Bank of Estonia and EAS were also attacked.[48]

In 2022, the Lithuanian NCSC's Incident Response Team (CERT-LT) registered a total of 4,080 cyber incidents, which was similar to the 2021 figure. However, the NCSC noted an increase in the number of DDoS attacks. At the end of June 2022, the NCSC recorded a massive wave of DDoS attacks targeting the public and private sectors. According to publicly available information, the attacks were directed at 130 publicly accessible websites. A pro-Russian hacker group claimed responsibility for the attacks.[49]

Overall, the intensity of cyber-attacks continued to increase in 2023 and 2024, with new trends emerging: private devices such as WiFi access points and Internet of Things (IoT) devices are increasingly being used to carry out cyber-attacks. There has also been a trend of cyber-attacks on software companies. After gaining access to the computer networks of these companies, attackers then attempt to gain access to the computer networks of their customers, who are often government agencies.[50] As in the past, the greatest threat to Latvia in 2024 was posed by Russian intelligence hacker groups. At the same time, Latvian State Security Service recorded significantly less interest in Latvia from Chinese intelligence hacker groups.

---

[46] RIA.EE: Cyber Security in Estonia 2023, p.10, January 2024, available at: https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf (last accessed 10.02.2025)
[47] RIA.EE, Cyber security in Estonia 2024, p.10, January 2025, available at: https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf (last accessed 10.02.2025)
[48] ERR.EE: Pro-Kremlin cybercriminals attack Eesti Energia, 19 Nov. 2022, available at: https://rus.err.ee/1608794218/prokremlevskie-kiberprestupniki-atakovali-eesti-energia (last accessed 10.02.2025)
[49] e Ministry of National Defence of the Republic of Lithuania: Key Trends And Statistics Of The National Cyber Security Status Of Lithuania 2022, 01 June 2023, available at: https://www.nksc.lt/doc/en/2022_key-trends-and-statistics-of-cyber-security.pdf (last accessed 10.02.2025)
[50] Latvijas Republikas Satversmes Aizsardzības Birojs: SAB 2023 Gada pārskats, January 2024, available at: https://www.sab.gov.lv/files/uploads/2024/02/SAB-2023.gada-parskats_LV.pdf (last accessed 10.02.2025)

The year 2024 brought other cybersecurity challenges: during the November cold snap, the conflict between Israel and HAMAS affected Estonia - a cyberattack on Israeli-made programmable logic controllers disrupted local Estonian heating and pumping stations. [51]

Actions to Strengthen Cyber security and Resilience of CI

To mitigate digital security risks and to build resilience to cyber-attacks, it is necessary to strengthen the ability to use technology solutions prudently and acquire IT literacy, or self-defence skills in the face of cyber security challenges.

Established in 2018, EU Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRTs), coordinated by Lithuania, is considered among the most successfully developing and advanced PESCO projects. One of the key activities of a EU CRRT is its constant development through refinement of the procedures and practices applied in the capability. Currently a CRRT comprises 8-12 cybersecurity experts delegated at national level by eight EU member states - Belgium, Croatia, Estonia, Lithuania, Netherlands, Poland, Romania, Slovenia. The team is capable of offering assistance in managing a cyber-incident or carrying out prevention (vulnerability assessments, elections observation, etc.).[52]

In 2022, the security of the supply chain of Lithuanian contractors continued to be strengthened, Lithuania started preparing the National Cyber Security Development Program and adopted a description of procedures governing the availability and recovery of state information resources. In 2022, Lithuania adopted legislation to ensure that CI entities, including 5G infrastructure, use equipment only from trusted manufacturers. Amendments were adopted to the Law on Public Procurement, the Law on Procurement of Customers Operating in the Sectors of Water Supply, Energy, Transport and Postal Services, and the Law on Procurement in the Defence and Security of the Republic of Lithuania.[53]

In March 2023, the Latvian Cabinet of Ministers approved the draft strategy "Latvian Cyber Security Strategy 2023-2026" developed by the Ministry of Defence. On September 1, 2024, the National Cyber Security Law came into effect, which imposes stricter requirements on companies, including the preparation of an organizational security self-assessment and the appointment of a cybersecurity executive. The Act transposed the requirements of Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022, establishing measures to achieve a single high level of cybersecurity throughout the Union. In addition to the requirements of Directive, the National Cyber Security Law will also apply to critical information and communication infrastructure supervised by the SAB.[54]

---

[51] RIA.EE, Cyber Security in Estonia 2024, January 2025, available at: https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf (last accessed 10.02.2025)

[52] Ministry of National Defence of the Republic of Lithuania: Lithuanian-coordinated EU Cyber Rapid Response Teams - incident response with the EU and in support of EU partners and military missions, 30 March 2023, available at: https://kam.lt/en/lithuanian-coordinated-eu-cyber-rapid-response-teams-incident-response-with-the-eu-and-in-support-of-eu-partners-and-military-missions/ (last accessed 10.02.2025)

[53] Ministry of National Defence of the Republic of Lithuania: Key Trends and Statistics of The National Cyber Security Status of Lithuania 2022, 1 June 2023, available at: https://www.nksc.lt/doc/en/2022_key-trends-and-statistics-of-cyber-security.pdf (last accessed 10.02.2025)

[54] Latvijas Republikas Satversmes Aizsardzības Birojs: SAB 2023 Gada pārskats, January 2024, available at: https://www.sab.gov.lv/files/uploads/2024/02/SAB-2023.gada-parskats_LV.pdf (last accessed 10.02.2025)

Latvia's cooperation with NATO allies in joint cyber threat hunts to detect the presence of adversaries in Latvia's CI systems can also be considered a success story. Such joint operations have been conducted since 2022. In 2023, a joint Latvian–Luxembourg team placed 4th out of 24 teams in Locked Shields 2023, the world's largest and most complex cyber defence exercise.
2023 also saw the launch of a coordinated vulnerability disclosure process in public administration, allowing agencies to voluntarily register their resources on the vulnerability reporting platform CERT.LV.[55]

According to CERT.LV, "Latvia is a leader in organizing and conducting threat search operations in the EU. Other European and NATO partner countries are also learning and gaining new experience from Latvian experts. Effective cooperation with representatives of the public administration infrastructure, as well as with security institutions in Latvia, is a major factor in successful results. By the end of 2023, threat hunting operations have analysed more than 100,000 endpoint devices in 25 organizations".[56]

The *DiBaX* digital *backbone* experiment has begun at Adazi Military Base, Latvia, in 2024. This experiment, which NATO conducted together with the Ministry of Defence, the National Armed Forces and mobile operator LMT, demonstrates the importance of industry and high technology in strengthening NATO and Baltic defence capabilities. The 5G Military Test Environment was established by the National Armed Forces at Adazi Military Base in 2022 in cooperation with LMT and provides the opportunity to develop and test various sensors, defence systems and platforms, including unmanned solutions, making a significant contribution to the technological development of the Latvian and Allied armed forces.[57]

The importance of public-private partnership and the understanding of business responsibility should also be stressed. A positive example is the close cooperation of national telecommunications operators of the Baltic countries with national CERTs, as well as responsible intelligence services and ministries. For example, in September 2024, Latvian mobile operator LMT blocked more than 167 million threats from 6.3 million malicious domains. Compared to the same period last year, the number of attacks increased more than 36 times.[58]

Collectively, the three Baltic States are assessed very well in terms of cyber-preparedness. All three are ranked by the Global Cybersecurity Index in the top 20 out of 193 countries. Estonia places third, after only the United States and the United Kingdom. Lithuania is ranked 6th, whereas Latvia is further down, ranking fifteenth. Lithuania and Estonia rank very high in the National Cyber Security Index, among the top ten, whereas Latvia is slightly behind, placing 25th.[59]

---

[55] CERT.LV: 2023. gads Latvijas kibertelpā, January 2024, available at: https://cert.lv/lv/2024/03/2023-gads-latvijas-kibertelpa (last accessed 10.02.2025)
[56] CERT.LV: 2023. gads Latvijas kibertelpā, January 2024, available at: https://cert.lv/lv/2024/03/2023-gads-latvijas-kibertelpa (last accessed 10.02.2025)
[57] SARGS.LV: Aizsardzības ministrija, NBS un LMT kopā ar NATO plāno unikālu digitālās savienojamības eksperimentu, 05 September 2024, available at: https://www.sargs.lv/lv/nozares-politika/2024-09-05/aizsardzibas-ministrija-nbs-un-lmt-kopa-ar-nato-plano-unikalu-digitalas (last accessed 10.02.2025)
[58] LMT: Kiberapdraudējumu līmenis pieaug - uzbrukts vairāk nekā pusei LMT tīklā esošo ierīču, 21 October 2024, available at: https://lmt.lmt.lv/jaunumi/kiberapdraudejumu-limenis-pieaug (last accessed 10.02.2025)
[59] Latvian Institute of International Affairs : Commonalities, Risks and Lessons for Small Democracies: Hybrid Threats in Baltics and Taiwan, 2022, p. 59, available online: https://www.liia.lv/en/publications/hybrid-

In general, despite the significant increase in cyber-attacks, public ICT resources and CI operators in the Baltic States proved to be very resilient to DDoS attacks thanks to the cooperation of local CERTs, ISPs, and state intelligence agencies. To more effectively counter cyber threats, both private and public sector resources and expertise should be combined. The structure and procedures of cyber defence units should combine best practices from the public, private, and military sectors, decision-making should be results-oriented and procedures automated.

In addition to Baltic cooperation and bilateral partnerships with national CERTs, cyber security issues have been raised at the EU and NATO levels. On October 4, 2024, European Union and NATO officials held their first structured dialogue on cyber issues. Building on previous talks by senior EU and NATO officials on cyber security and cyber defence, the dialogue aimed to strengthen EU-NATO cooperation on cyber security and cyber defence and to create new opportunities for improved cooperation in the future. The dialogue explored ways to further improve the harmonization of relevant cyber defence systems and tools to respond to malicious cyber activities. This is the seventh structured dialogue established between the EU and NATO as part of the implementation of the three EU-NATO Joint Declarations of Cooperation of 2016, 2018 and 2021. The EU and NATO have other structured dialogues on military mobility, resilience, new and disruptive technologies, climate and defence, space and defence industry.[60]

Attacks on critical infrastructure in Ukraine

Analysis of Kinetic Attacks on Energy Infrastructure

For a decade CI in Ukraine has been under cyber and military (kinetic) attacks from Russia aimed at inflicting direct physical damage. In particular, Russia's full-scale war since 2022 against Ukraine has caused economic disruption, affecting the provisions of vital services and inflicting significant damage to its CI. Ukraine's experience in resisting aggression and protecting its CI as well as efforts to restore provision of services and reduce its vulnerabilities can provide valuable lessons.

Therefore, this section aims to discuss the disruptions caused by Russia's attacks – both kinetic and cyber – and the methods used by Ukrainian authorities to protect and restore the functioning of CI. The focus is on energy infrastructure due to its importance for the society and functioning of state as well as regular targeting by Russia of its objects.

The kinetic attacks on the energy critical infrastructure in Ukraine have started in 2022 and continued through 2023 and 2024 affecting the energy and water supply and sometimes resulting in power outages across the country. The scale of the destruction is enormous, especially in the eastern and southern regions. According to the Energy Ministry, the total loss of Ukraine's power capacities due to these attacks exceeds 9 GW. As a result of the extensive damages to business consumers, decrease in number of households, and

threats-in-baltics-and-taiwan-commonalities-risks-and-lessons-for-small-democracies-954?get_file=1 (last access 10.02.2025)

[60] European Comission: Eiropas Savienība un NATO rīko pirmo strukturēto dialogu par kiberjautājumiem, 04 October 2024, available at: https://digital-strategy.ec.europa.eu/lv/news/european-union-and-nato-hold-first-structured-dialogue-cyber (last accessed 10.02.2025)

disruptions due to ongoing attacks, electricity demand in Ukraine declined by 30-35% compared to 2021.[61]

Additionally, Ukraine's power generation capacity, including hydroelectric, thermal, and the Zaporizhzhya Nuclear Power Plant (NPP – the largest in Europe), has been impacted by occupation and attacks. Ukraine now has only three operational nuclear power plants: Khmelnytskyi, Rivne, and South Ukraine NPPs. Notably, despite the ongoing war, Ukraine has begun transitioning to Westinghouse fuel. For the first time, it was utilized at the nuclear power plant in Rivne NPP. The prospect of producing this fuel in Ukraine would help reduce dependence on Russia.[62]

The current nuclear production capacity stands at 7.8 GW, nearly half of the prewar capacity of 13.5 GW. The thermal power stations have also suffered extensive damage, with attacks resulting in the loss of 80% of thermal generation capacity. All Ukrainian hydropower facilities have been damaged or attacked, and the Kakhovka Hydroelectric Power Plant was completely destroyed by Russian forces on June 6, 2023. Two hydropower plants, including the largest, the Dnipro HPP (DniproGes), have suspended operations.

In addition to the power system, Russia started attacking Ukraine's underground gas storage facilities. Those with the highest capacities were attacked multiple times.

According to KSS assessments 13% of Ukrainian Solar Power Plants (SPP) capacities are under occupation, with 8% of the total installed solar capacity destroyed or impaired. [63] As to Wind Power Plants (WPP), the 2023 installed capacity totalled 1.8 GW, with roughly 80% situated in occupied territories, with 1% of the total installed wind capacity (at least 10 wind turbines) is damaged or destroyed. Adding 1,3% of biogas stations, 4% of hydroelectric small power plants, totally 20% of the overall installed RES capacity being affected.

According to World Bank estimates (Recovery and Reconstruction Needs Assessment) released on 15 February 2024 and covering nearly two-year period from Russia's invasion of Ukraine on February 24, 2022, to December 31, 2023, has estimated the direct damage in Ukraine to almost $152 billion (including housing, transport, commerce and industry, energy, and agriculture). [64]

---

[61] It is important to note that the access to the energy data is significantly constrained due to limited access to information in accordance with the martial law currently in force in Ukraine. According to the resolution of the National Energy and Utilities Regulatory Commission (NEURC) No. 349 dated March 26, 2022, concerning information protection, it is stated that, under the conditions of a state of war, certain information included that related to critical infrastructure objects may be classified as restricted access information. This limitation leads to incomplete operational data, posing challenges in obtaining comprehensive information about system performance and generating accurate statistics.

[62] Westinghouse VVER-440 fuel loaded into reactor, 11 September 2023, World Nuclear News, available at: https://world-nuclear-news.org/Articles/Westinghouse-VVER-440-fuel-loaded-into-reactor (last accessed 13.02.25)

[63] Igor Piddubnyi, Dmytro Goriunov, Assessment of damages and losses to Ukraine's energy sector due to Russia's full scale invasion, May 2024, p16, available at: https://kse.ua/about-the-school/news/damages-and-losses-to-ukraine-s-energy-sector-due-to-russia-s-full-scale-invasion-exceeded-56-billion-kse-institute-estimate-as-of-may-2024/

[64] Updated Ukraine Recovery and Reconstruction Needs Assessment Released, Press release, February 15, 2024, World bank Group, available at: https://www.worldbank.org/en/news/press-release/2024/02/15/updated-ukraine-recovery-and-reconstruction-needs-assessment-released (last accessed 11.11.24)

The winter 2024-2025 turned out be challenging for Ukraine, as electricity supply was risking rolling blackouts (outages) and the unscheduled interruptions, heat supply system damages following extensive Russian attacks. The anticipated deficit in the energy system during the cold months could reach 6 GW, according to a report from the International Energy Agency (IEA) dated 19 September 2024.[65]

On November 28, 2024, a series of 11 coordinated attacks on the Ukrainian energy system targeted primarily the power delivery infrastructure of nuclear power plants, resulting in a 10-40% reduction in the capacity of eight power units.

The temporary loss of up to 3 GW of power necessitated the reintroduction of hourly outage schedules, initially affecting three to four consumer lines, and later impacting one or two lines. Additionally, long-term emergency repairs to damaged facilities were required, particularly in the Odessa and Kherson regions.

In December 2024, two coordinated attacks on Ukraine's energy system took place, with 93 missiles and 200 UAVs. On December 13, air- and sea-launched cruise missiles primarily targeted high-voltage substations essential for the operation of interstate intersections. Then, on December 25, the Russian forces once again struck power units and engine rooms of thermal and hydroelectric power plants, focusing mainly on Ukraine West of the Dnipro river. The number of weapons used reaching 1,300 missiles and nearly 1,000 attack UAVs since the beginning of war.

The damage from the Russian strikes could have been far worse had it not been for protective measures[66] implemented at fuel and energy facilities, along with the presence of second-level protection systems for electricity transmission and distribution.[67]

Over the course of the war, the tactics of kinetic attacks have evolved. Since 2022 until now, the Russian Federation has been destroying numerous power generation, transmission, and distribution facilities. At the beginning of the invasion, it started targeting distribution lines and transformator substations.

