Terrorism – Studies, Analyses, Prevention, 2025, special edition: 315–339

https://doi.org/10.4467/27204383TER.25.024.21527

Expert material

The value of EU research projects in critical infrastructure protection

Małgorzata Wolbach
Polish Platform for Homeland Security
https://orcid.org/0009-0005-1837-0389

Rashel Talukder
Polish Platform for Homeland Security
https://orcid.org/0000-0003-4743-9355

Critical infrastructure (CI) protection and ensuring its ongoing resilience, particularly against hybrid threats, are fundamental to the stability of modern societies. Reliable access to essential services such as energy, water, food, healthcare, and transportation underpins the secure and stable functioning of daily life.

The institutions of European Union in recent years have placed significant emphasis on strengthening the protection and resilience of CI. This has been influenced by the ongoing war in Ukraine, which has exacerbated concerns about CI security across Europe.

Key areas of EU action include:

- introduction of the CER Directive[1] (The Critical Entities Resilience Directive);
- introduction of the NIS 2 Directive[2] (Network and Information Systems Directive 2) on network and information security;
- establishment of an EU plan for CI (recommendations adopted by the Council of the EU, inter alia, coordinate responses to CI disruptions of cross-border significance)[3];
- cooperation with NATO[4];
- exchange of information and good practices, inter alia through the involvement of the Critical Entities Resilience Group (CERG), which facilitates cooperation and exchange of information between Member States to ensure the effective implementation of the CER Directive[5].

Moreover, EU provides substantial financial and strategic support for research and innovation in the field of CI protection through different funding programmes. These help to develop new technologies and introduce solutions to counter emerging threats and improve infrastructure resilience[6]. The EU has established several such programmes. By investing in these initiatives, the EU not only strengthens the protection of its CI but also promotes economic growth and sustainable development. As highlighted in the annual progress report on the implementation of common solutions to counter hybrid threats[7], EU-funded security research projects

---

1 *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.*

2 *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.*

3 *Council Recommendation of 25 June 2024 on a Blueprint to Coordinate a Response at Union Level to Disruptions of Critical Infrastructure with Significant Cross-Border Relevance.*

4 *NATO and European Union release final assessment report on resilience of critical infrastructure*, NATO, 29.06.2023, https://www.nato.int/cps/en/natohq/news_216631.htm [accessed: 6.01.2025].

5 *Critical infrastructure resilience at EU-level,* European Commission, 23.09.2024, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en [accessed: 6.01.2025].

6 Ibid.

7 *Joint Staff Working Document. Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats*, https://defence-industry-space.

play a crucial role in identifying existing gaps and enhancing the security and resilience of CI across the EU.

The article presents selected EU-funded projects under Horizon 2020 and Horizon Europe, such as: EU-HYBNET, EU-CIP, VIGIMARE, TESTUDO, NBSINFRA, ENDURANCE and TRANSCEND. Furthermore, the article analyses challenges associated with the implementation of these projects, including regulatory inconsistencies (different national regulations and inconsistent interpretations of EU directives), financial constraints, and the need for cross-border cooperation. Recommendations for future research directions were made and the importance of cyber security, quantum technology and real-time threat information sharing in enhancing the EU's ability to respond to evolving security threats was highlighted.

Funding for research and innovation in critical infrastructure protection using Horizon Europe as an example

One of the EU funding programmes that stands out for its significant contribution to research and development (aimed at strengthening CI resilience) is Horizon Europe. It is the EU's flagship programme for the period 2021–2027 dedicated to research and innovation (R&I), with a projected budget of EUR 93.5 billion. Supporting advances in science and technology is becoming more urgent, especially in the context of increasing geopolitical instability. Events such as Russia's full-scale invasion of Ukraine have highlighted threats to security, democracy and global supply chains, making the programme's objectives in the second half of its implementation even more relevant. Horizon Europe supports international cooperation and increases the impact of research and innovation on EU policy-making. At the same time, it plays a vital role in addressing pressing global challenges. Horizon Europe provides a diverse set of instruments – from basic research, to disruptive innovation, to the development and implementation of cutting-edge solutions – for research-based solutions[8].

ec.europa.eu/system/files/2025-01/SWD_Annual-Progress-Report-2024.PDF [accessed: 2.01.2025].

[8] *Horizon Europe,* https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en [accessed: 7.01.2025].

The Horizon Europe Strategic Plan 2025–2027[9] details the most important strategic objectives, priority actions, and thematic focus areas for the latter stages of its implementation. It aims to align the final years of this programme with emerging challenges, evolving EU policies, and the changing needs of its Member States. It is the EU's most ambitious research and innovation programme to date due to the fact that it responds to the global context, supports breakthroughs and facilitates access to funding for a diverse research groups and non-EU companies, and has a record budget. The plan combines overarching EU policy goals with the research and innovation activities carried out under the Horizon Europe programme. It offers planning stability that extends beyond the standard two-year work programme cycle. It provides predictability for the research community, while maintaining flexibility to address unexpected changes and challenges[10].

