InvigoratEU

Invigorating Enlargement and Neighbourhood
Policy for a Resilient Europe

Strengthening Critical Infrastructure Resilience in an Era of Hybrid Threats: Challenges, Lessons, and Policy Options for the EU and its Neighbourhood

Authors

Marts Ivaskis, Ramūnas Vilpišauskas, Danijela Jacimovic, Nana Tabagua, Svitlana Chekunova

Contributors

Marco Siddi, Dimitar Bechev, Artur Gruszczak, Julian Plottka, Kai Ole Vorberg

Funded by
the European Union

Executive summary

Strengthening Critical Infrastructure Resilience in an Era of Hybrid Threats: Challenges, Lessons, and Policy Options for the EU and its Neighbourhood.

Europe's critical infrastructure (CI) is facing an increasingly hostile threat environment from a variety of different actors. Russian hybrid operations, sabotage against energy and communications systems, and the vulnerabilities in increasingly interconnected systems highlight the importance of the topic. Recent attacks on European CI such as attacks on undersea cables in the Baltic Sea or incidents such as drone incursions into EU and NATO airspace highlight that protection as an inherent goal is unachievable. Instead, the goal should be to create resilient systems that can absorb and recover from disruptions.

The policy brief identifies two main clusters of challenges: 1) Systemic challenges; and 2) Operational challenges. Systemic challenges stem from divergent threat perceptions, limited awareness of CI related risks, and different levels of hybrid and geopolitical threats. Operational challenges, however, include uneven implementation of the CER and NIS2 Directives, fragmented national CI frameworks, underdeveloped PPPs, limited resources, and a lack of investment in CI resiliency planning.

The policy brief identifies several key lessons, where examined states have found creative or efficient solutions to the challenges previously identified. It is clear the CI resilience depends on early and continuous involvement of CI operators in policy planning, and a strong trust-based information sharing process between different actors. Only through these two aspects is it possible to create workable and efficient national policy frameworks, where CI operators are willing to fully engage. High threat awareness seems to correlate with better resilience practices, as demonstrated by the cases of Finland, the Baltic States, and Ukraine where holistic or whole-of-society approaches form the basis of CI governance. In these systems, there is strong civil-military coordination, as well as regional cooperation models to continuously strengthen systems. Furthermore, experience from the Western Balkans and Eastern Partnership countries shows that institutional fragmentation, weak PPPs, and resource constraints can be mitigated through EU support, regional collaboration, and phased implementation strategies.

Finally, the brief highlights that CI resilience is a EU-level issue. Resilience continues to be a shared vulnerability and a shared opportunity at the same time. 11 different recommendations are presented to different actors. Some of the priorities include harmonising incident reporting across directives; expanding EU-NATO cooperation; supporting candidate countries through technical assistance and capacity building; developing regional early-warning mechanisms; and promoting cross-border risk assessments and joint preparedness exercises.

Authors

Marts Ivaskis
Head of the European Union Programme
Latvian Institute of International Affairs

Ramūnas Vilpišauskas
Professor
Department of International Relations
Vilnius University

Danijela Jacimovic
Professor
Univerzitet Crne Gore

Nana Tabagua
Lead Researcher
PMCG – Research

Svitlana Chekunova
Research Associate
The Razumkov Centre

Contributors

Marco Siddi, Assistant Professor, FIIA
Dimitar Bechev, Senior Fellow, CEF
Artur Gruszczak, Head of the Department of National Security, JU
Julian Plottka, Senior Scientific Senior Project Manager, IEP
Kai Ole Vorberg, IEP Alumnus, IEP

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.18455004

Disclaimer: Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Funded by
the European Union

About the project: www.invigorat.eu

Contents

1 Introduction

The increasing number of incidents of Russian sabotage operations targeting energy and communication networks across Europe, illustrates the strategic vulnerability of systems. At the same time, recent incidents affecting electricity and communications undersea cables in the Baltic sea and unidentified drone incursions into the EU and NATO member states' territories show the need to reinforce both physical protection and resilience of critical infrastructure (CI). Furthermore, the Russian war of aggression in Ukraine has further highlighted the urgency of aligning policies, strengthening connectivity, and enhancing resilience across the EU and its neighbourhood, learning from Ukraine's experience and adjusting policies to changing technologies used by hostile powers.