In April 2024 it launched precision missiles at power plants in areas less defended than Kyiv. Some of them were not fully restored by winter. The consequences of the recent attacks are much stronger than in the winter of 2022-2023, as they are aimed at cutting off power to large cities and industrial areas.

Another significant difference from the winter of 2022-2023 is the increased use of costly ballistic missiles. For example, in a recent attack, Russia targeted a power plant with several missiles valued at $100 million. Ukraine has only a limited number of Patriot systems capable of intercepting them.

---

[65] Ukraine's Energy Security and Coming Winter, An energy action plan for Ukraine and its partners, EAI, September 2024, available at: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter (last accessed 11.11.24)

[66] Situation in the Energy Sector and Preparations for the Heating season: President Held a Meeting of the Staff, available at https://www.president.gov.ua/en/news/situaciya-v-energetici-ta-pidgotovka-do-opalyuvalnogo-sezonu-91681 (last accessed 07.02.25)

[67] These measures are being implemented under Cabinet of Minister's Resolution No 1482 dated 27 December 2022, available at: https://zakon.rada.gov.ua/laws/show/1482-2022-п#Text (last accessed 07.02.25)

In the winter of 2024-25, Russia used missiles with cluster warheads in attacks on the energy sector, causing significantly greater damage and prolonging recovery efforts due to the need for demining. As the scale and complexity of attacks increased, more advanced weaponry was deployed against Ukraine's energy infrastructure.

Ukraine entered the winter of 2023-2024 with a just-sufficient capacity to meet energy demand. However, the situation has deteriorated due to new waves of large-scale Russian strikes, which have further weakened Ukraine's energy infrastructure. The delayed delivery of military aid in late 2023 and early 2024, resulting in a shortfall in Ukraine's air defence capabilities, has significantly increased the vulnerability of its energy infrastructure to air strikes.

Cyber security as a critical element of CI Protection in Ukraine

Cyber security is a crucial component in countering Russia's aggression. Investments are essential to enhance Ukraine's capacity to respond to and recover from Russian cyber-attacks, particularly those targeting the CI operators. Cyber-attacks have tripled since the beginning of the invasion (for instance, the major cyber-attacks on energy facilities by Russian Sandworm group[68] or outage of Kyivstar network[69]). This highlights the need for robust cyber protection for all facilities connected to the internet.

On December 19, 2024, Ukraine experienced its largest cyber-attack on state registries in recent history. The attack, carried out by the Russian actors, temporarily disrupted the operation of unified and state registries under the jurisdiction of the Ministry of Justice of Ukraine.

Overall, the number of cyber-attacks on Ukraine increased by 69.8% in 2024, reaching 4,315 incidents, compared to 2,541 cyber incidents recorded in 2023.[70] This information was reported by the State Service for Special Communications and Information Protection.

Attackers frequently target local authorities, government and government agencies, the security and defence sector, the energy sector, commercial organizations, and telecommunications providers. The most common types of incidents involve malware distribution, phishing, malicious connections, and account or system compromises. The hackers' goals include stealing sensitive information and destroying data and information systems. Currently, there is a steady trend towards an increase in cyber-attacks, primarily against Ukraine's CI. A significant step in addressing these threats was the adoption of the Action plan[71] for implementing Ukraine's Cybersecurity Strategy[72].

---

[68] Daryna Antoniuk, Russian hackers target 20 energy facilities in Ukraine amid missile strikes, The Record, available at: https://therecord.media/russian-hackers-target-energy-facilities-ukraine (last accessed 05.02.25)

[69] Cyber-attack', BBC, available at: https://www.bbc.com/news/world-europe-67691222 (last accessed 05.02.25)

[70] CERT-UA recorded 4,315 cyber incidents in 2024, available at: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (last accessed 05.02.25)

[71] President's Order of December 19, 2023 No. 1163-r "On approval of the action plan for 2023-2024 for the implementation of the Cybersecurity Strategy of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/1163-2023-p#Text (last accessed 05.02.25)

[72] Decree of the President of Ukraine dated August 26, 2021 No. 447 "On approval of Cybersecurity Strategy of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (last accessed 05.02.25)

Lessons Learned from Incidents Targeting Critical Infrastructure

Ukraine needs to expand its distributed power generation, which is less vulnerable to air attacks due to its network of smaller-capacity facilities, such as gas-fired power generators, renewable energy facilities, and power storage plants. Authorities have introduced regulations to streamline the process of connecting gas turbines. However, the biggest challenge to accelerating this effort is the debt in the electricity market[73], which dampens investment interest, especially given the uncertainties of war.

Repairing damaged facilities remains crucial. Some of the damaged thermal power plants may be repairable by 2024-2025 and 2025-2026 winter, though this will require significant equipment, some of which can be manufactured in Ukraine, with the remainder sourced from other countries supporting Ukraine. Some countries have already committed to supplying Ukraine with equipment from their decommissioned power plants. All these efforts require substantial funding, which energy companies currently lack after three years of enduring Russia's energy-related attacks.

The government aims to make distributed generation more accessible by facilitating affordable financing options for energy equipment purchases and streamlining the processes for building, commissioning, and connecting new generation facilities to the grid. Distributed generation will secure district heating systems which are the primary source of heating in urban areas, where thermal power plants (TPPs), combined heat and power plants, nuclear power stations, and boiler plants provide heat for entire neighbourhoods. Natural gas meets a significant portion of heating needs, serving both district heating systems and individual residential heating: about 80% of Ukrainian households depend on a centralized gas supply, and more than half use centralized hot water systems heated by gas, coal, or, in some cases, biomass. In rural and suburban areas, individual gas, electric, and solid fuel heaters are commonly used by the other half of households.

The damage to underground gas storage facilities from Russian attacks also presents a risk to getting through the next winter, as about half of winter demand is covered by gas from storage facilities. It was assumed that Ukraine would probably have to rely more on gas imports from Europe during the winter. This presents yet another problem because in recent years, European countries have relied on storing gas in Ukraine.

Despite Russian attacks, all customer nominations for gas storage services and capacity reservations were fully met. However, by late November, commercial exports of gas stored by non-residents in the "customs warehouse" regime had nearly ceased. Anticipating the end of Russian gas transit to the EU via Ukraine on 31 December 2024, active withdrawals from storage facilities led to a decline in reserves from 0.5 to 0.1 billion cubic meters.

As of January 1, 2025, following the expiration of the gas transit contract, the transportation of Russian gas through Ukraine has ceased entirely[74]. Ukraine's gas transportation system continues to operate without Russian gas transit, having pre-emptively prepared to function

[73] The debt on the balancing electricity market of Ukraine reached a record level of UAH 34.5 billion for 2024, which poses a serious threat to the development of the country's energy sector. In 2024, debts to producers of electricity from renewable energy sources (RES) almost doubled and reached, according to some estimates, up to UAH 38 billion.

[74] Energy Ministry of Ukraine: The Russian gas transportation has stopped, available at: https://mev.gov.ua/novyna/tranzyt-rosiyskoho-hazu-zupyneno (last accessed 05.02.25)

in zero transit mode while ensuring a stable gas supply for domestic consumers. Ukraine has duly informed its international partners of this development. Notably, European Commission has proposed to phasing out Russian gas by 2027, aligning with the objectives of the REPowerEU initiative - an approach that mirrors Ukraine's current actions.[75]

The extensive missile and drone attacks on Ukraine's energy infrastructure have severely threatened the country's energy security, disrupting access to essential services such as electricity, heating, and water supply. In alignment with its EU accession goals and commitment to a green transition— including OECD-compliant corporate governance standards—Ukraine is receiving support from international partners to ensure a sustainable economic and social recovery of its critical energy infrastructure.

In cooperation with these partners, the Government of Ukraine has taken steps to secure its critical energy infrastructure. The Energy Community's "Ukraine Energy Support Fund" aims to protect this infrastructure from further attacks, including by bolstering Ukraine's air defence capabilities.

Ukraine's national CI protection system includes management bodies, resources, and personnel from central and local executive authorities (including military-civil administrations, if established), local self-governance bodies, and CI operators. These entities are responsible for developing and implementing national policy on CI protection. A key component of this system is collaboration with other countries and international organizations to exchange expertise and coordinate efforts in this area.

The government is reinforcing security measures at facilities vital to societal resilience. A comprehensive set of actions is underway, including monitoring and rapid responses to potential threats such as terrorist attacks, cyber-attacks, and natural disasters.

To sum up, the following factors should be considered when assessing the future protection of Ukraine's energy infrastructure:

- The ability of defence forces and energy market participants to provide robust active and passive protection of highly vulnerable facilities, particularly infrastructure critical to nuclear power generation.
- The availability of transmission and distribution system operators with a reserve of the most vulnerable equipment, sufficient stocks of consumables, and an adequate number of professional repair teams to swiftly restore networks and systems following attacks or natural disasters.
- The overall condition of the energy infrastructure, including the extent of wear and tear and the number of repairs already undertaken.[76]

[75] REPowerEU, European Commission, available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/repowereu-affordable-secure-and-sustainable-energy-europe_en (last accessed 05.02.25)
[76] Gennadiy Riabtsev, Volodymyr Omelchenko, Overview of the Energy Market Operation in December 2024, available at: https://razumkov.org.ua/images/2025/01/21/2025-PAKT-ENERGY-2.pdf (last accessed 07.01.25)

Cybersecurity is a crucial component in countering Russia's aggression. Investments are essential to enhance Ukraine's capacity to respond to and recover from Russian cyber-attacks, particularly those targeting the CI operators.

Incidents and attacks on critical infrastructure in the Baltic Sea

Damage to CI in the Baltic Sea has become more and more recurrent after Russia's attack on Ukraine in February 2022. While the Baltic Sea is relatively far from the war zone, it has been one of the main theatres of the escalation of tensions between Russia and NATO/the EU. Moreover, it appears that the first and arguably most destructive of the CI attacks in the Baltic Sea, the explosions along the Nord Stream pipelines in September 2022, is a direct spill-over of the Russo-Ukrainian war, if we accept Western official and press reports blaming Ukrainian nationals. For all the incidents in the Baltic Sea since 2022, however, no clear state responsibility has been identified thus far (as of January 2025). At the same time, it is highly plausible that all of them have a link to the ongoing conflict and the related tensions. Both Russia and Ukraine have taken measures to ensure the deniability of any official involvement; lacking evidence of deliberate state involvement has allowed shifting the blame on individuals or (shadow) commercial ships.

On 26 September 2022, both Nord Stream pipelines (as well as one of the two Nord Stream 2 pipes, which had not yet become operational) were damaged heavily by underwater explosions in the exclusive economic zones of Denmark and Sweden. None of these pipelines, built to transport gas from Russia to Germany and the EU, were delivering gas to markets at the time of the explosion. Nonetheless, they were filled with gas, hence the leaks caused considerable environmental damage to the already fragile Baltic Sea ecosystem. Nord Stream is owned by the Russian company Gazprom together with German, French and Dutch commercial partners. Gazprom is the sole owner of Nord Stream 2 project, but its EU-based partners invested significant sums in its construction.

Observers and state representatives, both in the West and Russia, argued that the pipelines had been sabotaged; however, different opinions and reciprocal accusations characterised the subsequent debate on responsibility.[77] Sweden, Denmark and Germany started separate investigations. In February 2023, Russia formally submitted a proposal to the UN Security Council calling for an investigation into the sabotage, which was, however, rejected. Also in February 2023, US journalist Seymour Hersh published an article arguing that United States Navy divers, acting with the support of the Norwegian secret service and navy, were responsible for destroying the Nord Stream pipelines.[78] Hersh's story was based on a single source that allegedly had "direct knowledge of the operational planning". In March 2023, an investigation of The New York Times, citing US intelligence sources, argued that an unspecified pro-Ukrainian group was to blame for the detonations; in response to the article, the Ukrainian government denied any involvement.[79]

---

[77] Lee, M. (2023) 'A global mystery: What's known about Nord Stream explosions'. AP News, 8 March. https://apnews.com/article/us-germany-russia-denmark-ukraine-gas-pipeline-attack-nord-stream-2561f98ba6462db700f7609552a28c24.

[78] Hersh, S. (2023) 'How America Took Out The Nord Stream Pipeline', 8 February. https://seymourhersh.substack.com/p/how-america-took-out-the-nord-stream.

[79] Entous, A., J. Barnes and A. Goldman (2023) 'Intelligence Suggests Pro-Ukrainian Group Sabotaged Pipelines, U.S. Officials Say'. New York Times, 7 March. https://www.nytimes.com/2023/03/07/us/politics/nord-stream-pipeline-sabotage-ukraine.html.

The Swedish and Danish investigations were closed in February 2024 without identifying any culprits. The German investigation continued, leading to an arrest warrant issued against a Ukrainian national in August 2024. However, the suspected culprit managed to leave the EU before being apprehended. German press reported that Polish authorities may have unofficially helped the suspected individuals to escape; incidentally, Poland had vigorously opposed the construction of the Nord Stream pipelines.[80] Regardless of who is to be blamed for the Nord Stream explosions, they remained a difficult topic for Western allies due to divergent views on the pipelines and the fact that – despite their controversial nature and the suspension of their utilisation in the context of Russia's aggression of Ukraine – they were at all effects European critical energy infrastructure. The lack of clear condemnation of the explosions did little to dispel the idea that similar attacks, far from the war theatre and on EU territory or economic zones, were "fair game".

While lacking a proved link to the Russian state, subsequent incidents are widely suspected to be Russian hybrid actions. As we shall see, the response of EU countries has evolved over time. On 8 October 2023, just over a year after the Nord Stream explosions, the gas pipeline Balticconnector between Finland and Estonia was damaged, together with a data cable connecting the two countries. Following a drop in pressure, damage was located in Finland's exclusive economic zone, which led to the opening of an investigation by Finnish officials, in cooperation with their Estonian counterparts. On 24 October, 2023, Finland's National Bureau of Investigation (NBI) and the Border Guard stated that an anchor was found near the hole in the pipeline. A Chinese ship named Newnew Polar Bear sailed over Baltic-connector at the exact time of the accident. Later, it was seen in Saint Petersburg without its second anchor. Hence, the NBI suspects that the Chinese ship broke the gas pipeline. The ship crew refused to cooperate with the Finnish investigators. Thereafter, Finnish authorities focused on cooperating with Chinese authorities and pursued the management of the shipping company that owns Newnew Polar Bear. The damage to Balticconnector was eventually repaired in April 2024.[81]

The next major disruption was the severing of two undersea fibre-optic telecommunication cables on 18 November 2024, C-Lion1 connecting Finland to Germany and Arelion linking Latvia and the Swedish Island of Gotland. This led to investigations from the affected countries, official claims of sabotage (however without openly blaming Russia or other actors) and a general resolve to increase navy patrols in the Baltic. A Chinese ship, the Yi Peng Three, was in the area of the accidents at the time when they happened, having left the Russian port of Ust-Luga, on 15 November. From 19 November, it was anchored in international waters off Denmark under the supervision of the Danish navy. China denied any involvement and declared its openness to cooperate in the investigations, but later rejected Sweden's request to investigate the ship, which resumed its voyage in late December. Also in the autumn 2024, Baltic Sea countries started to adopt a more security-oriented

[80] Diehl, J. et al. (2024) 'So entwischte der mutmaßliche Nord-Stream-Sprenger der Polizei', *Der Spiegel* 29 August. https://archive.ph/20240829120157/https://www.spiegel.de/politik/nord-stream-anschlag-wie-der-mutmassliche-pipeline-sprenger-der-polizei-entwischte-a-ecc235ff-2703-483e-bf19-c47badd28918#selection-877.0-877.62.