Projects funded under Horizon Europe aim to acquire new knowledge, technologies, and solutions that meet the requirements. These are projects that involve end-users working with researchers and industrial partners. This inclusive model ensures that the outcomes of research and innovation are closely aligned with the practical needs of those who will ultimately implement them, making projects more useful.

These projects play a crucial role in addressing current global challenges, including enhancing the CI resilience[11]. The war in Ukraine has underscored the importance of R&I in issues, such as providing clean energy, sustainable food, medicines, ensuring defence capabilities, and socioeconomic security. These efforts are essential not only for minimising immediate risks but also for ensuring long-term resilience and stability. Horizon Europe projects already contribute to overcoming rapidly evolving challenges related to CI with cross-border relevance. In the future, this will require even greater innovation and coordinated efforts.

[9] *Horizon Europe. Strategic Plan 2025–2027,*European Commission, 2024, https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/6abcc8e7-e685-11ee-8b2b-01aa75ed71a1 [accessed: 7.01.2025].

[10] *Strategic plan,* https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/strategic-plan_en [accessed: 3.01.2025].

[11] *Horizon Europe. Strategic Plan 2025-2027. Analysis*, European Commission, 2023, https://op.europa.eu/en/publication-detail/-/publication/b3baec75-fdd0-11ed-a05c-01aa75ed71a1/language-en [accessed: 9.01.2025].

The CI resilience, including energy, transport, and telecommunications, is a priority for the EU, particularly in the face of hybrid threats. Actions taken, e.g. the implementation of the CER Directive, aim to ensure both physical and cyber CI resilience. Security research under Horizon Europe supports these efforts by providing innovative methodologies for scenario planning, serving as a test environment for project solutions, stress tests, and threat minimisation. The EU Council has encouraged Member States to make full use of EU-funded research and innovation results, emphasising their importance in enhancing infrastructure resilience. In this context, R&I projects serve as a vital bridge between policy and practice, enabling the EU and its Member States to respond effectively to current and future challenges. Through collaboration, fostering innovation and resilience, these projects are integral to protecting the EU's infrastructure, security and competitiveness in an increasingly complex world[12].

Horizon Europe fosters R&I through its Work Programmes, which outline funding opportunities for various activities. The programme is structured around 3 key Pillars. Pillar II – Global Challenges and European Industrial Competitiveness – is divided into 6 clusters of R&I activities. The clusters were designed to foster integration and complementarities across thematic areas, while ensuring that the EU achieves significant and sustainable impact on the challenges identified in each Horizon Europe cluster in relation to the resources invested.

Cluster 3 – Civil Security for Society is dedicated to enhancing security by supporting efforts to prevent and build resilience to threats to security: internal, individual and society as a whole[13]. It also encompasses tackling the evolving threats, including terrorism, corruption, organised crime, and hybrid attacks on CI. By deepening the understanding of these threats and their societal roots, and by developing advanced tools to prevent, detect, and investigate them, Cluster 3 seeks to enhance the EU's security capabilities. R&I activities within the cluster also focus on ensuring the resilience of CI – such as energy, water, food supply, and healthcare systems – against physical or cyber attacks. A budget of EUR 1.596 billion has been allocated to Cluster 3.

[12] Ibid.

[13] *Horizon Europe. Strategic Plan 2025-2027*, European Commission, 2024...

Cluster 3 is organised into 6 main destinations, each focusing on specific priorities within the overarching theme of civil security. Destination 3, Resilient infrastructure, is dedicated to enhancing the resilience and autonomy of both physical and digital infrastructures. The expected results are described as follows: *Resilience and autonomy of physical and digital infrastructures are enhanced, and vital societal functions are ensured, thanks to more effective prevention, preparedness, and response, a deeper understanding of the associated human, societal, and technological aspects, and the development of cutting-edge capabilities for infrastructure operators*[14].

This destination is closely linked with Destination 6, Strengthened Security Research and Innovation, which provides the research, technological advancements, and innovative solutions that underpin and support Destination 3. These destinations both create a complementary framework to address EU security priorities, advancing the protection of CI while bolstering societal and economic resilience. They have practical applications in relation to equipping infrastructure operators with advanced tools and capabilities to respond effectively to emerging challenges.