The concept of 'resilience' has over time replaced 'protection' in European debates on CI. Traditional approaches concerning protection were mainly based on physical safeguards and prevention. However, through the concept of resilience, there is a recognition that no CI can be fully protected from disruptions. Instead, resilience emphasises preparedness, adaptability, and recovery. Resilience should be understood as the capacity of systems to absorb shocks and continue operating with minimal disruption. Part of the rationale in the move away from the previous concept of 'protection' was related to a sober and honest examination of the current threat landscape, and the number of attempted attacks on CI. Furthermore, within EU and NATO frameworks, resilience has become a unifying concept bridging civil, military, and private-sector responsibilities, linking traditional CI protection to notions of hybrid threat deterrence and continuity planning.

This conceptual evolution from 'protection' to 'resilience' is also closely connected to academic and policy debates. Scholars emphasise the growing interconnectedness of infrastructures across borders and sectors, and state that system vulnerabilities, rather than isolated assets, should be at the centre of policy design.[1] This literature also notes persistent weaknesses in public-private cooperation, which is particularly problematic, when much of the CI across Europe is privately owned.[2] Existing academic literature also highlights limited awareness of CI risks among private operators and the general public.[3]

The evolution of the EU's legislative instruments also reflects a similar shift. The EU legislative framework has expanded significantly since the first European Critical Infrastructure Directive.[4] The CER Directive[5] extends the scope of CI policy to eleven sectors and requires Member States to adopt national resilience strategies, conduct regular risk assessments, identify critical entities, and supervise compliance through competent

[1] Julian Plottka & Kai Ole Vorberg: Review of Literature on Critical Infrastructure Protection, Institut für Europäische Politik, Berlin, 2025.

[2] Ibid.

[3] Ibid.

[4] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of Euro¬ pean critical infrastructures and the assessment of the need to improve their protection, OJ L 545, 23.12.2008., p. 75/82.

[5] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, JO L 333, 27.12.2022., pp. 164-198.

authorities. Meanwhile the NIS2 Directive[6] strengthens cybersecurity obligations, enlarges the category of essential and important entities, and introduces multi-stage incident reporting and management accountability requirements. These two directives are complementary, integrating physical and cyber resilience through a shared all-hazards framework and requiring close cooperation between the competent authorities across regulatory domains.

However, there is still an implementation gap and variety of national practices in enforcement of CI-related regulations. Divergent threat and risk perceptions, institutional capacities, and governance approaches to CI protection illustrate the need for a better understanding of incentives and constraints related to CI protection, as well as the importance of increasing cooperation between public authorities, operators of CI and civil society actors.

CI protection also has a potentially increasing role to play in EU enlargement policy. The EU's internal resilience policies intersect with enlargement through two functional logics: 1) the connectivity logic, which links Member States and candidate countries through energy, transport, and digital networks; and 2) the security logic, which presumes that hybrid threats to CI in candidate states can have distinct impact on Member States as well. However, there is still a lack of a coherent, strategic EU approach to CI protection in the neighbourhood.

Against this backdrop, this policy brief aims to synthesize the challenges, lessons learned, and policy recommendations of previous reports concerning rules alignment of protecting CI in interdependent states[7], and common frameworks for CI protection in the EU and its Neighbourhood.[8]

2 Challenges and lessons learned

The analysis distinguishes between strategic and political challenges in tackling CI resilience – awareness of the urgency to strengthen CI resilience and hybrid and geopolitical threats – on the one hand, and operational challenges – challenges that affect the day-to-day governance of CI systems on the other. The chapter on challenges has therefore been split into two corresponding categories: 1) systemic challenges; and 2) operational challenges.

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ L 353, 27.12.2022., p. 80.-152.

[7] Vilpišauskas, Ramūnas, et al: *Invigorating enlargement and neighbourhood policy for a resilient Europe: Long policy report on rules alignment of protecting critical infrastructure in interdependent states* (InvigoratEU Report D7.1), 2025. https://doi.org/10.5281/zenodo.17340020

[8] Vilpišauskas, Ramūnas, et al: *Invigorating enlargement and neighbourhood policy for a resilient Europe: Long policy report on a Common Framework for the Protection of Critical Infrastructure in the EU and its Nieghbourhood*, 2025. . https://doi.org/10.5281/zenodo.17630178.