[81] Yle News (2024) 'Baltic gas pipeline ruptured by Chinese ship back in service after €40m repair job', 22 April. https://yle.fi/a/74-20084948.

approach to new energy projects in the Baltic Sea, as highlighted by Sweden's decision to veto the construction of 13 offshore windfarms due to security risks.[82]

Furthermore, on 25-26 December 2024, the Estlink-2 electricity cable and four telecommunications cables linking Finland and Estonia were damaged. An oil tanker flying the Cook Islands flag and *en route* from Saint Petersburg to Egypt was suspected of causing the damage with its anchor, as tracking data showed that it slowed down while passing over the Estlink-2 cable around the time the transmission was disrupted. According to British publication Lloyd's List, the Eagle S is part of Russia's "shadow fleet" carrying oil to international markets while avoiding the Western oil price cap and sanctions. The 20-year-old tanker is the only ship of Caravella, a company registered in the United Arab Emirates; its poor state of maintenance made its activities an environmental threat. This time, Finland's response was more resolute. The Finnish border guard boarded the ship and escorted it to Finnish territorial waters, and a three-kilometre no-fly zone was imposed in the area. The Finnish police began investigating the incident as a case of aggravated vandalism, focusing on the intentionality of the damage.[83] The investigation revealed that the ship left a 100-kilometre-long trail by dragging its anchor. However, as of January 2025, any intentionality remained difficult to ascertain and, based on media reports, the Finnish intelligence believed that the damage was caused by an accident rather than by Russia or another country.[84]

The string of increasingly frequent accidents continued. On 26 January 2025 an undersea fiber optic cable between Latvia and Sweden belonging to Latvia State Radio and Television Centre was damaged. Sweden launched an investigation into the damage and seized control of a vessel that was suspected of carrying out the sabotage. The Latvian Navy sent a patrol boat to inspect a ship suspected of involvement and launched an investigation of two other ships in the area.[85] Guaranteeing the full security of the CI in the Baltic Sea remains a daunting task. However, in mid-January 2025 NATO leaders met in Helsinki and decided to launch a new mission, dubbed Baltic sentry, including frigates, maritime patrol aircraft, and a fleet of naval drones to provide enhanced surveillance and deterrence.[86]

The combination of surveillance and quick response military measures, together with longer term investigations of accidents, appears to have developed into best practice for NATO countries, particularly those in the Baltic Sea region. The Baltic Pipe and Baltic-connector gas pipelines, high-voltage electricity connections including parts of the so-called Baltic Ring, as well as the denser network of undersea telecommunications cables, are seen as CI that needs protection from hybrid attacks. Existing and future wind farms (especially off the coast of Denmark, but also Poland and the Baltic States) are also critical, as offshore wind is essential to the achievement of EU climate targets. While onshore, the 10 existing

---

[82] Bryant, M. (2024) 'We assume damage to Baltic Sea cables was sabotage, German minister says', *Guardian*, 19 November. https://www.theguardian.com/world/2024/nov/19/baltic-sea-cables-damage-sabotage-german-minister.
[83] Yle News (2024) 'Estlink cable disruption: Finnish Border Guard detains tanker linked to Russia's 'dark fleet'', 26 December. https://yle.fi/a/74-20133516.
[84] Helsingin Sanomat (2025) 'Eagle S -tutkinnassa ei ole löytynyt näyttöä kaapeli-rikon tahallisuudesta – Supo ei usko Venäjän osallisuuteen', 21 January. https://www.hs.fi/tutkiva/art-2000010979641.html.
[85] DW (2025) 'Latvia: Undersea cable likely damaged by external influence', 27 January. https://www.dw.com/en/latvia-sweden-cable-damage-nato/a-71416470.
[86] DW (2025) 'NATO unveils Baltic Sentry pipeline, cable security mission', 14 January. https://www.dw.com/en/nato-unveils-baltic-sentry-pipeline-cable-security-mission/a-71292043.

LNG terminals and 2 more under construction in NATO countries are also deemed to be part of a fragile CI ecosystem that needs securing.[87]

Summing up, there are three types of threats to CI in the Baltic Sea, based on what we know so far: 1) those emanating directly from the Russo-Ukrainian conflict, with one side attacking the critical CI of its enemy (with only secondary, if any, involvement of the West), as in the case of the Nord Stream pipelines; 2) hybrid operations against critical CI that are likely linked to West-Russia tensions, with entities related to Russia in various ways damaging EU CI (this could be the case of Baltic-connector); 3) cases in which the damage seems to be linked to accidents, rather than deliberate action, linked for instance to the poor conditions of the "shadow fleet" exporting Russian oil (as of January 2025, this is possibly the case of the accident involving Eagle S). However, as one of the Baltic States' officials noted, referring to the sharp increase in a number of incidents against CI in the Baltic Sea, even having in mind poor state of Russia's "shadow fleet", it could hardly be a coincidence that this increase of incidents in the Baltic Sea and Taiwan Strait has been observed since the start of Russia's full-scale war in February 2022.[88] The suspected motives behind these acts of sabotage, constituting part of Russia's hybrid attacks, are to test responses of NATO countries, individually and collectively, to increase uncertainty and distrust within their societies as well as between allies.

Effective measures for the protection of CI in the Baltic Sea can involve surveillance of the critical areas by military ships, including coordination among NATO allies and bilateral cooperation in adjacent economic zones. In case of accidents, the patrolling ships would apprehend suspected vessels and confiscate them, within the boundaries of international law, if there are strong elements to believe that they are responsible for the damage. Swift investigation with international cooperation is essential to ascertain responsibility in a just manner. To strengthen the resilience of CI, besides the patrolling of the sea (which also acts as a deterrent), Western CI operators could insure CI with companies that are trained to and capable of swiftly repairing the damage. As official from Lithuania summed it up, there is a need: (1) to step up protection of CI by increasing patrolling in the Baltic Sea by NATO ships, (2) to upgrade the abilities to undertake repairs of damaged CI swiftly to restore their functionality, and (3) to be able to deter violators from such acts by signalling about the costs that would be imposed on potential aggressor, although acknowledging that Baltic Sea region states currently lack capacities for this.[89]

Concluding remarks and lessons learned

The analysis of evolving landscape of threats to energy, communications, transport and other CI in the Baltic States, Ukraine and the Baltic Sea region shows that hostile activities by authoritarian states, in particular, Russia, or actors linked to them have become increasingly frequent. Their proliferation especially intensified after Russia's full-scale war against Ukraine in 2022, as it also became a wider confrontation between the West and

[87] Dudzinska, K. (2025) 'Acute Need for Security of Critical Infrastructure in the Baltic Sea Region', PISM Bulletin 5, 16 January. https://www.pism.pl/publications/acute-need-for-security-of-critical-infrastructure-in-the-baltic-sea-region.
[88] Interview with a former senior official of the Government of Lithuania (2020-2024), February 8, 2025, Vilnius.
[89] Interview with a former senior official of the Government of Lithuania (2020-2024), February 8, 2025, Vilnius.

authoritarian powers. These attacks, often hybrid as they are accompanied by disinformation campaigns, currently constitute the most important threat to CI in the EU and candidate countries. The type of actual attacks varies from cyber-attacks and sabotage against EU member states to military aggression and physical destruction against Ukraine. This has important implications for the policies of protecting CI and increasing its resilience.

Probably the most important lessons include, first, the need for close and transparent partnerships between different actors within countries – CI operators, regulators, intelligence and defence authorities, civic society and media. Rules and procedures of conduct to minimise risks and increase robustness of CI facilities and rapidity in restoring their functions in case of shocks are important as well as regular practices aiming for agility and flexibility in the face of changing technologies used. Agile cooperation can sometimes substitute the lack of resources and insufficient capabilities which often require substantial investments and redundancies.

Second, cooperation between countries, especially within the EU and NATO formats, such as timely cross-border sharing of intelligence, pooled expertise and other resources, joint exercises contribute to being better prepared for potential incidents and for restoring the vital functions to society and state. While these are well-know factors which strengthen the resilience of CI they need to be regularly practiced. Besides, more systemic formats of cooperation between the EU and its candidate countries could be developed to facilitate such practices.

4 Overview of critical infrastructure policies in selected candidate countries

The following sections present the state of affairs with respect to CI policies in selected candidate countries, the key legislative initiatives related to protection and resilience of CI and the driving factors behind them, including external shocks hostile actors and evolving patterns of interdependencies and integration into the EU.

As it was underlined in the introduction, the country cases have been selected to represent three candidate countries, which differ in terms of their state of accession into the EU, their connectivity patterns and risks to their CI associated with them. Montenegro is a case of the candidate country from Western Balkans which is far advanced in EU accession negotiations, and it is a NATO member. Ukraine and Georgia are two of the three Eastern partnership countries that gained EU membership perspective after Russia's full-scale war against Ukraine in 2022, but their current situation is different due to divergent policies of their governments. These differences are likely to be reflected in different challenges they face with respect to CI policies and possibilities for their alignment with the EU.

Montenegro

Evolving landscape of threats to critical infrastructure

In Montenegro, the protection and resilience of CI have become paramount, especially in the face of evolving threats such as cyber-attacks and hybrid warfare.[90] In recent years, Montenegro has increasingly focused on strengthening the security and resilience of its CI. The country has recognized, the growing complexity of threats in official national strategies, laws, and political statements made by Montenegrin government officials, as well as in EU and NATO reports. Particularly in the cyber domain, which has led to heightened discussions among policymakers, security experts, and the public.[91]

Montenegro is susceptible to natural hazards such as floods, earthquakes, and wildfires. The increasing frequency and severity of these events, potentially exacerbated by climate change, have prompted discussions on enhancing the resilience of CI. A 2024 World Bank report emphasized the need for Montenegro to invest approximately $5.7 billion over the next decade to strengthen its resilience against climate impacts. The report advocates for nature-based solutions, such as floodplain restoration, as well as urban adaptation measures, including green infrastructure and improved water systems, to mitigate the effects of extreme weather events.

The digitalization of essential services has increased vulnerabilities to cyber threats. In August 2022, Montenegro experienced a significant cyberattack which disrupted government IT systems, affecting services in transportation, energy, and finance, and causing significant economic losses.[92] This incident underscored vulnerabilities within governmental operations and the potential widespread impact of cyber threats. Power companies were forced to revert to manual operations, highlighting the susceptibility of the energy sector to cyber threats. Financial institutions were also targeted, prompting discussions about the resilience of banking systems against cyber threats. The attack, attributed by Montenegrin authorities to Russian state-sponsored actors, was seen as a retaliation for Montenegro's alignment with NATO and EU sanctions against Russia.[93] The further investigations revealed that the attack was carried out by the Cuba ransomware group, a financially motivated cybercriminal organization with Russian-speaking members, although no direct ties to the Russian government were confirmed.[94] In response, the FBI and cybersecurity experts from France and the UK were called in to help investigate and strengthen Montenegro's cyber defences.

Despite an understanding of and efforts to appropriately address these issues, Montenegro remains vulnerable due to limited cyber security resources, outdated technology in some CI

[90] European Parliament: Montenegro's NATO accession and Russian influence in the Balkans, April 2021, available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/747096/EPRS_BRI%282023%29747096_EN.pdf (last accessed 21.01.2025)
[91] World Bank: Montenegro Country Climate and Development Report, December 2024, available at: https://www.worldbank.org/en/country/montenegro/publication/montenegro-country-climate-and-development-report (last accessed 22.01.2025)
[92] European External Action Service: Assessment of Cybersecurity Risks in Montenegro: Challenges and Recommendations'. EU Publications, October, 2023, available at: https://www.eeas.europa.eu/sites/default/files/documents/2024/Montenegro%20Report%202024.pdf (last accessed 21.01.2025)
[93] Based on the interview with the Ministry of Interior's officials, October 17, 2024, via Zoom.
[94] Political Violence at a Glance: Who Attacked Montenegro? The Moral and Strategic Hazards of Misassigning Blame, September, 2022, available at: https://politicalviolenceataglance.org/2022/09/21/who-attacked-montenegro-the-moral-and-strategic-hazards-of-misassigning-blame/ (last accessed 25.01.2025)

sectors, and a lack of coordination between public and private entities which is important for increasing resilience of CI.

Another concern is linked to the growing presence of authoritarian states in Montenegro through investments and other types of interdependencies. China has been expanding its economic footprint in Montenegro through debt financing infrastructure. One of the most controversial projects is the highway project financed by China's Exim Bank loan, which has left Montenegro with a $1 billion debt to China. This financial dependence has raised concerns about potential economic coercion and strategic vulnerabilities. Critics argue that reliance on Chinese technology and investment in CI sectors, such as telecommunications and energy, could compromise Montenegro's sovereignty. [95] The risks associated with foreign control over strategic infrastructure, which the European Parliament's 2021 study highlighted, emphasizing the need for stringent investment screening mechanisms to safeguard national security interests.[96]

In that regard, particularly important sectors are telecommunication, energy and finance[97]:

- Telecommunications: Potential usage of Chinese technology, such as Huawei's 5G infrastructure, could raise security concerns about data privacy and foreign surveillance.
- Energy: Russian and Chinese investments in energy infrastructure could led to fears of over-dependence on foreign-controlled resources.
- Finance: Foreign capital in Montenegrin banks poses risks of money laundering and undue political influence.

Potential foreign direct investments (FDI) into Montenegro's CI sectors have sparked debates about national security risks.[98] While investment is crucial for economic development, concerns persist about foreign control over CI and the potential for espionage or cyber threats. In response, Montenegro has tightened its investment screening mechanisms and increased cooperation with NATO and the EU to secure its infrastructure from potential geopolitical risks. However, balancing economic development with national security remains a challenge.

Legislative framework and institutions involved in the critical infrastructure policies

Montenegro has established a legal framework to regulate the protection and resilience of its CI. A cornerstone of this framework is the Law on Determination and Protection of Critical Infrastructure, adopted in December 2019 and coming into effect in January 2020. This Law was primarily driven by the need to align with EU standards, influenced by Council

[95] Center for European Policy Analysis: Chinese Influence in Montenegro', 2022, August , available at: https://cepa.org/comprehensive-reports/chinese-influence-in-montenegro/ (last accessed 25.01.2025)
[96] European Parliament: Foreign Direct Investment Screening in the EU and its Impact on Critical Infrastructure Protection, July, 2021, available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762844/EPRS_BRI(2024)762844_EN.pdf (last accessed 21.01.2025)
[97] European External Action Service: Assessment of Cybersecurity Risks in Montenegro: Challenges and Recommendations'. EU Publications, October, 2023, available at: https://www.eeas.europa.eu/sites/default/files/documents/2024/Montenegro%20Report%202024.pdf (last accessed 25.01.2025)
[98] European Parliament. (2021). 'Montenegro's NATO accession and Russian influence in the Balkans', 18, January. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/747096/EPRS_BRI%282023%29747096_EN.pdf (last accessed 21.01.2025)

Directive 2008/114/EC on the identification and designation of European Critical Infrastructure (ECI), and the EU Cybersecurity Strategy and the NIS Directive (2016/1148), which emphasize the resilience of critical information infrastructure (CII). This law outlines the procedures for identifying CI across various sectors, including energy, transport, water supply, health, finance, electronic communications, ICT, environmental protection, and the functioning of state bodies. However, the Law doesn't cover recent developments in the EU and the new Law is expected in 2025.[99]

Montenegro's Cybersecurity Strategy for 2022-2026 was adopted in December 2021. This strategy aims to enhance national cyber security and resilience by focusing on risk management, threat prevention, and incident response. It is an inter-ministerial document that outlines a five-year plan to improve the country's capacity to address challenges and threats in cyberspace.

This legislation mandates that relevant ministries propose CI within their sectors, with the government responsible for official designation. CI operators are required to develop Security Plans and appoint Coordinators to oversee protection measures. Institutions that play pivotal roles in formulating and implementing policies related to CI protection are:

- Ministry of Interior: Oversees the Police Directorate and is responsible for public safety, including aspects related to CI protection.
- Ministry of Defence: Manages the military aspects of CI protection, particularly concerning defence-related infrastructure.
- National Security Agency (ANB): Handles counterintelligence.

Public attention has particularly focused on the ICT sector, especially after the 2022. In response, Montenegrin authorities have engaged in discussions to understand the multifaceted nature of these threats and to develop comprehensive strategies to counter them. This includes enhancing cyber defenses, improving information sharing among institutions, and collaborating with international partners to address the challenges posed by hybrid attacks. In response to the increasing threat of hybrid attacks, the Montenegrin government has undertaken several initiatives to strengthen CI protection:

- Legislative Measures: Establishment of the Government Computer Incident Response Team (CIRT): Following the 2022 cyberattacks, the government established a CIRT to monitor and respond to cyber threats targeting state institutions. The CIRT operates 24/7, utilizing advanced tools to detect and mitigate potential attacks.
- International Collaboration: Recognizing the transnational nature of cyber threats, Montenegro has engaged in partnerships with the FBI and cybersecurity experts from France and the United Kingdom, to aid incident response and bolster cyber defences.

In the aftermath of the 2022 cyberattacks, the government proposed a new Law on Information Security, to address emerging cyber threats and align with EU directives. The law introduces stricter measures for both public and private sectors, encompassing entities from critical sectors such as energy, transport, healthcare, finance, and digital services. It

[99] Based on the interview with the official from the Department for Critical infrastructure, Ministry of Interior, February 10, 2025, Podgorica.

mandates the implementation of comprehensive technical and organizational measures to protect network and information systems, including cyber risk management and data encryption. The law was adopted at November 2024 and proposes the establishment of a Cybersecurity Agency and a Computer Incident Response Team within the Ministry of Public Administration.