An example of the implementation of Destination 3 was the Resilient Infrastructure (HORIZON-CL3-2024) call for funding in 2024[15] research and innovation to strengthen infrastructure resilience. Themes funded under HORIZON-CL3-2024 are:

- **INFRA01:** *Improved preparedness and response for large-scale disruptions of European infrastructures,*
- **INFRA02:** *Resilient and secure urban areas and smart cities.*

Details about these topics, including their type of action and the expected outcomes, are summarised in the table 1.

[14] *Horizon Europe. Work Programme 2023-2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024)*, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf, p. 8 [accessed: 10.01.2025].

[15] Ibid.

Table 1. Sub-topics of the Resilient Infrastructure Programme (HORIZON-CL3-2024).

Sub-topic INFRA01	HORIZON-CL3-2024-INFRA-01-01: Open Topic
Type of action	Innovation Actions
Expected outcomes	Projects' results are expected to contribute to all of the following outcomes: • CI operators are more resilient to natural and man-made threats; • improved monitoring, risk assessment, its forecast, limitation and modelling techniques aimed at increasing the CI resilience, validating multi-hazard scenarios, creating interactive hazard maps based on Earth observation and other data sources.
Sub-topic INFRA02	**HORIZON-CL3-2024-INFRA-01-02: Resilient and secure urban planning and new tools for EU territorial entities**
Type of action	Innovation Actions
Expected outcomes	Projects' results are expected to contribute to all of the following outcomes: • evaluation of the resilience of an urban and peri-urban environment, identification of weaknesses and recommendations for changes to organisational processes; • creation of new tools and cost-efficient security upgrades of urban infrastructures with possibilities of pooling and sharing of complex security systems, taking into account limited budgets of local authorities; • improved efficiency of the security forces and emergency services (police, firefighters, paramedics, etc.) for the benefit of the European citizens and residents; • promotion of best practices, creation of EU sovereign trusted decision support tool/solution and spreading of effective tools and capabilities across entities in different EU territories despite their size and location.

Sub-topic INFRA02	**HORIZON-CL3-2024-INFRA-01-03: Advanced real-time data analysis used for infrastructure resilience**
Type of action	Research and Innovation Actions
Expected outcomes	Projects' results are expected to contribute to some or all of the following outcomes: • improved capabilities for risk and faulty events identification in infrastructure networks and smart cities through real-time analysis (including big data) by public and private actors via secured and trusted platforms and interconnected systems where the collaboration follows clear legal and political frameworks; • tools and processes for facilitating stakeholders efforts to identify, analyse, assess and continuously monitor risks and boost adaptive capacity to unexpected events risks in advance by allowing for the analysis of various data sources (e.g. audio, video, social media, web-content, spatial information, sensor or machine generated data); • fast and continuous real-time identification, classification and tracking of hazardous agents, contaminants or anomalies in infrastructure networks and supply-chains; interoperable interfaces and improved collaboration between infrastructure operation detection and response systems, national/EU risk management/coordination centres and first responder equipment in order to allow for remote on-scene operations considering citizen knowledge; • increased cyber-resilience of industrial xG networks and cloud data covering specific infrastructure domains; • improved ability to map in real-time the source(s) of risk that could endanger the networked infrastructure supported by Earth Observation and geolocation data. If the analysis includes processing of personal data, it should consider including assessment of associated risk or privacy impact of individuals and society.

Source: *Horizon Europe. Work Programme 2023-2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024)*, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf, pp. 91–97 [accessed: 10.01.2025].

An indicative budget of EUR 16 million has been allocated for the Resilient Infrastructure Programme in 2024[16].The deadline for applications was 20 November 2024. Of the 79 that were submitted, only three will be successful, with implementation starting in September 2025. This shows not only competitiveness of the contest, but also the reduction in the overall budget for research and innovation in CI protection.

Overview of selected research and innovation initiatives funded under Horizon 2020 and Horizon Europe Programmes

EU-funded initiatives in the field of CI protection are developing both technological and non-technological solutions. At the same time, these initiatives strengthen European cooperation. The aim is to demonstrate the opportunities such projects offer to a wide range of stakeholders, including research institutions driving innovation, businesses developing cutting-edge security solutions, public organisations implementing policies, as well as CI owners and operators responsible for ensuring service continuity.

EU-HYBNET
(Empowering a Pan-European Network to Counter Hybrid Threats)[17]

The Project, funded by the European Union's Horizon 2020 Research and Innovation Programme (a predecessor of Horizon Europe). It is the first EU initiative that brings together security practitioners, academics, industry players and business as well as non-government organisations to collaborate, identify and analyse common challenges, and requirements to counter hybrid threats.

The main project objectives of EU-HYBNET are to:

1. Create and develop the network of European organisations countering hybrid threats and ensure long-term sustainability of the network.

[16] *Resilient Infrastructures,* https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/resilient-infrastructures_en [accessed: 10.01.2025].