Political and strategy challenges concerning awareness, hybrid and geopolitical threats, and divergent risk perceptions

Awareness of the urgency to strengthen CI resilience remains limited across parts of the Western Balkans and Eastern Partnership 'trio' – both among the wider public and the political elite. In several cases, decision-makers fundamentally underestimate the scale and impact that hybrid and security threats to CI pose. They are still perceived as technical questions, rather than existential problems that can lead to very tangible and distinct consequences. The trend that can be identified in examined countries seems to be correlated to geopolitical risk perception. In contexts, where political elites and populations do not perceive Russia or other external actors as high-level threat-actors, such as the case of Georgia – commitment to CI protection, and alignment with EU and NATO standards remains weak. Conversely, in countries with a strong perception of external risks, such as the Baltic States, Ukraine or Finland, CI resilience has become a central element of national security strategy.

Hybrid and geopolitical threats constitute one of the most significant challenges to CI protection and resiliency. Russia's war of aggression against Ukraine has fundamentally changed the European security landscape, with hybrid threats against CI networks growing exponentially in recent years. Through hybrid threats certain actors such as Russia seek to leverage vulnerabilities in the EU's energy, digital and transport networks. Some Member States, such as the Baltic states and Finland, are exposed to particularly high risks due to their geographical proximity to Russia, but threats are emerging across all Europe. Threat landscapes in this regard vary by region: while underwater infrastructure and energy interconnectors have been priority targets in the Baltic Sea region, border states face continuous cyber intrusions and disinformation campaigns, while Wester Balkan countries experience hybrid threats that exploit institutional weaknesses and political fragmentation. These developments illustrate that CI resilience is inseparable from Europe's broader geopolitical environment, in which state and non-state actors use hybrid tools to challenge the Europe's cohesion, strategic autonomy, and long-term stability.

Operational challenges concerning harmonisation, public-private partnerships, coherent national frameworks in CI protection, the neglect of physical protection, and securing adequate resources for CI policy.

The cross-border nature of CI systems demands EU-wide coordination, yet cooperation mechanisms remain fragmented. This lack of harmonized approaches limits the effectiveness of crisis responses, data sharing and resilience-building, especially between EU Member States and candidate countries. However, there seems to be an ***inherent trade-off between the need for harmonisation and the flexibility*** required to adapt to evolving threats and technological advancements. Overly rigid frameworks may hinder innovation or quick adaptation, whereas too much flexibility risks incoherence and uneven implementation. Therefore, it is crucial to find the right balance for a resilient and adaptive CI governance model.

Public-private partnerships (PPPs) remain another critical operational challenge. The private sector operates much of Europe's CI, but collaboration with governments is often done on an *ad hoc* basis. Information sharing of private companies with governments is limited in certain MS by lack of trust, unclear liability frameworks, and data protection constraints. This seems to be especially important in candidate countries, where PPPs remain significantly underdeveloped in the field of CI protection and resiliency.

Western Balkan and Eastern Partnership countries also face institutional, legal, and resource-based limitations in aligning with EU standards on CI protection and resilience. Furthermore, in some candidate countries a ***lack of a coherent national CI framework and inter-agency coordination limits resilience-building*** and leads to increased vulnerabilities and fragmented governance. Furthermore, EU support, while financially important, is cyclical and project-based in nature. Therefore, long-term planning is inherently difficult and limits a focus on systemic capacity development.

Another recurring issue is the ***neglect of physical protection***. While cybersecurity has become a central focus of both EU and national resilience strategies, the physical dimension of CI protection often remains underdeveloped. Funding opportunities, regulatory frameworks, and international assistance programs tend to prioritize digital infrastructure, leaving gaps in the protection of physical assets such as energy grids, transport hubs, and underwater or cross-border interconnectors. Besides, there is ***uncertainty over the methodologies of threat and risk assessments*** and related decision on the investments into protection and accumulation of redundancies by CI operators, especially in face of fast changing hybrid hostile activities.

Finally, ***securing adequate financial and human resources for CI protection*** remains a challenge across all EU Member States and candidate countries. Even where institutional frameworks are advanced, limited fiscal space and competing budgetary priorities often restrict the capacity to invest in resiliency measures. The simple reality is that financing large-scale infrastructure upgrades requires an incredible amount of planning, risk-assessments and the continuous training of experts. Candidate countries in this regard face additional constraints due to their reliance on project funding, which cannot ensure the continuous development of infrastructure.