In the meantime, the Law on Prevention of Money Laundering and Financing of Terrorism was adopted in December 2023. This law aims to align Montenegro's legal framework with relevant EU directives and comply with the recommendations of the Financial Action Task Force. It underscores the importance of safeguarding financial infrastructure against illicit activities.[100]

Nevertheless, experts from the European External Action Service have raised concerns about potential overlaps in responsibilities between the proposed Cybersecurity Agency and the government's CIRT, which could lead to inefficiencies and challenges in implementation, and highlighted the need for a clearer delineation of responsibilities among institutions involved in CI protection. [101] They have also raised questions about the readiness of Montenegro's public and private sectors to meet the stringent requirements outlined in the Law on Information Security, given existing resource constraints. Strengthening public-private partnerships, regulatory clarity, and financial support for infrastructure resilience will be key to enhancing Montenegro's CI protection in the future.

Lessons and concluding remarks

Montenegro's critical infrastructure protection strategy is driven by the need to comply with EU regulations, address emerging cyber threats, and strengthen national security. These efforts focus on legal reforms, cyber security, physical security, and improved coordination between public and private actors.

First, strengthening the legal and regulatory framework has been a key priority. The Law on Determination and Protection of Critical Infrastructure (2019) establishes a comprehensive framework for identifying, designating, and protecting critical infrastructure sectors, aligning with EU standards. To further enhance security, Montenegro has harmonized its legislation with EU directives, including the NIS Directive (Network and Information Security Directive) and Council Directive 2008/114/EC on European Critical Infrastructure. Additionally, stricter investment screening mechanisms have been implemented to control foreign investments in sensitive sectors such as telecommunications, energy, and finance, aiming to prevent potential security risks.

Second, significant cybersecurity measures and efforts to enhance digital resilience have been implemented. A National Cybersecurity Strategy was created to strengthen the protection of critical infrastructure, particularly in response to the cyber-attacks of 2022. Alongside this, Montenegro developed a National Computer Emergency Response Team (CERT) responsible for monitoring, detecting, and responding to cyber threats. CI operators

[100] European External Action Service: Assessment of Cybersecurity Risks in Montenegro: Challenges and Recommendations'. EU Publications, October, 2023, available at: https://www.eeas.europa.eu/sites/default/files/documents/2024/Montenegro%20Report%202024.pdf (last accessed 25.01.2025)
[101] European External Action Service: Assessment of Cybersecurity Risks in Montenegro: Challenges and Recommendations'. EU Publications, October, 2023, available at: https://www.eeas.europa.eu/sites/default/files/documents/2024/Montenegro%20Report%202024.pdf (last accessed 25.01.2025)

are now subject to increased cyber security obligations, including the requirement to report cyber incidents, conduct regular security audits, and implement stronger encryption and data protection standards. Additionally, Montenegro has fostered international cooperation, receiving support from NATO, the EU, the FBI, and cyber security experts from France and the UK to bolster its digital infrastructure and prevent future cyber threats.

Montenegro actively collaborates with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) and EU cyber security bodies, focusing on knowledge-sharing and training to enhance its cybersecurity capabilities. Additionally, the country is working closely with its neighbouring countries in the Western Balkans to counter hybrid threats and strengthen energy security, reflecting a strong commitment to regional coordination. Montenegro also participates in joint cyber defence exercises with its international allies to improve its response capabilities against sophisticated cyber threats[102].

Third, physical security and risk mitigation measures have been implemented, including sector-specific security protocols for energy facilities, transport hubs, and financial institutions. CI operators are also required to develop emergency preparedness plans, conducting risk assessments and establishing crisis response mechanisms to ensure continuity during natural disasters, cyber incidents, or sabotage. Additionally, backup systems and redundancy measures have been put in place to ensure that alternative infrastructure is available in the event of power failures, cyber disruptions, or terrorist attacks.

Fourth, public-private collaboration and institutional coordination have been prioritized through the creation of a National Critical Infrastructure Coordination Body, which facilitates information-sharing and joint security planning between government agencies and private sector critical infrastructure operators. Public-private partnerships are encouraged to promote investment in modern infrastructure while ensuring compliance with national security requirements. Additionally, private CI operators, including telecommunications companies, banks, and energy providers, are mandated to adhere to government-imposed security measures and participate in national cyber drills to enhance resilience and preparedness.

Ukraine

Legislative framework and institutions involved in the critical infrastructure policies

Building on the chapter 3.2. which presented the main threats related to kinetic and cyber attacks of Russia on Ukrainian energy CI, this chapter analyses legislative framework regulating CI-related policies, interdependencies between Ukraine's energy system and that of the EU, assessing connectivity and the implications of these connections in both the short and long term. It explores opportunities for rebuilding the energy system by leveraging progressive trends and attracting investments.

The national legislation on protection and resilience of CI outlines the state's core principles and objectives in this area. Emerging threats to CI, such as natural and man-made disasters, cyberattacks, and terrorist acts, require robust preventive and mitigation measures. The State Service for Critical Infrastructure Protection oversees policy in this field,

[102] Based on the interview with the official from the Department for Critical infrastructure, Ministry of Interior, February 10 2025.

facilitating coordination and cooperation among various protection entities. It was formed under the recent Cabinet of Minister's Resolution.[103]

Under Ukrainian law, entities within the national critical infrastructure protection system include government agencies, local authorities, and essential enterprises, institutions, and organizations that contribute to national security. Private companies providing critical services to the country's operation are also recognized as part of this system.

The following types of actors are institutionalised within the CI policy system. Critical Infrastructure Operator – a legal entity and/or individual that manages a critical infrastructure facility by ownership, lease, or other lawful basis and is responsible for its ongoing operation. Sectoral Body for Critical Infrastructure Protection (Sectoral Body) – a government body that, according to legislation, develops and implements state policy on critical infrastructure protection within a specific sector. Authorized Body for Critical Infrastructure Protection in Ukraine (Authorized CIP Body) – responsible for formulating and implementing state policy on critical infrastructure protection, overseeing the national critical infrastructure protection system, and coordinating the activities of ministries and critical infrastructure operators on resilience and protection matters.

Additionally, this authorized body maintains and administers the CI Register, a key tool for coordinating Ukraine's CI protection efforts. The register enables stakeholders in the national protection system to synchronize their activities, exchange information, and build a centralized database of threats and vulnerabilities. It also facilitates the certification, security, and assessment of critical infrastructure facilities, ensuring a comprehensive overview of protection status across sectors.

The protection of CI involves implementing a range of measures aimed at preventing, detecting, and mitigating the effects of emergencies that may disrupt the operation of these facilities. These measures are carried out both in peacetime and under the current conditions of martial law.

According to No. 1109 Resolution of the Cabinet of Ministers of Ukraine dated October 9, 2020, "Some issues of critical infrastructure facilities" four levels of criticality have been established for critical infrastructure facilities in Ukraine.[104] The first category includes all facilities of national significance, such as nuclear power plants. The fourth category encompasses general regional facilities (such as kindergartens and schools), classified as such by local authorities.

The specific measures for protecting CI and its legal status in the event of unpredictable crisis situations, extreme conditions, and military actions are outlined in Ukraine's laws "On the Legal Regime of Martial Law," "On the Legal Regime of the State of Emergency," "On the Functioning of the Unified State System of Civil Protection in a Special Period," and "On the Defence of Ukraine."

---

[103] Resolution No. 787 of the Cabinet of Ministers of Ukraine dated July 12, 2022, titled "On the Establishment of the State Service for Critical Infrastructure Protection and Ensuring the National Resilience System of Ukraine, available at: https://zakon.rada.gov.ua/laws/show/787-2022-п#Text (last accessed 11.12.24)

[104] Resolution of the Cabinet of Ministers of Ukraine No 1109 dated 9 October 2020 "On certain Critical infrastructure issues, available at: https://zakononline.com.ua/documents/show/490116___742722 (last accessed 07.02.25)

For 2024, the Ukrainian government has worked out a CI protection policy aimed at safeguarding essential infrastructure from potential threats and hostile attacks. In particular, the deployment of air defence systems within the country is aligned with the criticality levels of facilities, ensuring protection against enemy attacks and technological disasters.

On 19 November, 2024, President of Ukraine presented Ukraine's Internal Resilience Plan (10 Points including Energy).[105] This plan includes a confidential annex detailing measures for the active and passive protection of energy facilities, which hold managers personally accountable for their implementation. The document encompasses:

- Development of regional energy stability passports.
- Demand management and encouragement of rational fuel and energy consumption.
- Implementation of measures to enhance energy efficiency.
- Preparation of regulatory and legal frameworks for establishing a Ukrainian energy hub.
- Support for the development of nuclear energy.
- Increased production and resumption of natural gas and oil processing.
- Further integration of Ukrainian and European gas storage and transportation infrastructure.

It is worth noting that the Law of Ukraine No. 4059-IX (November 19, 2024), concerning the State Budget of Ukraine for 2025.[106] This law allocates the funds for protection of the critical energy infrastructure as follows:

- UAH 115 billion drawn under state guarantees for the restoration of critical infrastructure, including energy infrastructure.
- UAH 42.3 billion for subsidizing housing and communal service payments.
- UAH 18.0 billion for the "5-7-9" lending program.
- UAH 12.2 billion to bridge the gap between actual and economically justified tariffs for heating energy.
- UAH 2.4 billion for restructuring the coal industry.
- UAH 1.8 billion for financing projects under the State Fund for Decarbonization and Energy Efficient Transformation

Overview of the legislation in Ukraine CI Protection is presented in Appendix 1.

Ukraine's energy integration with the EU

In line with EU membership aspirations Ukraine strives to become an electricity supplier for Europe, focusing on its green energy potential. Despite the war, the energy system of Ukraine has preserved its integrity and continued to work with the European continental grid ENTSO-E. The electricity grids of Ukraine (and Moldova) were successfully synchronized with the European power system operated by ENTSO-E. Yet, Ukraine needs to implement EU legislation to enable market integration and competition.

The emergency synchronisation of Ukraine and Moldova to the European continental grid serves short- and long-term interests on both sides. In the short term, this integration has

[105] Volodymyr Zelenskyy Presented Ukraine's Internal Resilience Plan, available at: https://www.president.gov.ua/en/news/volodimir-zelenskij-predstaviv-plan-vnutrishnoyi-stijkosti-u-94505 (last accessed 7.02.25)
[106] Law No. 4059-IX (November 19, 2024), concerning the State Budget of Ukraine for 2025, available at: https://itd.rada.gov.ua/billinfo/Bills/Card/44888 (last accessed 07.02.25)

enabled Ukraine to stabilize its electricity supply during periods of intensive Russian bombardment and maintenance of its nuclear power plants. Furthermore, it has facilitated substantial electricity exports to European neighbours, generating critical revenue for Ukraine.

According to data from ExPro Electricity, Ukraine has quadrupled its total electricity imports in 2024 compared to 2023. From June to August alone, over 2.1 million MWh were imported, which is three times more than the entire previous year. In 2023, the maximum import capacity from European countries in Ukraine from increased 1200 MW to 1700 MW. The transborder trade capacities have been reviewed recently. Prime Minister Denys Shmyhal stated[107] that Kyiv is in the final stages of negotiations with ENTSO-E, the European network of transmission system operators, to raise import limits from the current 1.7 GW to 2.2 GW. From December 1, the maximum capacity for importing electricity from EU countries will be increased from the current 1.7 to 2.1 GW. According to the Energy Ministry, Ukraine will have a guaranteed 250 MW transborder capacity in the emergency aid mode.[108]

Within 10 months in 2022, Ukraine exported electricity worth USD 542.5 million. However, the continuous attack and consequential damages to the power sector also resulted in the Ukrainian government's decision to stop the electricity export to the EU/ENTSO-E starting from 11 October 2022. This was a forced step, as all generation capacities were redirected to meet Ukraine's internal needs. In the future these transactions must be carefully handled to provide enough electricity to Ukrainian consumers. The architecture of trading electricity with EU has to be organised according to the EU rules under the transparent competitive auctions in which companies will purchase the access to interstate power lines.

The next step after the technical synchronization of Ukraine's energy system with the European grid is the integration of our energy markets. Ukraine and the EU are making productive progress in this direction, and in 2022, during Ukraine's chairmanship of the Energy Community, the relevant Regulation and Roadmap were approved[109]. These measures set the stage for the full integration of Ukrainian and European energy markets.

For the EU market, this integration supports more economical energy exchange, strengthens electricity supply security, and diversifies supply routes. For Ukraine, connection to the European transmission system guarantees access to imports and emergency supplies.

Various stakeholders across ENTSO-E are interested in enhancing electricity exchange and advancing transmission system development plans. Ukrenergo, the Ukrainian Transmission System Operator (TSO), has been negotiating with Poland's TSO, PSE, on coordinated actions along the shared transmission profile. A recent modification reconfigured an existing interconnector between Poland and Ukraine, reducing it from 750 kV to 400 kV.

In 2018, SEPS (the Slovakian TSO) and Ukrenergo conducted a bilateral study to assess future system requirements for reinforcing the Slovakia-Ukraine transmission profile as the

[107] Ukraine is negotiating with Europe on expanding electricity imports to 2.2 GW – Denys Shmyhal, available at: https://www.ukrinform.ua/rubric-economy/3902823-ukraina-vede-peregovori-z-evropou-sodo-rozsirenna-importu-elektroenergii-do-22-gvt-smigal.html (last accessed 12.11.24)
[108] ENTSO-E has increased the capacity to import electricity to Ukraine -up to 2.1 GW, available at: https://expro.com.ua/en/tidings/entso-e-has-increased-the-capacity-to-import-electricity-to-ukraine-up-to-21-gw (last accessed 12.11.24)
[109] Ukraine's Power Network Integration with EU ENTSO-E, Energy Ministry of Ukraine, available at: https://mev.gov.ua/en/reforma/ukraines-power-network-integration-eu-entso-e (last accessed 12.11.24)

current interconnector approaches the end of its service life. Further studies will determine whether to upgrade the line to a single-circuit configuration with higher load capacity or to a double-circuit configuration.

MAVIR, the Hungarian TSO, has announced an upgrade of an existing 220 kV line, currently outside of synchronization. Transelectrica, Romania's TSO, has informally agreed with Ukrenergo to include the 400 kV (formerly 750 kV) OHL Pivdennoukrainska NPP (Ukraine) – Isaccea (Romania) line in the upcoming editions of the TYNDP and National Development Plans. This line is already recognized as a Project of Mutual Interest (PMI) by the Energy Community.

In recent years, Ukraine has embarked on a transition to a clean energy system, aligning with its net-zero commitments. National programs and strategies reflect key decarbonization trends, including the electrification of end-use sectors, production of clean hydrogen and its derivatives, carbon capture and storage (CCS, BECCS), and the transformation of gas infrastructure to support a hydrogen and biomethane economy.

One of Ukraine's primary objectives in decarbonizing its energy system is to reduce greenhouse gas (GHG) emissions from the energy sector by decreasing energy demand, electrifying end uses and expanding renewable and low-carbon energy sources. In November 2021, at the UN Conference of the Parties (COP), Ukraine presented its Second Nationally Determined Contribution (NDC-2), committing to a 65% reduction in GHG emissions by 2030 compared to 1990 levels. Despite the challenges of war, over 70% of Ukraine's electricity is generated from non-carbon sources, including nuclear, hydro, and renewable energy.

Beginning in 2026, Ukrainian exports to the EU will be subject to the Carbon Border Adjustment Mechanism (CBAM) under the Fit for 55 package.[110] Ukraine has already begun monitoring its emissions, with plans to introduce an Emissions Trading System as outlined in Directive 87/2003/EC. In 2019, trade with the EU accounted for 40.1% of Ukraine's total trade in goods and services.

Ukraine estimates that emissions from Russia's invasion amount to approximately 33 million tonnes of CO2 from the conflict itself and an additional 23 million tonnes of CO2 from fires caused by the invasion. All new projects in Ukraine will need to address the significant environmental contamination and associated costs.

The renewable energy sector has been sustaining damage from shelling, missiles, and drone attacks. RES development objective need to increase the RES share in electricity, heating and cooling, and in the transport sector.

The National Energy Strategy until 2035 targets 25% of RES in electricity production while the National economic strategy until 2030 sets an even more ambitious goal – 25% of electricity production from RES. The draft National Action Plan for the Development of Renewable Energy until 2030 (to implement the Directive 2018/2001/EC) envisages a 3-fold increase of the RES share in gross final energy consumption: from 9% in 2020 up to 27% in 2030.