[17] *Empowering a Pan-European Network to Counter Hybrid Threats,* European Commission, https://cordis.europa.eu/project/id/883054 [accessed: 13.01.2025].

2. Define common requirements to fill knowledge gaps, address performance needs, and enhance capabilities of research, innovation and training endeavours concerning hybrid threats.
3. Monitor developments in research and innovation activities as applied to hybrid threats.
4. Identify priorities for the implementation of innovation and industrialisation, and to increase the role of European network in effectively countering hybrid threats.
5. Establish conditions for enhanced interaction among security practitioners, industry, and academia to foster meaningful dialogue and increase network membership.
6. Foster capacity building and knowledge exchange on countering hybrid threats.
7. Create a basis for effective cooperation with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats.

The project addresses 4 core themes to ensure coherence in its results, and to facilitate a focus on all hybrid threat domains (including CI). These are:

1. Future trends of hybrid threats.
2. Cyber and future technologies.
3. Resilient civilians, local level and national administration.
4. Information and strategic communication.

These themes emphasise domains, as identified and defined by the European Commission and EU Joint Research Centre (JRC). This provides essential support for research and innovation activities in hybrid threat domains deemed crucial for delivering solutions during the project cycles.

Although the project ended in April 2025, the network is ever-growing (currently consisting of more than 150 organisations from EU countries, Ukraine, and the UK)[18].

[18] *EU-HYBNET*, https://euhybnet.eu/ [accessed: 13.01.2025].

EU-CIP
(European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection)[19]

This is also a networking initiative, but focused only on CI. It runs from October 2022 to September 2025.

The main goal of EU-CIP is to establish a unique pan-European knowledge network for resilient infrastructures, enabling policymakers to shape and produce data-driven, evidence-based policies, while boosting the innovation capacity and competitiveness of CI operators, authorities, researchers, and innovators. In this direction, the project develops the European Cluster for Securing Critical Infrastructures, ECSCI – established and operated by the project partners – Europe's most prominent R&I knowledge network for security and resilience of CI. The ECSCI cluster brings together 22 projects that collaborate on CI resilience. EU-CIP leverages the capacity, organisation, community, and achievements of the ECSCI cluster to establish an EU-wide knowledge network.

EU-CIP offers advanced information analysis capabilities for evidence-based policymaking and innovation support to facilitate the exploitation and commercialisation of research outcomes. To maximise the impact of its activities, EU-CIP establishes and expands a vibrant ecosystem of interested and committed stakeholders around the project's information analysis and innovation support services.

EU-CIP main objectives:

1. Analysis: enhancing Europe's analytical capability regarding research outcomes, technologies, and policies – foster data-driven evidence-based policy and innovation development. EU-CIP establishes a data collection, information monitoring, and analysis methodology and infrastructure, which continually collects, analyses, curates, extracts, and presents information and insights about resilient infrastructures. As part of this objective, EU-CIP presents foresight and insights about gaps in current knowledge and solutions, technologies that address these gaps, as well as research outcomes and practices that can be employed.
2. Amplification: maximising the impact of R&I activities in the field of critical infrastructure protection (CIP) and critical infrastructure resilience (CIR) in Europe. The project provides a set of innovation

[19] *European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection,* European Commission, https://cordis.europa.eu/project/id/101073878 [accessed: 13.01.2025].

support and solution validation services for research outcomes in the areas of resilient infrastructures (CIP/CIR). In this direction, the project leverages the analytical outcomes of the EU-CIP-ANALYSIS pillar to identify gaps in existing solutions and CI areas with significant innovation potential. Accordingly, EU-CIP offers a range of services that will support CIP/CIR innovators (including Small and Medium sized Enterprises, SMEs) in their activities related to the exploitation and commercialisation of research results. Moreover, the project offers a virtualised testbed for the experimentation with standards-based CIP/CIR solutions and certification schemes, along with relevant validation and evaluation processes involving stakeholder engagement.

3. Creating the ecosystem: establishing a Knowledge-Hub and creation of a vibrant ecosystem of interested and committed stakeholders around the project's results. EU-CIP establishes and grows an EU-wide ecosystem of CIP/CIR stakeholders, covering EU-27 and other European Economic Area (EEA) countries. The ecosystem facilitates stakeholders' access to the knowledge, results, services, and infrastructures developed in previous objectives, as well as their engagement with innovation development and policymaking outcomes of EU initiatives (e.g. research projects, technology initiatives, policymaking initiatives). At the heart of the ecosystem is a Knowledge-Hub, which provides access (via the relevant digital infrastructure) to the project's knowledge assets, including the infrastructures and results developed in previous objectives. It allows collaboration between different stakeholders.