Linking Systemic and Operational Challenges to Lessons for Strengthening CI Resilience

The challenges identified reveal not only where CI resilience systems face difficulties, but also where some of the most valuable lessons for future governance can emerge. The lessons that follow therefore distil what has worked, where progress has been possible, and which governance principles are essential for building resilient, interconnected systems.

Early and continuous involvement of CI operators improves the feasibility and effectiveness of resilience measures. It is clear that effective CI resilience requires the active involvement of national authorities, regulators, CI operators, and civil society during the policy development process. This approach can improve the quality and practicality of resilience measures, especially with regard to CI operator obligations. Early engagement of operators in designing implementation measures produces solutions that are both technically feasible and operationally effective. Involving civil society further ensures both legitimacy and public awareness, which in turn has positive effects on risk-preparedness.

The literature review confirms that resilience is strongest when all relevant stakeholders – public, private, and civic – are engaged in a transparent and coordinated manner.[9]

Trust-building and institutionalised information sharing are essential for functional cooperation. To successfully involve different actors in policy development, and the implementation of policy, there needs to be a certain level of trust in institutions, and the system. Where institutionalised trust-building mechanisms and clear information-sharing procedures exist, response coordination is faster and more effective. However, where mistrust or fear of liability is much more prevalent, critical information is often withheld, damaging the effectiveness of crisis-management. Therefore, a level of trust is fundamental for any functioning PPP framework in CI resilience. The experiences of the Baltic States and Finland with the early involvement of private actors in resilience planning underline that transparency, consistent communication, and trust between the public and private sectors both enhances operational effectiveness and situational awareness. Similar lessons also emerge from Montenegro, where modest institutional resources have been offset by pragmatic inter-agency cooperation and close coordination with EU.

Common risk assessment methodologies are essential for coherent CI governance across borders. Divergent risk perceptions and differing geopolitical and hybrid threats lead to fragmented policy implementation across Europe. Even though the NIS2 and CER Directives, as well as sectoral regulations set minimum standards, there still exist significant disparities, firstly, between EU Member States, and, secondly, even more so between EU Member States and candidate countries on how they define, regulate and manage CI protection and resilience. The analysis of the Baltic Sea region shows that interdependent CI cannot be safeguarded based on nationally isolated risk assessments. Without shared methodologies, risk visibility, prioritisation, and investment decisions will remain fragmented.

High threat awareness lays the groundwork for effective CI resilience. States, which are continuously exposed to a high level of hybrid threats as well as geopolitical risks, have also demonstrated some of the most adaptive and practical solutions in CI resilience. For example, the Baltic countries and Finland have developed advanced models of cybersecurity governance, civil-military coordination, and regional cooperation that integrate resilience as a core tenet. Their success is rooted in high threat awareness, institutionalised cooperation between public authorities and private operators, and a long-term commitment to resilience as a strategic rather than regulatory goal. The case of Ukraine offers extremely valuable insights into resilience under extreme conditions. Ukraine's ability to maintain essential services and restore damaged CI amidst ongoing war demonstrates how crucial adaptability, and decentralised governance in crisis management is. These examples illustrate how adversity leads to innovation and institutional development, providing best practices for other EU Member States and candidate countries alike.

[9] Vira Ratsyborinska: EU-NATO and the Eastern Partnership Countries Against Hybrid Threats (2016-2021), in: National Security and the Future, 2 (23), 2022, p. 89. See also: Donika Elshani: What Can Kosovo Learn From the Baltic States' Approach to Critical Infrastructure Protection, KCSS, 2023.

Hybrid and geopolitical threats require integrated whole-of-society, holistic approaches. Both the empirical research[10] and the literature review confirm that resilience cannot be built through regulation alone.[11] Whole-of-society and all-hazards approaches, where governments, private actors, and citizens domestically on the one hand, as well as coordinating within the EU and NATO on the other, are all part of preparedness and response structures. Models that effectively invovle different actors accelerate readiness and sustain it more effectively than rule-based compliance models.

Coherent national CI frameworks and clear institutional mandates are prerequisites for effective governance. Case studies from Montenegro and Georgia illustrate how institutional fragmentation can result in duplicated efforts, overlooked vulnerabilities, and inconsistent operator compliance. Therefore, a clear national coordination system and framework is necessary for the supervision, enforcement, and strategic direction of CI policy.