[110] European Council, Fit for 55, available at: https://www.consilium.europa.eu/en/policies/fit-for-55/ (last accessed 12.11.24)

Actions to boost Renewable Energy generation include:

- Remove Regulatory Barriers: The regulatory obstacles to renewable energy development need to be dismantled.
- Review Payment Terms for Green Electricity: Payment terms for renewable energy have changed multiple times during the war and require reassessment.
- Address Curtailments and Forecasting Challenges: The TSO continues to apply curtailments to RES generating companies, and production forecasting remains problematic.
- Support for RES Producers: The feed-in tariff should gradually be replaced by other market-based instruments, including net billing, guarantees of origin (in line with the Renewable Energy Directive II (EU) 2018/2001), and corporate power purchase agreements (Corporate PPAs). The necessary legislation is already in place.
- Better storage opportunities. Legislative changes[111] were introduced in Ukraine on electric energy storage, as well as licensing conditions approved to carry out economic activities for energy storage.

According to the Energy Community Secretariat Report,[112] despite ongoing military action, "Ukraine has managed to keep its electricity market model largely intact and has provided assurances that emergency measures taken in the gas sector will be swiftly lifted once the war ends." However, several issues must be addressed before launching new projects.

The electricity market model requires improvements, as various market segments currently face distortions, including Public Service Obligations (PSOs), price caps on day-ahead and intraday markets, artificial regulation, and unresolved debts between major market participants.

Enhancing the market model is essential for attracting new projects and facilitating post-war reconstruction, aligning Ukraine's energy sector with the European market to support greater transparency in price formation.

Agreements with international partners indicate significant potential for Ukraine's involvement in the emerging hydrogen economy.[113] However, implementation of them will largely depend upon conclusion of the military combat and subsequent reconstruction efforts, in which European support will be essential.

Ukraine has been identified as a key partner of the European Clean Hydrogen Alliance for participation in the production and supply (export) of hydrogen, considering natural resources, interconnected infrastructure and the level of technological development.

---

[111] Law of Ukraine "On Amendments to Certain Laws of Ukraine on the Development of Energy Storage Facilities" No. 5436-d of 17 September 2021, available at: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72789 (last accessed 09.12.24)

[112] Secretariat's Implementation Reports, available at http://www.energy-community.org/implementation/report/reports.html (last accessed 09.12.24)

[113] In 2021, an MoU was signed on hydrogen collaboration between Germany and Ukraine on green hydrogen production.
In April 2023 Ukraine signed an MoU with the EU resulting in a strategic partnership on "biomethane, hydrogen and other synthetic gases". In early 2023 Hydrogen Europe published a recovery plan that included the export of green ammonia, and the use of 2 - 4 GW of nuclear power for hydrogen production, with Germany being the preferred off-taker.

Research is underway in Ukraine about the possibilities of low-carbon hydrogen production, competitive price, and supply routes.

This potential role is associated with facilitating the infrastructure development, both by building new assets (electrolysers, renewables, pipelines) and by repurposing existing assets, namely the gas network.

Ukraine can perform the functions of hydrogen hub provided there is the decision on Ukraine regarding the green energy production perspectives. Perspective of being part of European Hydrogen Backbone (EHB) initiative.[114] As the demand for hydrogen as a vector of energy grows, there will be a need to expand a regulated hydrogen network (pipelines, storage).

As stated in the EU Hydrogen Strategy, hydrogen" offers a solution to decarbonise industrial processes and economic sectors where reducing carbon emissions is both urgent and hard to achieve". [115] Overview of the potential inland and cross-border hydrogen projects are presented in Appendix 2.

Lessons and concluding remarks

Ukraine's strategic location and abundant renewable energy resources, including solar, wind, and biomass, position it favourably for a transition towards clean energy. By investing in renewable energy infrastructure and implementing policies to incentivize clean energy adoption, Ukraine can not only reduce its carbon footprint but also reduce its vulnerability to external shocks, enhance energy security and resilience of CI, and stimulate economic growth.

Collaboration with international partners, including the EU, can also play a crucial role in supporting Ukraine's decarbonisation efforts. Through strategic partnerships and cooperation agreements, Ukraine can leverage external expertise and resources to accelerate its transition to a low-carbon economy.

CI rehabilitation is essential to the energy transition in Ukraine to achieve both its ambitious climate goals and to provide the basis for competitive economy in post war period and integration into the European energy market. Despite the full-scale invasion in February 2022 and the enormous pressure, Ukraine has so far managed to maintain the operation of its energy CI and capability to provide essential services, however, sometimes with disruptions.

Nowadays the major challenges remain the political and war risks insurance for the potential private investors in Ukraine. With the war risks being very high, the insurance companies are faced with the issue of offering very expensive coverage for the private investors. Many EU member states see the lack of war insurance as a barrier to private sector involvement in Ukraine's reconstruction.

---

[114] Analyzing future demand, supply, and transport of hydrogen, European Hydrogen Backbone, June 2024, available at: https://ehb.eu/files/downloads/EHB-Analysing-the-future-demand-supply-and-transport-of-hydrogen-June-2021-v3.pdf (last accessed 11.12.24)

[115] European Commission, Brussels, Hydrogen, 2023, available at: https://energy.ec.europa.eu/topics/eus-energy-system/hydrogen_en (last accessed 11.12.24)

Not all aspects of the recovery can or will be funded solely by the public sector. Ukraine, with the support of the EU and other partners, must establish a conducive environment for private investment. This includes the provision of comprehensive security guarantees for Ukraine and financial assurances for early private investments. Equally vital is the enhancement of the rule of law, achieved through increased transparency, judicial reform, and anti-corruption measures.

The ongoing situation in Ukraine presents obstacles when seeking private political risk insurance for investments due to the active phase of war. The information about the current state of war risk insurance is presented in Appendix 3.

The heightened war-related risks make insurance from private providers for investors rather costly. Thus, the responsibility for insuring investments falls on the state. The implementation of insurance mechanisms will facilitate support for economic investment activities by distributing the associated risks among investors, the government, or international donors, with the latter covering the expenses for insurance and potential loss compensation. To fund reconstruction, foreign investors will have to pay premiums to protect themselves against the potential for losses from war destruction.[116]

To address these obstacles and draw private investments into Ukraine, it is crucial to enact substantial economic and regulatory reforms. These reforms should form the basis for Ukraine's economic recovery in the aftermath of the conflict.

Georgia

Evolving landscape of threats to critical infrastructure

This chapter examines the legislative framework for CI-related policies in Georgia, and analyses established practices and experiences in addressing physical, cyber, and hybrid threats. The concluding section assesses the challenges in implementing a whole-of-society approach to CI protection and resilience.

Having in place a robust and well-defined framework for CI protection and resilience is becoming increasingly vital amid today's complex and rapidly evolving security landscape.[117] For countries like Georgia, this need is especially pressing. With a long history of facing Russian military and hybrid aggression,[118] coupled with persistent regional instability, ensuring the resilience of critical infrastructure is not just a matter of strategic importance, but a fundamental necessity for national security.

Another key reason Georgia should have in place a comprehensive approach to CI protection is its strategic location and central role in the Middle Corridor, a vital transport route linking Asia and Europe and an alternative to the Eurasian Northern Corridor[119]. The geopolitical and economic significance of this route has grown considerably following Russia's invasion of Ukraine and the ensuing sanctions, further highlighting Georgia's critical position in regional and global connectivity. Ensuring the security and resilience of its CI is not

[116] Ukraine calls for war insurance to attract private investors, available at: https://www.politico.eu/article/ukraine-war-insurance-attract-private-investors-volodymyr-zelenskyy/ (last accessed 11.12.24)
[117] Council of the European Union: Conclusions on EU Security and Defence, 2024.
[118] Ministry of Foreign Affairs of Georgia: National Security Concept, 2024.
[119] The Northern Eurasian Corridor is a key transcontinental trade route linking Asia and Europe through Russia.

only essential to safeguard trade flows but also to attract foreign investment, enhance logistical efficiency, and foster sustainable economic growth.

Modern critical infrastructure seemingly serves as an effective instrument in the hands of adversaries able and willing to use hybrid tools.[120] In Georgia, the absence of a general framework for CIP makes the lack of a dedicated approach or policy on hybrid threats unsurprising. The issue is particularly pressing given that Georgia was the first target of Russia's hybrid warfare in 2008, and, since then, it has remained a battlefield for Russian hybrid aggression, having been subjected to nearly every tool in Russia's hybrid toolkit.[121]

Hybrid threat activity specifically tends to target democratic systems, and countries in the process of democratization are in a particularly vulnerable position because they have the systemic vulnerabilities of a democracy but not all of the protection of established institutions, traditions, and processes of democracy.[122] Georgia is a case in point. The obstruction of the Namakhvani Hydro Power Plant (HPP) project serves as a vivid example of how hybrid actors capitalize on systemic vulnerabilities and through a sophisticated array of hybrid tactics, including coercive economic activities, disinformation campaigns, social media manipulation, and the spread of ethno-nationalist narratives, hinder the development of Georgia's energy sector that would decrease reliance on Russian energy resources.[123] Beyond the immediate impact of the project's cancellation by the Georgian government, the decision has long-term strategic consequences, undermining Georgia's international reputation and further weakening its investment climate. After long and complex negotiations between opponents of the project and the Georgian government mediated by the Energy Community Secretariat, the contract between ENKA Renewables LLC and the Georgian government to build and operate the Namakhvani HPP in western Georgia (a project worth USD 800 million) was terminated.[124] In addition, it brought a substantial financial burden, as Georgia lost an international arbitration case against the investor, resulting in a compensation payout of nearly USD 400 million—approximately 2% of the country's GDP.[125]

Another critical lesson with implications not only for Georgia's national resilience but also for broader Black Sea security is the Anaklia Deep Sea Port project. The project has endured decades of setbacks and ambiguity, despite its vital economic and political significance for Georgia.[126] The developments surrounding this project also raise significant concerns from a hybrid threat perspective.

The Anaklia Deep Sea Port project was initially viewed as a pivotal opportunity for Georgia, positioning the country as a key trade hub between Europe and Asia while strengthening its ties with NATO and the EU. However, the project took a negative turn in 2020, when the Georgian government decided to terminate its contract with the initial Western-led consortium, consisting of A.P. Moller - Maersk and Conti Group, reportedly due to artificial legal, regulatory, and financial obstacles.[127] In 2023, the Georgian government issued a

[120] Savolainen, J.: Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure, 2019.
[121] Seskuria, N.: Russia's 'Hybrid Aggression' against Georgia, 2021.
[122] Aho et al.: Hybrid Threats: A Comprehensive Resilience Ecosystem, 2023.
[123] Lazari, A., & Tabagua, N.: Critical Infrastructure Security and Resilience in Georgia, 2024.
[124] Civil Georgia: ENKA "Finally" Terminates Namakhvani HPP Contract, 2022.
[125] ITV: ENKA Wins Arbitration Against Georgia Over Namakhvani HPP, 2024.
[126] RFE/RL: The Black Sea Port That Could Define Georgia's Geopolitical Future, 2023.
[127] Hess and Otarashvili: Georgia's Doomed Deep-Sea Port Ambitions, 2020.

statement revealing that it had awarded the project to a Chinese-Singaporean consortium led by China Communications Construction Company Limited (CCCC), a subsidiary of the state-owned China Communications Construction Group (CCCG). CCCC, a major player in China's Belt and Road Initiative (BRI), has a controversial reputation, having been hit with sanctions from the World Bank and several countries. As of February 2025, the Georgian government and the Chinese-Singaporean consortium were finalizing contract negotiations.[128]

While direct evidence linking disruptions in Georgia's strategic projects to foreign malign influence is lacking, the nature of these incidents and their strategic repercussions suggest that hybrid tactics are being applied. This shortage of clear-cut evidence is a key reason why such tactics are particularly effective in the hands of authoritarian regimes. Hybrid actors often exploit a combination of tools to achieve their objectives covertly, aiming to avoid detection, resistance, and response.[129]

Legislative framework and institutions involved in the critical infrastructure policies

Although the Government of Georgia (GoG) marked the development of a legislative framework for protecting CI as a priority within the country's security policy in 2018, no substantive progress has been made in that regard as of early 2025. Initially, an interagency commission was established under the Ministry of Internal Affairs of Georgia.[150] However, after two years, its coordination was transferred to the Office of the National Security Council.[151] Despite this institutional shift, legislative efforts related to CI have remained stagnant, raising concerns about the effectiveness of policy implementation. The interagency commission drafted a legislative framework for protecting CI, but the GoG has not taken it further, leaving the project paused at the draft stage.[152]

The absence of a comprehensive CI policy framework puts Georgia in a highly vulnerable position. The country has adopted a disparate and non-cohesive approach to the physical and cyber security of potential CI, leaving hybrid threats entirely unaddressed in the national legislation and relevant policy documents.

While certain national laws contain terminology that may appear relevant to CIP, they do not effectively address its core principles. As a result, the overall approach remains fragmented and insufficient in responding to the complexities of the modern security landscape. For example, the national legislation includes terms such as "Subjects with high risk for state security"[153] and "Objects of strategic and/or special importance."[154] However, these classifications do not align with the modern understanding of CI protection and resilience. The "subjects" or "objects" mentioned above include certain state institutions, energy companies, Georgian Railway, Georgian Air Navigation Service, airports, and ports, all

[128] Civic IDEA: Anaklia Port – Another Step in Shifting Foreign Policy, 2024.
[129] Aho et al.: Hybrid Threats: A Comprehensive Resilience Ecosystem, 2023.
[150] Government of Georgia: Decree N2033, 2018.
[151] National Security Council of Georgia: First Session of the Interagency Commission on the Development of the National Security Strategy, 2024.
[152] Lazari, A., & Tabagua, N.: Critical Infrastructure Security and Resilience in Georgia, 2024.
[153] Government of Georgia: Law on Approval of the List of Entities Containing High Risks to National Security, 2015.
[154] Government of Georgia: Ordinance No. 361, 2024.

of which are subject to a state security protection regime under the Law of Georgia on the State Security Service.[155] However, this falls significantly short of contemporary CI protection standards. The criteria for selecting entities for inclusion in these lists remain unclear, and, more critically, the framework overlooks essential aspects of modern physical security, such as risk-based assessments, resilience planning, and the integration of physical threat mitigation strategies.

Furthermore, the "objects of strategic and/or special importance" list bears no connection to CI and has increasingly been used over the past two years as a tool to suppress civil protests and enable political repression.[156] The list was originally developed under Georgia's criminal law, specifically in relation to Articles 222 and 330,[157] which establish criminal liability for the seizure or blockade of such objects. These provisions criminalize actions that disrupt or could potentially disrupt the normal operation of designated institutions or facilities, as well as those carried out for terrorist purposes. Notably, the first provision (regarding seizure or blockade of objects) has been frequently applied against peaceful protesters, in some cases leading to their imprisonment.[158] Moreover, the scope of the list has expanded over time, often encompassing locations associated with public demonstrations, raising concerns about its potential use as a means of restricting civic activism and public dissent.[159]

Although Georgia lacks a comprehensive regulatory framework and legislative principles for CISR, substantial efforts have been directed toward strengthening cyber security in the country.[140] This stems primarily from the lessons learned during the 2008 Russo-Georgian war, when Georgia faced significant cyber-attacks before kinetic operations,[141] which have since continued unabated. Russian hackers have consistently exploited Georgia's digital ecosystem, targeting various sectors, including public institutions, healthcare, and the highly digitized financial sector.[142]

Georgia has adopted three versions of its National Cybersecurity Strategy (2013-2015, 2015-2017, and 2021-2024),[143] underscoring the country's strong commitment to cybersecurity within its broader security architecture. The Law of Georgia on Information Security, which sets standards for information security, has been in force since 2012. Over the years, it has undergone multiple amendments, with the most significant revision coming in 2022. This amendment introduced the term *"critical information system,"* which was defined as an information system whose uninterrupted operation is essential to national defense, economic security, and the normal functioning of the state and society.[144]

---

[155] Parliament of Georgia: Law on the State Security Service of Georgia, 2015.
[156] BBC News: Georgia's PM hits back as protests and resignations intensify, 2024.
[157] Parliament of Georgia: Criminal Code of Georgia, 2024.
[158] Ministry of Internal Affairs of Georgia: Official Statement, February 1, 2025.
[159] Radio Free Europe/Radio Liberty: How 'Georgian Dream' Revived a 'Dead Article' of the Criminal Code, 2025.
[140] Lazari, A., & Tabagua, N.: Critical Infrastructure Security and Resilience in Georgia, 2024.
[141] Atlantic Council: Russian Cyber Strategy and the War Against Georgia, 2014.
[142] Civil Georgia: Bloomberg: Russia Hacked Entire Georgia Between 2017-2020, 2024.
[143] All strategies are accessible at https://matsne.gov.ge/
[144] Parliament of Georgia: Law on Information Security, 2012.