The expected results of the EU-CIP are as follows:

- enhanced resilience of CI – through comprehensive analysis, the project identifies and addresses gaps;
- evidence-based policy development – by aggregating and analysing a broad spectrum of data, the project supports the creation of more effective policies for CIP/CIR;
- boosting innovation and competitiveness – the project through advanced information analysis capabilities and innovation support services, enhances the capacity of European innovators, particularly in exploitation and commercialisation of research outcomes;
- fostering a collaborative ecosystem – the establishment of a vibrant ecosystem of stakeholders facilitates knowledge

sharing, collaboration, and the co-creation of solutions, enhancing the collective ability to address CIP/CIR challenges[20].

VIGIMARE

(Vigilant Maritime Surveillance of Critical Submarine Infrastructure)[21]

This is an innovation action type of project, what means that it is focused on developing solutions with higher Technology Reediness Level (TRL).

The project has developed an innovative solution to improve security and mitigate the risk of physical attacks and cyber threats. The project seeks to identify early warning signals and support analysis by mapping submarine systems, assessing vulnerabilities, and creating real-time awareness of both surface and underwater CI. The project takes a systematic approach to strengthen the European CI sector of submarine telecommunication cables, power cables and gas pipelines. The analysis as well as the VIGIMARE system will support the CI operators of the submarine network by enhancing its resilience against attacks and damages.

VIGIMARE objectives:

- provide information sharing environment to the CI operators against threats to the EU submarine CI;
- increase the resilience of CI operators against physical, cyber and hybrid threats by implementing risk preventing and risk reducing measures;
- strengthen the situational awareness of European maritime areas, both offshore and onshore, to recognise physical (both man-made and natural), cyber and hybrid attacks and incidents for both CI operators and the Member States, enabling better planning of the response and repairs;
- support the EU Member States to fulfil CER and NIS 2 Directives' requirements. The outcomes of this project will also introduce the European Maritime Safety Agency's (EMSA) Common Information Sharing Environment (CISE) to this new area of interest. The solution proposed by VIGIMARE project will be stress-tested using data from real incidents and validated in 3 different European

[20] *EU-CIP,* https://www.eucip.eu/ [accessed: 13.01.2025].

[21] *Vigilant Maritime Surveillance of Critical Submarine Infrastructure,* European Commission, https://cordis.europa.eu/project/id/101168016 [accessed: 14.01.2025].

sea areas – the Mediterranean Sea, the Irish Sea and the Baltic Sea – in order to promote its valuable outcome to the European society[22].

TESTUDO

(Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention)[23]

This project aims to enhance the surveillance of the European CI and its protection using autonomous systems and advanced technologies to ensure their robust operation.

TESTUDO objectives:

- utilise advanced unmanned vehicles along with existing equipment for continuous monitoring even in harsh environments and remote territories;
- incorporate state-of-the-art technologies for detecting, preventing and anticipating hazardous events to enhance capabilities in this area;
- identify the resources needed for operational activities through optimisation techniques, contributing to the total autonomy of the system;
- bring together a multidisciplinary group comprising specialists in: AI-based models, chemical, biological, radiological, nuclear threats (CBRN), cyber security threats, digital twins (digital replication of physical objects, processes and system) and CI, in order to develop innovative solutions to protect various CI facilities operating in the long term and completely anonymously[24].

NBSINFRA

(Citynature-based Solutions Integration to Local Urban Infrastructure Protection for a Climate Resilient Society)[25]

This is a pioneering European initiative that supports the enhancement of local urban CI protection against natural and manmade hazards.

[22] *VIGIMARE*, https://vigimare.eu/ [accessed: 15.01.2025].

[23] *Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention*, European Commission, https://cordis.europa.eu/project/id/101121258 [accessed: 15.01.2025].

[24] *TESTUDO*, https://testudo-project.eu/ [accessed: 15.01.2025].

[25] *Citynature-based Solutions integration to local urban infrastructure protection for a climate*

It involves co-design and co-creation of Nature-based Solutions (NbS) to build a climate-resilient society. NBSINFRA demonstrates that the NbS are: a) technically viable for the protection of CI against hazards, b) socially acceptable and cost-effective at the local scale, c) efficiently capable to increase the empowerment of communities, through the increase of their ecological, social, and economic resilience.

NBSINFRA establishes 5 representative European regions with an equal number of "City Labs" in: Fingal (Ireland), Cologne (Germany), Ruse (Bulgaria), Aveiro (Portugal), Prague (Czechia). Labs will assess the cost-effectiveness of NbS solutions in the protection of local infrastructure and maximise their impact. These solutions will be owned by citizens and co-created by end-users and managers as well as civil society.