Meaningful progress in CI resilience is possible when countries leverage external support, regional cooperation, and phased implementation approaches. Even where resources for CI reforms are limited, that does not necessarily always prevent meaningul change in the system. Candidate countries have managed to strengthen CI resilience through drawing on EU financial instruments, international technical assistance, and cooperation with EU Member States. This has enabled legislative development, operators training, and early warning capacities. Furthermore, Member States have strengthened their competence through embedding in regional frameworks. Finally, several countries have also adopted phased, adaptive implementation, prioritising the most exposed sectors and gradually expanding compliance as capacity increases.

It is also important to mention that, even though discussions of CI protection and resilience are often framed in terms of "front-line" states with heightened risk perceptions, and stronger political stances, CI resilience is an issue, that all EU Member States and NATO Allies are grappling with. This broader framing matters for two reasons: 1) it reinforces the fact that CI vulnerabilities are a systemic problem in EU/NATO Member States, rather than just limited to specific regions, or as a result of differing levels of integration; 2) it also highlights the fact that any effort to enhance CI resilience, either through regulation, investment, information sharing or cooperation, must be conceived as large-scale, Union-wide endeavours.

[10] Vilpišauskas, Ramūnas, et al: *Invigorating enlargement and neighbourhood policy for a resilient Europe: Long policy report on rules alignment of protecting critical infrastructure in interdependent states* (InvigoratEU Report D7.1), 2025. https://doi.org/10.5281/zenodo.17340020. See also: Vilpišauskas, Ramūnas, et al: *Invigorating enlargement and neighbourhood policy for a resilient Europe: Long policy report on a Common Framework for the Protection of Critical Infrastructure in the EU and its Neighbourhood*, 2025. https://doi.org/10.5281/zenodo.17630178.

[11] Youri Devuyst: The European Union's Handling of Hybrid Threats: In Search of the Enlargement Dimension, in: L'Europe Unie, 22, 2025. See also: Donika Elshani: What Can Kosovo Learn From the Baltic States' Approach to Critical Infrastructure Protection, KCSS, 2023 & Vasko Popovski et al.: Crisis Prevention and Critical Infrastructure in the Western Balkans, IDSCS Policy Paper, 9/2023.

3 Conclusions and recommendations

The analysis of EU Member States, and candidate countries[12] confirms that CI resilience is not a regionally isolated issue, but rather a European-level priority. While geopolitical pressures have accelerated reforms in some regions, institutional fragmentation, differing risk perceptions, and resource and capacity limitations continue to hinder coherent resilience-building as a systemic issue across the European continent. At the same time, the case studies demonstrate that meaningful progress is possible when institutional trust, stable coordination structures, and sustained political attention are present. Effective resilience is not produced through legislation, but through continuous cooperation between authorities and operators, creating a culture of preparedness and shared situational awareness. There is also a slow, yet palpable shift from threat-specific to system-wide perception and understanding of the concept of resiliency, which emphasizes joint governance models, bridging civil, military and private-sector obligations and responsibilities.

CI resilience remains both a shared vulnerability, as well as a shared opportunity for deeper integration, improved and increased levels of security, as well as strengthened levels of cooperation. As a result, this policy brief will provide a concrete set of 11 recommendations for different actors, to improve the CI resiliency framework within the EU and its candidate countries.

Recommendations for the European Union

1. EU institutions and relevant agencies should systematically disseminate common threat and risk assessment methodologies, including best practices, sector-specific guidance, and practical implementation tools.
2. Support candidate countries through technical assistance, twinning programs, and regulatory mentoring to adopt and operationalize EU norms, as well as prioritizing institution and capacity building over one-off projects

Recommendations for Member States and Neighbourhood Countries

3. Encourage public education and community involvement in resilience planning to build societal and institutional trust and awareness at all levels. Engage academia and civil society as well.
4. Create clear legal bases for information sharing and joint risk assessments between CI operators and national authorities.
5. Incentivize investment in resilience through tax benefits, co-funding.

[12] Vilpišauskas, Ramūnas, et al: *Invigorating enlargement and neighbourhood policy for a resilient Europe: Long policy report on rules alignment of protecting critical infrastructure in interdependent states* (InvigoratEU Report D7.1), 2025. https://doi.org/10.5281/zenodo.17340020. See also: Vilpišauskas, Ramūnas, et al: *Invigorating enlargement and neighbourhood policy for a resilient Europe: Long policy report on a Common Framework for the Protection of Critical Infrastructure in the EU and its Neighbourhood*, 2025. https://doi.org/10.5281/zenodo.17630178.