The law's scope was broadened to cover a wider range of entities, requiring the classification of critical information system (CIS) subjects. This revision aimed to enhance regulatory efficiency and oversight by assigning specific supervisory agencies to each category.

The 2022 amendments to the Law of Georgia on Information Security categorize CIS subjects into the following three distinct tiers:[145]

- First Category: All state bodies and institutions, legal entities under public law, and state-owned enterprises with the Operative-Technical Agency (OTA) of the State Security Service of Georgia acting as the supervisory agency;
- Second Category: Telecommunications companies and internet service providers, also falling under the supervision of the OTA; and
- Third Category: Private entities such as financial institutions, energy providers, transportation companies, and insurance firms, which are supervised by the Digital Governance Agency of the Ministry of Justice.

Despite strong criticism from Georgian civil society organizations (CSOs) of the amendments, which they argue grant the OTA unrestricted access to public and telecom data, as well as experts'[146] concerns about the need for further refinements to meet international cyber security standards, the reforms marked a significant step toward aligning with EU standards and strengthening Georgia's cybersecurity framework.[147]

Lessons and concluding remarks

As it was noted, the absence of a comprehensive CI policy framework puts Georgia in a highly vulnerable position. The country has adopted a disparate and non-cohesive approach to the physical and cyber security of potential CI, leaving hybrid threats entirely unaddressed in the national legislation and relevant policy documents. More progress has been achieved in the field of cyber security, although it has been criticised by CSOs on the basis of privacy concerns which is related to broader political polarisation within the country and distrust of the current authorities.

The challenges in developing a CI protection and resilience framework in Georgia extend beyond the confines of governmental spheres.[148] The engagement of civil society and academia with this critical issue has been notably slack. Moreover, there exists a significant void of awareness within the private sector regarding the notion of CI. The absence of a public-private partnership model, due to the lack of a national CI protection policy, further exacerbates this issue.

It should be noted that donor assistance has predominantly focused on enhancing the cybersecurity aspects of CISs, often overlooking other critical areas such as overarching CI protection and resilience governance, physical infrastructure protection, and intersectoral coordination. Recent backslide of the Georgian government in terms of EU accession and cooperation with Western partners is likely to further complicate needed steps towards adopting adequate policy framework and daily routines in protecting CI and strengthening

[145] Government of Georgia: Ordinance No. 646, 2021.
[146] Exploratory interview with Cyber Security Expert Giorgi Iashvili, December 20, 2024, Tbilisi.
[147] Clayton, M. (2021, June 10). X.
[148] Exploratory interview with Security Policy Expert Shalva Khutsishvili, January 30, 2025, Tbilisi.

its resilience through trust based networks of actors domestically and cooperation with the EU and NATO member states.

5 Conclusions and recommendations

The report provided an extensive discussion of evolving landscape of threats to the CI in the EU and candidate countries in recent years and the challenges which, while varying depending on particular countries, also are common to all states affected by geopolitical tensions.

As it was noted before, the analysis of threats to energy, communications, transport and other CI in the Baltic States, Ukraine and the Baltic Sea region shows that hostile activities by authoritarian states, in particular, Russia, or actors linked to them have become increasingly frequent. Their proliferation especially intensified after Russia's full-scale war against Ukraine in 2022, as it also became a wider confrontation between the West and authoritarian powers.

These attacks, often hybrid as they are accompanied by disinformation campaigns, currently constitute the most important threat to CI in the EU and candidate countries. The type of actual attacks varies from cyber-attacks and sabotage against EU member states to military aggression and physical destruction against Ukraine. This has important implications for the policies of protecting CI and increasing its resilience in the EU and candidate countries.

The most important lessons include, first, the need for close and transparent partnerships between different actors within countries – CI operators, regulators, intelligence and defence authorities, civic society and media. Rules and procedures of conduct, for example, for monitoring suspicious cyber activities to minimise risks and increase robustness of CI facilities and rapidity in restoring their functions in case of shocks are important as well as regular organisational exercises aiming for agility and flexibility in the face of changing technologies used. Trust based networks including all stakeholders of CI ecosystems are important for the stronger protection, in particular, faster recovery from shocks to the provision of vital services which is particularly important for strengthening resilience of CI.

High risks originating from ongoing war against Ukraine as well as competing needs for public and private investments in other candidate countries complicate their efforts at upgrading CI facilities and improving their resilience. Agile cooperation can sometimes substitute the lack of resources and insufficient capabilities which often require substantial investments and redundancies.

However, the state of war that Ukraine has been in because of unprovoked aggression by Russia, complicates systematic practicing of private and public partnerships. High political polarisation, as it is the case in Georgia, also complicates partnerships of different stakeholders and reduces trust of society in official authorities and their policies. Without addressing these broader geopolitical and domestic tensions, policies aimed at improving protection and resilience of CI in candidate countries are likely to be of limited effectiveness. Ultimately deterrence from actual attacks by imposing significant costs on hostile actors is an effective form of protection but it requires such capacities that most European countries lack. Therefore more attention should be given to strengthening resilience, in

particular, fast recovery from incidents or attacks, and diversification of energy and other infrastructure connections to reduce vulnerabilities from being weaponized by authoritarian powers. Again, examples of Baltic States redirecting their energy and transport connections from Russia to the Northern and Central European countries as well as Ukraine's energy integration could be seen as good practice examples how to reduce vulnerability of CI to external risks.

Another important observation is that connectivity patterns and ongoing processes of integration require intense cooperation between countries to manage risks related to cross-border activities, including those that affect functioning of CI. Therefore cooperation between sub-regional groups like Baltic States, Baltic Sea Region states or Western Balkan countries, also within the EU and NATO formats is important. It includes timely cross-border sharing of intelligence, pooled expertise and other resources, joint exercises contributing to better preparedness for potential incidents and for restoring the vital functions to society and state.

While these are well-known factors which strengthen the resilience of CI they need to be regularly practiced. Joint exercises in preventing cyber risks, such as conducting stress tests and regular cyber training for responsible structures, testing technologies and equipment under near-critical conditions with EU and NATO partners are important. Besides, more systemic formats of cooperation between the EU and its candidate countries could be developed to facilitate such practices, for example, by jointly reacting to particular external shocks and drawing lessons for improving the resilience of CI entities.

Bibliography/List of References

Aho, A., Alonso Villota, M., Giannopoulos, G., Jungwirth, R., Lebrun, M., Savolainen, J., Smith, H., & Willkomm, E. (2023). Hybrid Threats: A Comprehensive Resilience Ecosystem. European Centre of Excellence for Countering Hybrid Threats & European Commission Joint Research Centre. Available at: https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/ (last accessed: 13.02.2025).

Atlantic Council: Russian Cyber Strategy and the War Against Georgia. Available at: https://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia/ (last accessed: 13.02.2025).

BBC: Georgia's PM hits back as protests and resignations intensify, December 2, 2024. Available at: https://www.bbc.com/news/articles/cp87881918wo (last accessed: 13.02.2025).

BBC, Ukraine mobile network Kyivstar hit by 'cyber-attack' available at: https://www.bbc.com/news/world-europe-67691222 (last accessed 05.02.25)

BBC: How a cyber attack transformed Estonia, 27 April 2017, available at https://www.bbc.com/news/39655415 (last accessed 09.02.2025)

Bernhard Hammerli/Andrea Renda: Protecting Critical Infrastructure in the EU, CEPS Task Force Report, Centre for European Policy Studies, 2010, p. 1.

BNS 2008. "Internet Invaders Paralyzed more than 300 Lithuanian Websites," June 30.

Bryant, M. (2024) 'We assume damage to Baltic Sea cables was sabotage, German minister says', Guardian, 19 November. https://www.theguardian.com/world/2024/nov/19/baltic-sea-cables-damage-sabotage-german-minister.

CBAP: The Changing Face of Cybersecurity in the Baltics and Finland, 03 May 2023, available at https://cbap.cz/archiv/5299 (last accessed 09.02.2025)

Center for European Policy Analysis: Chinese Influence in Montenegro', 2022, August, available at: https://cepa.org/comprehensive-reports/chinese-influence-in-montenegro/ (last accessed 25.01.2025)

CERT-UA recorded 4,315 cyber incidents in 2024, available at: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (last accessed 05.02.25)

CERT.LV: 2022. gads Latvijas kibertelpā, available at: https://www.cert.lv/lv/2023/01/2022-gads-latvijas-kibertelpa (last accessed 10.02.2025)

CERT.LV: 2023. gads Latvijas kibertelpā, January 2024, available at: https://cert.lv/lv/2024/03/2023-gads-latvijas-kibertelpa (last accessed 10.02.2025)

CERT.LV: Publiskais pārskats par CERT.LV uzdevumu izpildi, January 2016, p.11, available at: https://www.cert.lv/uploads/parskati/CERT.LV_gada_parskats_2015.publ.pdf (last accessed 10.05.2025
Christer Pursiainen: The Crisis Management Cycle, Routledge, 2017, cited in 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

Civic IDEA: Anaklia Port – Another Step in Shifting Foreign Policy, May 2024. Available at: https://civicidea.ge/wp-content/uploads/2024/05/ANAKLIA-PORT-ANOTHER-STEP-IN-SHIFTING-FOREIGN-POLICY.pdf (last accessed: 13.02.2025).

Civil Georgia: Bloomberg: Russia Hacked Entire Georgia Between 2017-2020, October 21, 2024. Available at: https://civil.ge/archives/629367 (last accessed: 13.02.2025).

Civil Georgia: ENKA 'Finally' Terminates Namakhvani HPP Contract, March 24, 2022. Available at: https://civil.ge/archives/481355 (last accessed: 13.02.2025).

Clayton, M. (2021, June 10). [Title of the Post]. X. Available at: https://x.com/MarkClaytonFCDO/status/1403286833644150784 (last accessed: 13.02.2025).

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 (text with relevance to EEA), available at https://eur-lex.europa.eu/eli/dir/2008/114/oj/eng (last accessed: 10.01.2025).

Council of the European Union: Conclusions on EU Security and Defence, May 27, 2024.

CSIS: Russia aims at Montenegro: Cyberattacks and Geopolitics. Center for Strategic and International Studies, February 2023, available at: https://www.csis.org/analysis/russia-aims-montenegro (last accessed 21.01.2025)

Daryna Antoniuk, Russian hackers target 20 energy facilities in Ukraine amid missile strikes, The Record, available at: https://therecord.media/russian-hackers-target-energy-facilities-ukraine (last accessed 05.02.25)

Decree of the President of Ukraine dated August 26, 2021 No. 447 "On approval of Cybersecurity Strategy of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (last accessed 05.02.25)

DELFI.LV: Количество помех в работе спутниковой системы навигации в воздушном пространстве Латвии увеличилось в пять раз, 06 February 2025, available at: https://rus.delfi.lv/57860/latvia/120060243/kolichestvo-pomeh-v-rabote-sputnikovoy-sistemy-navigacii-v-vozdushnom-prostranstve-latvii-uvelichilos-v-pyat-raz (last accessed 10.02.2025)

Diehl, J. et al. (2024) 'So entwischte der mutmaßliche Nord-Stream-Sprenger der Polizei', Der Spiegel 29 August. https://archive.ph/20240829120157/https://www.spiegel.de/politik/nord-stream-anschlag-wie-der-mutmassliche-pipeline-sprenger-der-polizei-entwischte-a-ecc235ff-2703-483e-bf19-c47badd28918#selection-877.0-877.62.

Dudzinska, K. (2025) 'Acute Need for Security of Critical Infrastructure in the Baltic Sea Region', PISM Bulletin 5, 16 January. https://www.pism.pl/publications/acute-need-for-security-of-critical-infrastructure-in-the-baltic-sea-region.

DW (2025) 'Latvia: Undersea cable likely damaged by external influence', 27 January. https://www.dw.com/en/latvia-sweden-cable-damage-nato/a-71416470.

DW (2025) 'NATO unveils Baltic Sentry pipeline, cable security mission', 14 January. https://www.dw.com/en/nato-unveils-baltic-sentry-pipeline-cable-security-mission/a-71292043.

e Ministry of National Defence of the Republic of Lithuania: Key Trends And Statistics Of The National Cyber Security Status Of Lithuania 2022, 01 June 2023, available at: https://www.nksc.lt/doc/en/2022_key-trends-and-statistics-of-cyber-security.pdf (last accessed 10.02.2025)

Energy Ministry of Ukraine: The Russian gas transportation has stopped, available at: https://mev.gov.ua/novyna/tranzyt-rosiyskoho-hazu-zupyneno (last accessed 05.02.25)

Entous, A., J. Barnes and A. Goldman (2023) 'Intelligence Suggests Pro-Ukrainian Group Sabotaged Pipelines, U.S. Officials Say'. New York Times, 7 March. https://www.nytimes.com/2023/03/07/us/politics/nord-stream-pipeline-sabotage-ukraine.html.

Eric Stern/Brian Nussbaum: Critical Infrastructure Disruption and Crisis Management, Oxford Research Encyclopedia of Politics, 2022.

ERR.EE: Pro-Kremlin cybercriminals attack Eesti Energia, 19 Nov. 2022, available at: https://rus.err.ee/1608794218/prokremlevskie-kiberprestupniki-atakovali-eesti-energia (last accessed 10.02.2025)

European Comission: Eiropas Savienība un NATO rīko pirmo strukturēto dialogu par kiberjautājumiem, 04 October 2024, available at: https://digital-strategy.ec.europa.eu/lv/news/european-union-and-nato-hold-first-structured-dialogue-cyber (last accessed 10.02.2025)

European Commission: Critical infrastructure resilience at EU-level, 23 September 2024, available at https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en (last accessed 10.01.2025).

European Commission: European Reference Network for Critical Infrastructure Protection: ERNCIP Handbook 2018 edition, Joint Research Centre Technical report, 2018, and European Commission activities on Critical Infrastructure Protection in the EU Science Hub, available at https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en (last accessed 10.01.2025).

European External Action Service: Assessment of Cybersecurity Risks in Montenegro: Challenges and Recommendations'. EU Publications, October, 2023, available at: https://www.eeas.europa.eu/sites/default/files/documents/2024/Montenegro%20Report%202024.pdf (last accessed 25.01.2025)

European Parliament: Foreign Direct Investment Screening in the EU and its Impact on Critical Infrastructure Protection, July, 2021, available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762844/EPRS_BRI(2024)762844_EN.pdf (last accessed 21.01.2025)

European Parliament: Montenegro's NATO accession and Russian influence in the Balkans, April 2021, available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/747096/EPRS_BRI%282023%29747096_EN.pdf (last accessed 21.01.2025)

Foreign Policy Research Institute (FPRI): Hess, M., & Otarashvili, M. (2020). Georgia's Doomed Deep-Sea Port Ambitions: Geopolitics of the Cancelled Anaklia Project. Available at: https://www.fpri.org/wp-content/uploads/2020/10/georgias-doomed-deep-sea-port-ambitions.pdf (last accessed: 13.02.2025).

Gennadiy Riabtsev, Volodymyr Omelchenko, Overview of the Energy Market Operation in December 2024, available at: https://razumkov.org.ua/images/2025/01/21/2025-PAKT-ENERGY-2.pdf (last accessed 07.01.25)

Government of Georgia: Decree of the Government of Georgia N2033, October 31, 2018. Available at: https://www.gov.ge/files/495_68573_326517_2033.pdf (last accessed: 13.02.2025).

Government of Georgia: Decree On Approval of the List of Entities Containing High Risks to National Security, December 23, 2015. Available at: https://matsne.gov.ge/ka/document/view/3056223?publication=0 (last accessed: 13.02.2025).

Government of Georgia: On the Approval of the List of Strategic and/or Specially Important Facilities, October 23, 2024. Available at: https://www.matsne.gov.ge/ka/document/view/6296025?publication=0 (last accessed: 13.02.2025).

Government of Georgia: Ordinance No. 646: On the Approval of the List of Critical Information System Subjects of the First, Second, and Third Categories, December 31, 2021. Available at: https://matsne.gov.ge/document/view/5346058?publication=0 (last accessed: 13.02.2025).

Hannah Brandt/Funda Tekin/ Pol Bargues, Ramūnas Vilpišauskas: Growing Resilient Together: Reshaping EU Enlargement and Neighbourhood Policy in a Geopolitical Era, InvigoratEU Conceptual Background Paper, 2024, available at https://invigorat.eu/invigorateu-publications/ (last accessed 11.01.2025).

Helsingin Sanomat (2025) 'Eagle S -tutkinnassa ei ole löytynyt näyttöä kaapeli¬rikon tahallisuudesta – Supo ei usko Venäjän osallisuuteen', 21 January. https://www.hs.fi/tutkiva/art-2000010979641.html.

Hersh, S. (2023) 'How America Took Out The Nord Stream Pipeline', 8 February. https://seymourhersh.substack.com/p/how-america-took-out-the-nord-stream.