NBSINFRA provides a toolkit that the different stakeholders and society can use to compare and choose the most effective NbS for local CI protection. The main object is to increase its protection against hazards through NbS co-design, co-monitoring, and co-creation, serving the development of sustainable and resilient society[26].

ENDURANCE

(Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe)[27]

The ENDURANCE project aims to strengthen sectors such as energy, health, drinking water in Europe. The project ensures alignment with Europe's regulatory frameworks, particularly CER and NIS 2 Directives, empowering operators and authorities with the necessary tools, strategies, and knowledge to minimise risks and recover efficiently from disruptions.

ENDURANCE objectives:

- enhance strategic cooperation and collaboration among the CI stakeholders from different sectors and countries at all levels;
- develop datasets, registries, methodologies, technologies, and services (at TRL 6-7) for secure sharing processing of CER-relevant data, joint assessment of relevant risks and resilience, and large-scale stress-testing of preparedness;

resilient society, https://cordis.europa.eu/project/id/101121210 [accessed: 17.01.2025].

[26] *NBSINFRA*, https://nbsinfra.eu/ [accessed: 17.01.2025].

[27] *Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe*, European Commission, https://cordis.europa.eu/project/id/101168007 [accessed: 17.01.2025].

- provide harmonised and pragmatic strategy for the continuity of the interconnected essential services[28].

TRANSCEND

(Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption)[29]

TRANSCEND project aims to:

- provide freight transport operators with an integrated set of advanced tools, guidelines and technological solutions to reduce risks to transport networks and services that may arise from cyber and non-cyber events;
- enhance the protection and resilience of transport systems against physical, cyber and hybrid threats.

To achieve these objectives, the project will provide a digital platform for monitoring threats and risks and will develop 5 real-world pilots. They are divided into 3 main ones: the airport pilot in Luxembourg, the rail-road terminal pilot in Bologna, Italy and the tri-modal port pilot implementation in Spain; and 2 followers: the fluvial port of Budapest and the Egnatia highway in Greece.

The project results will be integrated into a Control Tower, a digital platform with embedded business intelligence giving stakeholders a shared and continuous visibility of threats and risks by breaking down silos within and between organisations. In order to test the effectiveness of the approach, five different transport CI sites will experiment with methodological and technological solutions, 3 in the roles of leaders and 2 followers[30].

Challenges and lessons learned with regards projects implementation

Competition for EU funding is intense and securing such funds presents a valuable opportunity for international cooperation. The implementation of successive EU research and innovation projects is highly respected

[28] *ENDURANCE,* https://endurance-horizon.eu/ [accessed: 17.01.2025].

[29] *Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption,* European Commission, https://cordis.europa.eu/project/id/101168023 [accessed: 17.01.2025].

[30] *TRANSCEND,* https://www.transcend-logistics.eu/ [accessed: 17.01.2025].

within the research community. Compared to national grants, which sometimes include an international component, EU projects assume cooperation between participants from European countries, representing different organisations, including universities, research institutions, private companies, public sector entities, and non-governmental organisations. Although an average project budget of EUR 3–5 million may seem substantial, it must be distributed among consortia of 10–15 or even more partners over a 3-year implementation period. Given the high expectations – according to the authors – for project outcomes, along with the impact of inflation in Europe in recent years, the available budget may not be as significant as it was a few years ago.

After analysing all these factors, conclusions were drawn and several challenges were identified. In the field of coordination across Member States one of the challenges is the different legal regulations and interpretation of EU directives. Albeit the EU provides common directives for CIP, cyber security, and data governance, their implementation and interpretation vary across Member States. Some countries strictly align national laws with EU directives, while others apply looser interpretations or have delays in their transposition into national legislation. For instance, CER and NIS 2 Directives aim for a common security framework, but their practical enforcement differs across countries[31]. These regulatory inconsistencies might lead to delays in project implementation, and complications in joint initiatives between Member States.

Addition challenge might be different perception of risks and national priorities which also have influence on EU projects. It translates into the engagement of these countries in facilitating the exchange of lessons learned and improving knowledge on hybrid threats, as well as in conducting international exercises which involve hybrid scenarios[32]. This divergence is particularly visible in the case of Russia and China, in relation to which EU Member States have different positions. For example, both governments and societies in Poland and the Baltic States consider China as a threat to cyber security and Russia as an aggressor after the attack on Ukraine,

[31] *The Commission calls on 23 Member States to fully transpose the NIS2 Directive*, European Commission, 28.11.2024, https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive [accessed: 29.01.2025].