6. One-stop or harmonised/unified incident & threat reporting that both satisfies CER, NIS2, and sectoral regulations.

7. Integrate physical, organizational, and societal resilience into national CI strategies. Furthermore, promote multi-hazard preparedness that includes environmental, technological, and hybrid risks.

8. Continue systematic regular training exercises involving domestic stakeholders and partners from EU and NATO.

Recommendations for International and Regional cooperation

9. Expand cooperation under the EU-NATO Task Force on CI resilience to include select partner states (e.g. Ukraine, Georgia, Montenegro).

10. Encourage regional resilience clusters (e.g. Baltic-Nordic, Black Sea) to foster cooperation, integration and mutual assistance.

11. Establish joint early-warning systems and shared awareness mechanisms.

12. Promote cross-border risk assessments and shared capacity-building

Bibliography

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of Euro¬ pean critical infrastructures and the assessment of the need to improve their protection, OJ L 545, 23.12.2008., p. 75/82.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, JO L 333, 27.12.2022., pp. 164-198.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, OJ L 353, 27.12.2022., p. 80.-152.

Donika Elshani: What Can Kosovo Learn From the Baltic States' Approach to Critical Infrastructure Protection, KCSS, 2023

Julian Plottka & Kai Ole Vorberg: Review of Literature on Critical Infrastructure Protection, Institut für Europäische Politik, Berlin, 2025.

Vasko Popovski et al.: Crisis Prevention and Critical Infrastructure in the Western Balkans, IDSCS Policy Paper, 9/2023.

Vilpišauskas, Ramūnas, et al: *Invigorating enlargement and neighbourhood policy for a resilient Europe: Long policy report on rules alignment of protecting critical infrastructure in interdependent states* (InvigoratEU Report D7.1), 2025. https://doi.org/10.5281/zenodo.17340020.

Vilpišauskas, Ramūnas, et al: *Invigorating enlargement and neighbourhood policy for a resilient Europe: Long policy report on a Common Framework for the Protection of Critical Infrastructure in the EU and its Neighbourhood*, 2025. https://doi.org/10.5281/zenodo.17630178.

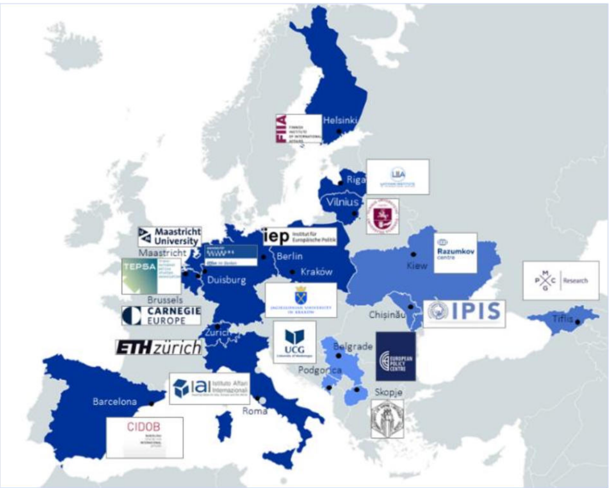
Vira Ratsyborinska: EU-NATO and the Eastern Partnership Countries Against Hybrid Threats (2016-2021), in: National Security and the Future, 2 (23), 2022, p. 89.

Youri Devuyst: The European Union's Handling of Hybrid Threats: In Search of the Enlargement Dimension, in: L'Europe Unie, 22, 2025.

About InvigoratEU

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

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



Our first goal is to investigate <u>how to reform </u>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 <u>evidence-based, forward-looking vision for the EU's political agenda and institutional frameworks for co-designing a multidimensional toolbox</u> (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 <u>aiming at recommendations from Day 1</u> to maximize our scientific, policy and societal impact in invigorating the EU's enlargement and neighbourhood policies to enhance Europe's resilience. <u>Ultimately, InvigoratEU is a deliberately large consortium</u> <u>respecting the diversity of Europe</u> and <u>political perspectives</u>; 7 out of 18 are from <u>Georgia, Moldova, Ukraine</u>, and the western Balkans (<u>North Macedonia, Montenegro, Serbia</u>), 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.

Disclaimer: Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Funded by
the European Union