Igor Piddubnyi, Dmytro Goriunov, Assessment of damages and losses to Ukraine's energy sector due to Russia's full scale invasion, May 2024, p16, available at: https://kse.ua/about-the-school/news/damages-and-losses-to-ukraine-s-energy-sector-due-to-russia-s-full-scale-invasion-exceeded-56-billion-kse-institute-estimate-as-of-may-2024/

Jon Coaffee: Future Proof. How to Build Resilience in an Uncertain World, 2019
Latvian Institute of International Affairs : Commonalities, Risks and Lessons for Small Democracies: Hybrid Threats in Baltics and Taiwan, 2022, p. 59, available online: https://www.liia.lv/en/publications/hybrid-threats-in-baltics-and-taiwan-commonalities-risks-and-lessons-for-small-democracies-954?get_file=1 (last access 10.02.2025)

Latvija Avīze: Dezinformatori Igaunijā rada paniku par atslēgšanos no Krievijas energotīkla; kritiskā infrastruktūra tiek apsargāta, 06 February 2025, available at: https://www.la.lv/dezinformatori-igaunija-radijusi-tik-lielu-paniku-par-atslegsanos-no-krievijas-energotikla-ka-cilveki-izperk-generatorus (last accessed 10.02.2025)

Latvijas Republikas Satversmes Aizsardzības Birojs: SAB 2022 Pārskats, January 2023, available at: https://www.sab.gov.lv/files/uploads/2023/07/2022_parskats.pdf (last accessed 10.02.2025)

Latvijas Republikas Satversmes Aizsardzības Birojs: SAB 2023 Gada pārskats, January 2024, available at: https://www.sab.gov.lv/files/uploads/2024/02/SAB-2023.gada-parskats_LV.pdf (last accessed 10.02.2025)

Latvijas Republikas Valsts Drošības Dienests: VDD Publiskais Pārskats 2023, January 2024, available at: https://vdd.gov.lv/uploads/materials/34/lv/vdd-publiskaisparskats-2023-web.pdf (last accessed 10.02.2025)

Lazari, A., & Tabagua, N. (2024). Critical Infrastructure Security and Resilience (CISR) Policy in Georgia: State of Play and Future Prospects. PMC Research Center. Available at: https://pmcg-i.com/app/uploads/2024/04/CISR-Policy-in-Georgia-2024_Final.pdf (last accessed: 13.02.2025).

Lee, M. (2023) 'A global mystery: What's known about Nord Stream explosions'. AP News, 8 March. https://apnews.com/article/us-germany-russia-denmark-ukraine-gas-pipeline-attack-nord-stream-2561f98ba6462db700f7609352a28c24.

LMT: Kiberapdraudējumu līmenis pieaug - uzbrukts vairāk nekā pusei LMT tīklā esošo ierīču, 21 October 2024, available at: https://lmt.lmt.lv/jaunumi/kiberapdraudejumu-limenis-pieaug (last accessed 10.02.2025)

LSM: Krisjanis Kariņš fell for a ruse of Russian pranksters, 14 November 2023, available at: https://rus.lsm.lv/statja/novosti/politika/14.11.2023-krisyanis-karins-popalsya-na-ulovku-prankerov-iz-rf.a531622/ (last accessed 10.02.2025)

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.

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.

Michel Bruneua at el.: A Framework to quantitatively assess and enhance the seismic resilience of communities, 2003, cited in 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, Ministry of Foreign Affairs of the Republic of Estonia: Regional activities, Last updated: 13.01.2022, available at: https://www.vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/regional-activities (last accessed 10.02.2025)
Ministry of Foreign Affairs of Georgia: National Security Concept. Available at: https://mfa.gov.ge/en/national-security-concept (last accessed: 13.02.2025).

Ministry of Internal Affairs of Georgia: Official Statement, February 1, 2025. Available at: https://www.police.ge/en/shinagan-saqmeta-saministros-gantskhadeba/16554 (last accessed: 13.02.2025).

Ministry of National Defence of the Republic of Lithuania: Key Trends and Statistics of The National Cyber Security Status of Lithuania 2022, 1 June 2023, available at: https://www.nksc.lt/doc/en/2022_key-trends-and-statistics-of-cyber-security.pdf (last accessed 10.02.2025)

Ministry of National Defence of the Republic of Lithuania: Lithuanian-coordinated EU Cyber Rapid Response Teams - incident response with the EU and in support of EU partners and military missions, 30 March 2023, available at: https://kam.lt/en/lithuanian-coordinated-

eu-cyber-rapid-response-teams-incident-response-with-the-eu-and-in-support-of-eu-partners-and-military-missions/ (last accessed 10.02.2025)

National Security Council of Georgia: First Session of the Interagency Commission on the Development of the National Security Strategy, news article. Available at: https://nsc.gov.ge/en/NEWS/first-session-of-the-inter-age.html (last accessed: 13.02.2025).

NATO Strategic Communications Centre of Excellence: 2007 cyber-attacks on Estonia, May 2007, available at https://stratcomcoe.org/publications/download/cyber_attacks_estonia.pdf (last access 09.02.2025)

NATO-EU Task Force on the Resilience of Critical Infrastructure: Final Assessment Report, June 2023.

OECD: Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies, OECD Publishing, 2019,

On critical assessment of EU's Hybrid Toolbox see Kenneth Lasoen: Realising the EU Hybrid Toolbox: opportunities and pitfalls, Clingendael Policy Brief, December 2022.

Parliament of Georgia: Criminal Code of Georgia, October 23, 2024. Available at: https://matsne.gov.ge/document/view/16426?publication=269 (last accessed: 13.02.2025).

Parliament of Georgia: Law on Information Security, June 5, 2012. Available at: https://matsne.gov.ge/document/view/1679424?publication=7 (last accessed: 13.02.2025).

Parliament of Georgia: Law on the State Security Service of Georgia, July 8, 2015. Available at: https://matsne.gov.ge/en/document/view/2905260?publication=1 (last accessed: 13.02.2025).

Political Violence at a Glance: Who Attacked Montenegro? The Moral and Strategic Hazards of Misassigning Blame, September, 2022, available at: https://politicalviolenceataglance.org/2022/09/21/who-attacked-montenegro-the-moral-and-strategic-hazards-of-misassigning-blame/ (last accessed 25.01.2025)

President's Order of December 19, 2023 No. 1163-r "On approval of the action plan for 2023-2024 for the implementation of the Cybersecurity Strategy of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/1163-2023-p#Text (last accessed 05.02.25)

Radio Free Europe/Radio Liberty: The Black Sea Port That Could Define Georgia's Geopolitical Future, August 14, 2023. Available at: https://www.rferl.org/a/georgia-anaklia-port-geopolitics-russia-chna-eu/32547539.html (last accessed: 13.02.2025).

RAI EE: Cyber Security in Estonia 2023, January 2024, available at% https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf (last accessed 10.02.2025)

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.

REPowerEU, European Commission, available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/repowereu-affordable-secure-and-sustainable-energy-europe_en, (last accessed 05.02.25)

Resolution of the National Energy and Utilities Regulatory Commission (NEURC) No. 349 dated March 26, 2022

RIA.EE, Cyber Security in Estonia 2024, January 2025, available at: https://www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf (last accessed 10.02.2025)

RIA.EE: Cyber Security in Estonia 2023, p.10, January 2024, available at: https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf (last accessed 10.02.2025)

Roberto Setola et al. (eds.) Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, 2016.

Roberto Setola/Eric Luiijf/Marianthi Theocharidou: Critical Infrastructures, Protection and Resilience, 2016.
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,

SARGS.LV: Aizsardzības ministrija, NBS un LMT kopā ar NATO plāno unikālu digitālās savienojamības eksperimentu, 05 September 2024, available at: https://www.sargs.lv/lv/nozares-politika/2024-09-05/aizsardzibas-ministrija-nbs-un-lmt-kopa-ar-nato-plano-unikalu-digitalas (last accessed 10.02.2025)

Tim Prior: Measuring Critical Infrastructure Resilience: Possible Indicators, Risk and Resilience Report 9, Centre for Security Studies (CSS), ETH Zurich, 2014, p. 5.

Ukraine's Cabinet of Minister's Resolution No 1482 dated 27 December 2022, available at: https://zakon.rada.gov.ua/laws/show/1482-2022-п#Text (last accessed 07.02.25)

Ukraine's Energy Security and Coming Winter, An energy action plan for Ukraine and its partners, EAI, September 2024, available at: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter (last accessed 11.11.24

Ulrich Beck: Risk Society: Towards a New Modernity, published in German in 1986 and translated into English in 1992 by Sage Publications. For more recent studies see Jon Coaffee: Future Proof. How to Build Resilience in an Uncertain World, Yale University Press, 2019; Markus K. Brunnermeier: The Resilient Society, Endeavor Literary Press, 2021.

Westinghouse VVER-440 fuel loaded into reactor, 11 September 2023, World Nuclear News, available at: https://world-nuclear-news.org/Articles/Westinghouse-VVER-440-fuel-loaded-into-reactor (last accessed 13.02.25)

World bank Group, Updated Ukraine Recovery and Reconstruction Needs Assessment Released, Press release, February 15, 2024, available at: https://www.worldbank.org/en/news/press-release/2024/02/15/updated-ukraine-recovery-and-reconstruction-needs-assessment-released (last accessed 11.11.24)

World Bank: Montenegro Country Climate and Development Report, December 2024, available at: https://www.worldbank.org/en/country/montenegro/publication/montenegro-country-climate-and-development-report (last accessed 22.01.2025)

Yle News (2024) 'Baltic gas pipeline ruptured by Chinese ship back in service after €40m repair job', 22 April. https://yle.fi/a/74-20084948.

Yle News (2024) 'Estlink cable disruption: Finnish Border Guard detains tanker linked to Russia's 'dark fleet'', 26 December. https://yle.fi/a/74-20133516.

Interviews:

Interview with a former senior official of the Government of Lithuania (2020-2024), February 8, 2025, Vilnius;
Interview with the Ministry of Interior's officials, October 17, 2024, via Zoom;
Interview with the official from the Department for Critical infrastructure, Ministry of Interior, February 10, 2025, Podgorica;
Exploratory interview with Cyber Security Expert Giorgi Iashvili, December 20, 2024, Tbilisi;
Exploratory interview with Security Policy Expert Shalva Khutsishvili, January 30, 2025, Tbilisi.

Appendix 1

Overview of the legislation in Ukraine CI Protection

Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, November). Retrieved from https://zakon.rada.gov.ua/laws/show/1882- 20#Text.

Resolution of the Cabinet of Ministers of Ukraine dated November 12, 2022 No. 787 "On the Establishment of the State Service for Critical Infrastructure Protection and Ensuring the National Resilience System of Ukraine."

Resolution of the Cabinet of Ministers of Ukraine No. 1109 dated October 9, 2020, "Some issues of critical infrastructure facilities"

Decree of the President of Ukraine No. 722/2019 "On Sustainable Development Goals of Ukraine for the period until 2030". (2019, September).

Law of Ukraine No. 2163-VIII "On the Fundamental Principles of Ensuring Cyber Security of Ukraine". (2017, October).

Law of Ukraine No. 2469-VIII "On National Security of Ukraine". (2018, June).

Decree of the President of Ukraine No. n0014525-16 "On Improving Measures to Ensure the Protection of Critical Infrastructure Objects". (2016, December). Retrieved from https://zakon.rada.gov.ua/laws/show/n0014525-16#Text.

The decision of the National Security and Defence Council of Ukraine No. n0001525-17 "On Urgent Measures to Neutralize Threats to the Energy Security of Ukraine and Strengthening the Protection of Critical Infrastructure". (2017, January). Retrieved from https://zakon.rada. gov.ua/laws/show/n0001525-17#Text.

Resolution of the Cabinet of Ministers of Ukraine No. 1109-2020-п "On Some Issues of Objects of Critical Infrastructure". (2020, October). Retrieved from https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

Resolution of the Cabinet of Ministers of Ukraine No. 563 "On the Approval of the Procedure for the Formation of the List of Information and Telecommunication Systems of Objects of Critical Infrastructure of the State". (2016, August). Retrieved from https://zakon.rada.gov.ua/ laws/show/563-2016-%D0%BF#Text. https://zakon.rada.gov.ua/laws/show/n0001525-17#Text.

Law of Ukraine No. 2163-VIII "About the Main Principles of Ensuring Cyber Security of Ukraine". (2017, October). Retrieved from https:// zakon.rada.gov.ua/laws/show/2163-19#Text.

Decree of the President of Ukraine No. 392/2020 "On the Decision of the National Security and Defense Council of Ukraine "On the National Security Strategy of Ukraine". (2020, September). Retrieved from https://zakon.rada.gov.ua/laws/show/392/2020#Text.

Law of Ukraine No. 1882-IX "On Critical Infrastructure". (2021, November). Retrieved from https://zakon.rada.gov.ua/laws/show/1882- 20#Text

Appendix 2

Hydrogen projects in Ukraine

Green hydrogen can help transform energy sector, industry, and transport to achieve sustainability and climate neutrality. Ukraine has high potential for RES development, water resources, as well as human and educational potential.

Ukraine, along with relevant transit countries, possesses well-established infrastructure, including pipelines and seaports, for exporting hydrogen and Power-to-X products to Western Europe. However, further investigations are needed to repurpose this infrastructure effectively.

The European Union (EU) is considering Ukraine as a potential hydrogen supplier, aiming to meet European energy demand, and supporting Ukraine's recovery from the Russian invasion.

EU has called Ukraine as a "priority partner" in its hydrogen strategy[149] published in 2020. Several companies in Ukraine have become members of European Clean Hydrogen Alliance.

Under the 2x40 GW initiative of Green Hydrogen for a European Green Deal Ukraine was included as neighbouring country for the development of a hydrogen economy with a dedicated 10 GW electrolyser capacity of which 2.5GW are intended for domestic hydrogen use mostly for ammonia production and 7.5 GW for export capacity.

Before the war broke out there were a lot of activities in Ukraine: a few memoranda and international agreements were signed on both governmental and business level, the national Hydrogen Strategy[150] was drafted. Hydrogen remains a weak case for Ukraine, however, before the war several projects have been identified (Table 1.)

Table 1. Perspective hydrogen projects in Ukraine before the Russian invasion

No	Company - developer	Project	Brief description	Investment
1	Regional Gas Company (RGC)	**RGC-hydrogen project**, (started in August 2020)	Substitute natural gas by hydrogen in Ukrainian gas distribution system. The company has started the trial of its own gas equipment: preparing 20% hydrogen mix and testing the equipment to be followed by testing the equipment with 50% hydrogen mix. Over 90 experiments have demonstrated that the national gas distribution system is capable to tolerate 20% hydrogen but needs to be redesigned.	$ 12,5 bln
2	Hydrogen Ukraine,	H2EU	Construction of renewable hydrogen plant in the Odesa region (port Reni[151] for the domestic consumption and exports to EU. The planned capacity of the first stage of green hydrogen plant is 100MW with production of 8 thousand tonnes hydrogen per year and the capacity can be further increased to 3GW in the coming years.	$400 mln
3	Eco -Optima.	H2EU+Store	Construction of green hydrogen plant to export it to Austria and Germany. It is envisaged to build 100 MW electrolysis plant in Sambir district of Lviv region. Eco-Optima possesses 4 wind and 7 solar facilities in Lviv region and one PV in Ivano-Frankivsk region of total capacity 154 MW	$320 mln

[149] Hydrogen, https://energy.ec.europa.eu/topics/energy-systems-integration/hydrogen_en
[150] Hydrogen Strategy of Ukraine, https://www.ive.org.ua/wp-content/uploads/ENG-Hydro-Beauty-final.pdf
[151] The location chosen for the hydrogen plant is a strategic one not only because of the enormous wind potential (ranging from 1.5 to 4 GW) and solar potential (with average solar radiation of 1,600 (kW/m2) but also from a logistic point of view, due to a very-well developed transport infrastructure. It can also count on significant water resources with an average annual water flow of the Danube River of 6,400 cubic metres per second. Finally, the developed transport infrastructure of Reni's port makes it possible to transport the produced hydrogen to 10 countries in the Danube region.