[32] P. Szymański, *Towards greater resilience: NATO and the EU on hybrid threats*, Ośrodek Studiów Wschodnich, 24.04.2020, https://www.osw.waw.pl/en/publikacje/osw-commentary/2020-04-24/towards-greater-resilience-nato-and-eu-hybrid-threats [accessed: 7.02.2025]

while some governments in Member States (e.g. Hungary and Slovakia) are pursuing intensive economic and infrastructure cooperation with China and Russia, particularly in the field of energy. This lack of a unified risk assessment makes it difficult to fully implement joint protective measures and ensure consistent infrastructure security standards across the EU.

Experience from EU projects, confirmed by the observations of the article's authors, shows that Member States have different capacities to successfully implement CI protection projects due to different financial, technological, and human resources. Western and Northern European states are in a better position. Eastern and Southern European countries, on the other hand, face more budgetary constraints, leading to slower implementation of new security technologies and infrastructure upgrades.

A problem in many EU security projects is the complexity of cross-border cooperation including data sharing. However, it should be highlight that both European Commission and the Member States are implementing specific mechanisms and creating institutions (establishing new structures within existing institutions or new institutions) to support this process in the area of CI protection. These include the CER and NIS 2 Directives, European Programme for Critical Infrastructure Protection (EPCIP), European Cybersecurity Competence Centre (ECCC), and activities provided in cyber security by European Union Agency for Cybersecurity (ENISA). All these mechanisms and institutions should support both the implementation of projects and the use of their results.

Another group of challenges is related to balancing innovation with practicality. EU-funded projects focused on CIP (particularly under Horizon Europe Cluster 3), aim to introduce innovative solutions to enhance security, resilience, and efficiency. However, implementing state-of-the-art solutions is difficult due to technological feasibility, regulatory constraints, safety risks, lack of cost-effectiveness and applicability, among other factors.

Many research projects focus on developing high-tech solutions, such as AI-driven threat detection, advanced cyber security tools, quantum encryption. However, many innovations are in the experimental phase and require months or even years of testing and calibration before they can be safely integrated into existing infrastructure. CI operates for many years (so-called long life cycle), meaning new technology must be compatible with older systems, which is often difficult and expensive. Some emerging technologies (e.g. AI; blockchain; Internet of Things (IoT)

security systems) may not yet be mature enough for real-world application in high-risk environments. Thus, while innovation is essential, it must be practical, scalable, and proven to work in real-life conditions before it can be adopted.

Even when an innovation is technically feasible, it may face legal and regulatory hurdles[33]. EU and national regulations on cyber security, data protection, and CI security might slow down or restrict the use of new technologies. Different legal interpretations across Member States create inconsistencies, making it difficult to implement a single innovative solution across multiple countries. Governments and operators must ensure that new technology does not create additional risks, which in practice means long approval processes, testing, and security evaluations. As a result, even the most advanced innovations may take years to gain regulatory approval.

Additional challenge is that innovation often comes with high upfront costs for the development, testing, and implementation of new technologies. Also, CI such as energy grids, transportation networks, water systems, and telecommunications systems is often built on decades-old technologies. Consequently, technological feasibility does not always translate into rapid practical implementation due to incompatibility and operational considerations.

While new technologies can enhance security, they also cause security gaps. Advanced technologies (e.g. IoT, AI, cloud computing) are targeted by cyber criminals and state actors and require constant updates as well as security patches[34]. Moreover, some innovations can rely on hardware or software from non-EU countries, raising concerns about data security, backdoors, and foreign interference.

Innovation in CI protection requires cooperation between governments, private sector operators, and the public. However, there are often resistance and scepticism regarding new technologies, related to lack of trust in automation and AI, as well as privacy concerns. Technologies like biometric security, and smart monitoring often face public opposition due to fears of mass surveillance and misuse of data. In some countries,

[33] *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses*, OECD Publishing, Paris 2021. https://doi.org/10.1787/8fa190b5-en.

[34] *The cybersecurity challenges of legacy OT and how to manage them*, Control Engineering, 21.03.2024, https://www.controleng.com/the-cybersecurity-challenges-of-legacy-ot-and-how-to-manage-them [accessed: 7.02.2025].

e.g. Germany, France or Poland, there is a strong public backlash against the involvement of private tech companies or foreign entities in CI projects. If stakeholders do not trust the technology, they will not support its implementation. This inclusion ensures that the voices of the citizenry are considered in shaping policies for technologies that significantly impact society[35].

Future directions in EU research on critical infrastructure protection

Definitely future directions on EU research on CI protection must address forthcoming challenges. Based on research and publications, including finding from EU-HYBNET project and reports from European Centre of Excellence for Countering Hybrid Threats, authors point out following areas as most relevant in a short and medium term:

- cyber attacks (including AI driven attacks, and lack of IoT security);
- quantum technology (especially post-quantum cryptography transition and vulnerabilities related to it);
- critical raw materials and supply chain security (batteries, semiconductors, telecommunications);
- physical threats (fires, drones);
- satellites;
- special care on energy resilience;
- secure telecommunications (5G but also 6G).