4	H2Drive (founded in 2021)	**H2Drive**	Development of electrical and hydrogen charging stations network. It was planned to build 23 innovation charging stations in Kyiv, Kharkiv, Dnipro, Odesa, Lviv. The first pilot hydrogen filling station had to be launched in Kyiv in 3Q 2022.	$50 mln
5	Danube Hydrogen Valley Coordinator: Energy Ministry	**Danube Hydrogen Valley**	Construction of a renewable hydrogen production plant "Danube Hydrogen Valley" Electrolyses capacity: 3000 MW I. Stage - 50 MW (H2- 65 mln Nm^3/year) II.Stage - 150 MW (H2 -195 mln Nm^3/year) III stage - 300 MW (H2 - 390 mln Nm3 per year IV stage - 2 500 MW (H2 -2,2 bln Nm^3/year Capacity of green stations for power supply of electrolysers 5000 MW including: 3000 MW of wind power station 2000 MW of solar power station	EUR 100 mln (first stage)
6	DTEK LLC - Public Private Partnership with German and Ukrainian industrial stakeholders Coordinator - Energy Ministry	**Green hydrogen industrial cluster - 5 MW pilot project**	Electrolyser capacity for pilot project: 5 MW,150 - 550 tons of H2 per year depending on the electrolyser capacity load. Electrolyser capacity potential: 200 MW, 6 000 - 22 000 tons of H2 per year depending on the electrolyser capacity load. 2 000 MW capacity of green energy supply for H2 production with electrolysers through certificates of origin scheme, including existing 450 MW solar and 500 MW wind energy clusters.	EUR 12-14 mln
6	GEOTHERMIKA LLC Coordinator: Energy Ministry	**Construction of a renewable hydrogen production plant in Trans Carpathian region of Ukraine**	1.Solar power plants: up to 100 MW 2. Electrolysers: up to 30 MW 3. H2 compressors (Germany) 4. H2 storage and filling system of automobile carriers of hydrogen. 5. Water pumps and filters 6. Storage of electricity up to 30 MW (lithium-ion batteries, or vanadium flow batteries) 7. Backup power 8. Guard of territory. 9. Water capacity V = max. on the territory to provide electrolysers up to 30 MW (available in the location).	EUR 130mln
7	Nyzhnodnistrovska HPP, PJSC	**Green hydrogen production from hydropower**	1. HPP capacity is 40.8 MW (possibility to install equipment for "green" hydrogen production) 2. Plots of land on which the installation of solar and wind power plants is planned: 1st - 10 hectares: 8 MW capacity SPP. 10 MW capacity WPP. 2nd - 12 hectares:10 MW capacity SPP (3 MW capacity SPP was in operation) 3d - 5.56 hectares: 4MW capacity SPP 4th - 20,863 hectares (15 MW SPP).	EUR 14 mln

Several cross-border hydrogen projects involving Ukraine and EU countries have been announced. These include:

- **The Green Hydrogen e Blue Danube scheme**, which envisages hydrogen production and transport along the river, with imports to Germany. The project targets the

large-scale production of green hydrogen in Southeastern Europe and its subsequent transport via LOHC and ships to industrial offtakers along the Danube River. The Green Hydrogen @ Blue Danube project is being implemented by Verbund, Austria's largest renewable electricity producer, for the production, transportation, and use of green hydrogen by industrial consumers and in the mobility sector and has received EU support under a pan-European program IPCEI (Important Projects of Joint European Interest).

Source: https://hydrogen.ua/en/news/1281-blue-danube-an-opportunity-to-develop-the-hydrogen-economy-in-ukraine

- **The Central European Hydrogen Corridor (CEHC)**, which would send hydrogen from Ukraine to Germany by dedicated pipelines via Slovakia and the Czech Republic. The Central European Hydrogen Corridor (CEHC) initiative was launched in 2021 by four gas infrastructure companies (OGE, NET4GAS, Eustream, Gas TSO of Ukraine) driven by the vision to develop a hydrogen "highway" through Central Europe. The initiative explores the feasibility of creating a hydrogen pipeline corridor in Central Europe for transporting hydrogen from major hydrogen supply areas in Ukraine via Slovakia and the Czech Republic to hydrogen demand areas in Germany. The hydrogen corridor will also enable the transport of hydrogen between hydrogen production facilities and hydrogen consumers in the Czech Republic and Slovakia.

https://www.cehc.eu/cehc-project/

Challenges for the hydrogen projects in Ukraine.

- **Russian invasion** of Ukraine that has caused enormous damage to the infrastructure and operations. Energy infrastructures and land suitable for renewable energy sources (RES) deployment are currently occupied by the russian military.
- **Cost of hydrogen**. To support the development of hydrogen, the world's leading countries provide legal and financial support the hydrogen production. It is important to create the support instruments and tax incentives and other types of support.
- **Legislation**. Ukraine needs to align legislation with EU-standards regulating the production, consumption, storage, and transportation of hydrogen. European standards should be adopted to facilitate hydrogen exports to the EU, ensuring compliance and seamless integration into European markets.
- **Investment risks**. The existing threats related to the ongoing war's uncertain duration and outcome increase investment risks in developing Ukraine's large RES potential.
- **Water scarcity** (especially in the Southern regions) due to its usage in the agricultural sector may limit large-scale hydrogen production in Ukraine, potentially leading to higher energy costs for households.
- **Introduction by EU of Carbon Border Adjustment mechanism (CBAM)** would become a significant barrier for Ukraine carbon intense industries

exports to EU potentially reducing the margins up to 40% for industries as steel, cement, fertilizer production. Ukrainian steel production is 80% for export, making decarbonisation of local steel production a top priority.

To rehabilitate the energy sector and the economy of the country it is feasible to rely on the green transition also including hydrogen technologies.

- Together with representatives from Europe's hydrogen and energy sectors, a proposed 10-point plan[152], the Timmermans Recovery Plan, has been devised to guide the rebuilding of Ukraine with a focus on its renewables and nuclear potential, as well as its ability to become a major actor in the hydrogen space.
- Memorandum[153] of understanding between the EU and Ukraine on Strategic Partnership on Biomethane, Hydrogen and other Synthetic Gases to launch a strategic partnership on renewable gases.

Ukrainian Hydrogen Council. The association is the main stakeholder among those interested in the development of the Ukrainian hydrogen sector and performs the mission of ensuring interaction between Ukrainian and European partners.

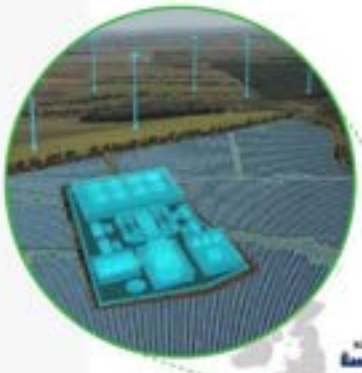
Ukraine has appeared on the global hydrogen valley platform[154] which includes 23 European countries. It is funded by the European Commission with the aim of developing a new hydrogen economy and transitioning to green energy. It contains information about the most developed and ambitious hydrogen valleys around the world.

[152] 10-point Timmermans Recovery Plan, available at:https://hydrogeneurope.eu/wp-content/uploads/2023/01/Timmermans-Recovery-Plan-for-Ukraine2-003.pdf (last accessed 11.12.24)
[153] Memorandum of understanding between the European Union and Ukraine on Strategic Partnership on Biomethane, Hydrogen and other Synthetic Gases, available at: https://energy.ec.europa.eu/system/files/2023-04/MoU_UA_signed.pdf (last accessed 11.12.24)
[154] Mission Innovation Hydrogen Valley Platform, available at: https://h2v.eu/ (last accessed 11.12.24)

H2U Hydrogen Valley in Odesa Region, Ukraine

Electrolyser capacity: 100MW
Solar: 120MW
Wind: 80MW
Period of construction: 24 months

Project name	H2U Hydrogen Valley
Lead developer	Hydrogen Ukraine LLC
Location	Reni, Odesa region, Ukraine
Description	Constructing a renewable hydrogen plant aiming for an initial electrolysis capacity of 100 MW, dedicated to producing renewable electricity and green hydrogen for export to EU countries.
Advantages	Abundant water resources, optimal PV and wind power configuration H2 production is strategically located near the EU border
Challenges	Despite challenges due to the Russian invasion, H2U continues to advance the project and contribute to Ukraine's hydrogen energy strategy



The focus of the EU and most countries on the development of green hydrogen, and considering the natural potential of Ukraine's RES, has prompted Ukrainian researchers to focus on green hydrogen. The use of grey hydrogen produced by use of fossil fuels or pink - produced by electrolysis of water from electricity from nuclear power plants should be considered exclusively for the transition period, which is aimed to achieve sufficient green hydrogen production.

Appendix 3

War-risk insurance for investment into Ukraine's reconstruction

The current budget limitations make it impractical to rely solely on guarantees from the Ukrainian government. Therefore, the Ukrainian Government is inviting foreign governments to collaborate on the establishment of a specialized program to insure against war-related risks for both domestic and foreign investors. These insurance products should be more widely accessible through refinancing and reinsurance funds, with favourable terms for risk coverage.

Several initiatives regarding new partnership towards war-risk insurance for investment into Ukraine's reconstruction and international trade were launched during the Ukraine Recovery Conference in London[155]:

[155] Ukraine Recovery Conference, 21-22 June 2023, London, UK, available at https://www.urc-international.com/ (last accessed 11.12.24)

- The European Commission has introduced a new initiative called the **'Ukraine Facility'**[156], to offer war risk insurance for Ukraine. This innovative program is intended to address both immediate recovery requirements and the longer-term reconstruction and modernization needs of Ukraine. The Facility is designed to be adaptable, considering the unique challenges of supporting a nation at war, while also prioritizing the transparency, predictability, and accountability of funds. The Facility, if adopted by the European Parliament and Council of the EU, will mobilise up to €50 billion over four years in the form of both grants and loans. This proposal acknowledges the potential for a protracted conflict and the ongoing necessity for macro-financial assistance.
- **War Insurance Pilot Scheme** – Ukraine Recovery and Reconstruction Guarantee: The European Commission has shown an interest in backing an inventive pilot program by the EBRD, contemplating the utilization of its guarantee funds. This program's objective is to address market deficiencies, making it easier for both Ukrainian and international companies to obtain war insurance. The guarantees will serve the dual purpose of safeguarding forthcoming private investments and providing insurance coverage for international shipping and trade against the risks associated with armed conflict.
- **Multi-agency Donor Coordination Platform for Ukraine**[157] oversees the coordination of funding to meet Ukraine's immediate financial requirements and address its future needs for economic recovery and reconstruction, utilizing a range of funding sources and established financial instruments. Launched on January 26, 2023, with its inaugural Steering Committee meeting, this initiative unites senior officials from Ukraine, the EU, G7 nations, and partners from international financial institutions.

Initiatives on investment insurance from Ukraine's partners

Within the new framework for war risk insurance initiated during the London conference, partners announced their support for the Support for Ukraine's Reconstruction and Economy (SURE) Trust Fund of the World Bank's Multilateral Investment Guarantee Agency (MIGA), with a total guarantee of € 40.85 million. The European Bank for Reconstruction and Development (EBRD) also expressed its intention to develop a pilot scheme for insurance against war risks. Moreover, according to lawmakers, certain countries such as the United Kingdom, Japan, Germany, France, Canada, Australia, Israel, and others have already established special funds for insuring investments in Ukraine.

---

[156] Brussels, 20.6.2023 COM(2023) 338 final 2023/0200 (COD), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing the Ukraine Facility, available at: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-06/COM_2023_338_1_EN_ACT_part1_v6.pdf (last accessed 11.12.24)

[157] Donor Coordination Platform for Ukraine, https://coordinationplatformukraine.com/

- **United Kingdom.** The United Kingdom Export Finance (UKEF), the National Export Credit Agency of the United Kingdom, has recently committed to provide up to £200 million for political and war risk insurance for British investors considering investment opportunities in Ukraine.
  In June 21 Great Britain[158] pledged £20 million ($25 million) to boost access to a World Bank scheme which helps derisk business operations in Ukraine, a move designed to encourage more investment in the country.
- **Germany.** The German Ministry for Economic Affairs offers insurance coverage for its investors through the Investment Guarantee Scheme. This allows German companies to invest in Ukraine without the need to delay their investments until after the war. With this tool, the federal government safeguards German investors from political risks to prevent or compensate for potential losses. Under the terms of the scheme, the German government has appointed the international consulting company "Pricewaterhouse-Coopers" (PwC) to administer the Investment Guarantee Scheme. This scheme covers the following risks: war, expropriation (nationalization), specific acts of terrorism, as well as the risk of contract breach.
- **Poland.** The draft law on investment insurance for Polish companies in Ukraine includes the reinsurance of risks for companies registered in Ukraine with Polish capital. The Polish Export Credit Agency, KUKE, will implement this insurance mechanism for a long-term period (two years or more). They also propose introducing reinsurance for cargoes transported to Ukraine.
- Similar insurance funds are also being created in other countries. In particular, the Export Credit Agency of France has a limit on credit risk insurance in Ukraine in the amount of € 1 billion. Similar projects were launched in Japan.
- **Denmark** created special fund that would insure the investments of Danish residents in Ukraine. This fund[159] launched by the Danish government, amounts of $57 million. The projects of the "Nibulon" company in the Mykolaiv and Kherson regions were insured from it. Also, Danish Government facilitated Carlsberg's investment in its Ukrainian branch. On June 19, the company opened a production line at the Kyiv plant, the investment amounted to UAH 1.5 billion.

Ukraine has agreed with a few players to launch an investment insurance mechanism during hostilities.

[158] UK pledges up to 20 million pounds to help derisk investment in Ukraine https://www.reuters.com/business/uk-pledges-up-20-mln-pounds-help-derisk-investment-ukraine-2023-06-21/
[159] The Danish Government established the Ukraine Fund which has already accumulated 7 billion DKK for 2023, available at: https://denmark.mfa.gov.ua/en/news/danish-government-established-the-ukraine-fund (last accessed 07.11.24)

- **The Multilateral Investment Guarantee Agency (MIGA)**, a division of the World Bank Group, has committed to a pilot project valued at $30 million for Ukraine. Initially, one investment project will be selected to refine the processes of offering guarantees to foreign investors. MIGA already possesses instruments like Political risk Insurance, which includes War risk Insurance as part of its offerings. On September 2023 MIGA issued guarantees to Ukrainian Industrial Property Holding Limited (UIPH) to cover its equity and shareholder loan investments of up to $ 9.6 million into Limited Liability Company "Industrial Park M10[160] in Lviv, Ukraine. The term of the MIGA guarantee is up to 10 years against the risk of War and civil disturbance.
- As political leaders and G7 finance ministers converged on London for the Ukraine Recovery Conference, **Marsh McLennan** has proposed the creation of a vast "war risk pool" to insure the reconstruction work required to rebuild the country's infrastructure and shattered economy. Ukraine has activated a data platform[161], supported by Marsh McLennan, that would allow insurers, investors and governments to analyse war risks in the country. The data platform aggregates comprehensive maps detailing war-related incidents in Ukraine. These incidents are defined as individual events linked to Russian hostilities, encompassing activities such as missile attacks, drone attacks, and shelling, all occurring since the Russian invasion in February 2022.
- The European Bank for Reconstruction and Development (EBRD)[162] has entered into a statement of intent in collaboration with the European Commission, Norway, Switzerland, the TaiwanBusiness - EBRD Technical Cooperation Fund, and Ukraine. The aim is to revitalize the private insurance market in Ukraine through joint efforts with essential market and public-sector participants to establish a guarantee facility. The key challenge lies in offering suitable insurance options for private-sector investors. They will also explore leveraging donor support to re-engage Ukraine domestic insurance and reinsurance industries and their global counterparts, as well as creating a platform for dialogue among key public and private insurance market stakeholders, to identify further areas where cooperation may be possible.
- The Government of Ukraine is also engaged in cooperation with the American Development Finance Corporation (DFC), [163] which provides insurance for war-related risks. The DFC is evaluating several projects within Ukraine. It has endorsed a Memorandum of Understanding, outlining the framework

[160] M10 Industrial Park Ukraine, available at: https://www.miga.org/project/m10-industrial-park-ukraine-0 (last accessed 07.11.24)
[161] Ukraine launches Marsh McLennan-supported war risk data platform, available at: https://www.reinsurancene.ws/ukraine-launches-marsh-mclennan-supported-war-risk-data-platform/(last accessed 07.11.24)
[162] International move to unlock war insurance for Ukraine investments, available at: https://www.ebrd.com/news/2023/international-move-to-unlock-war-insurance-for-ukraine-investments.html (last accessed 07.11.24)
[163] Joint statement on support for Ukraine Investment platform, available at: https://www.dfc.gov/media/press-releases/joint-statement-support-ukraine-investment-platform (last accessed 07.11.24)

for collaboration, particularly in the private sector, in Ukraine. This agreement, officially signed during the Ukraine Recovery Conference in London, follows through on the initial commitment made by the EBRD and the G7's Development Finance Institutions (DFIs) to establish the Ukraine Investment Platform, a commitment initially announced during the G7 meeting in Tokyo. With new participants now coming on board, the total number of participating entities has reached 19.

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.