Due to the rapid development of technologies, geopolitical instability and changing the societies perception around the world, it is difficult to predict and accurately foresee all future risks. Additionally, these areas should be also included in future projects and innovative activities:

- enhance real time joint cyber and physical threat monitoring and real-time threat intelligence sharing;
- joint exercises across EU;
- engaging with global standardisation organisations, to ensuring EU priorities on secure-by-design infrastructure, ethical AI, and privacy-first cyber security are reflected in global standards;
- increasing public-private partnerships with technology providers;

[35] K. Kieslich, M. Lünich, *Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations*, preprint, https://arxiv.org/abs/2401.13605v3 [accessed: 7.02.2025]. https://doi.org/10.48550/arXiv.2401.13605.

- cooperation with trusted EU partners including the UK, US, Canada, Japan, South Korea and Australia.

Conclusions

The protection of CI remains a cornerstone of European security policy, particularly in the face of evolving hybrid threats. The European Union is making relevant effort in funding innovation initiatives aimed at strengthening the resilience of CI. Projects such as: EU-HYBNET, EU-CIP, VIGIMARE, TESTUDO, TRANSCEND, NBSINFRA, and ENDURANCE show the extent of efforts to enhance security involving the development of technology, policy coordination, and cross-border collaboration.

One of the conclusions from this analysis is the increasing complexity of threats facing CI operators. The convergence of cyber and physical security risks, difficulties due to differing national regulations and inconsistent interpretations of EU directives across EU Member States, and the challenges of balancing innovative projects with their implementation all emphasise the need for sustained research and development efforts. While Horizon Europe project and other funding mechanisms have provided great support, additional financial and strategic resources are required to maintain the EU's leadership in infrastructure resilience.

Another significant insight is the necessity of fostering stronger cooperation among stakeholders. The projects reviewed in this article demonstrate the importance of integrating perspectives from industry, academia, public authorities, and civil society. Fostering more agile and adaptive partnerships will be essential to keep pace with the rapidly evolving threat landscape. Additionally, ensuring that research findings are translated into practical applications will require closer alignment between policymakers, technology developers, and infrastructure operators.

The next phase of research and policy development should focus on enhancing resilience through strategic foresight, technological innovation, and cross-sector collaboration. In this way, the EU can ensure that its CI remains resilient to future threats, thereby protecting the security and stability of societies on the continent.

The authors believe that it is worth monitoring and analysing whether and how the outcomes of projects described in the article have been implemented in practice.

Bibliography

Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses, OECD Publishing, Paris 2021. https://doi.org/10.1787/8fa190b5-en.

Internet sources:

Autonomous Swarm of Heterogeneous resources in infrastructure protection via threat prediction and prevention, European Commission, https://cordis.europa.eu/project/id/101121258 [accessed: 15.01.2025].

Citynature-based Solutions integration to local urban infrastructure protection for a climate resilient society, https://cordis.europa.eu/project/id/101121210 [accessed: 17.01.2025].

Critical infrastructure resilience at EU-level, European Commission, 23.09.2024, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en [accessed: 6.01.2025].

Empowering a Pan-European Network to Counter Hybrid Threats, European Commission, https://cordis.europa.eu/project/id/883054 [accessed: 13.01.2025].

ENDURANCE, https://endurance-horizon.eu/ [accessed: 17.01.2025].

EU-CIP, https://www.eucip.eu/ [accessed: 13.01.2025].

EU-HYBNET, https://euhybnet.eu/ [accessed: 13.01.2025].

European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection, European Commission, https://cordis.europa.eu/project/id/101073878 [accessed: 13.01.2025].

Horizon Europe, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en [accessed: 7.01.2025].

Horizon Europe. Strategic Plan 2025–2027, European Commission, 2024, https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/6abcc8e7-e685-11ee-8b2b-01aa75ed71a1 [accessed: 7.01.2025].

Horizon Europe. Strategic Plan 2025–2027. Analysis, European Commission, 2023, https://op.europa.eu/en/publication-detail/-/publication/b3baec75-fdd0-11ed-a05c-01aa75ed71a1/language-en [accessed: 9.01.2025].

Horizon Europe. Work Programme 2023-2025. 6. Civil Security for Society (European Commission Decision C(2024) 2371 of 17 April 2024), https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf [accessed: 10.01.2025].

Joint Staff Working Document. Eighth progress report on the implementation of the 2016 Joint framework on countering hybrid threats and the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats, https://defence-industry-space.ec.europa.eu/system/files/2025-01/SWD_Annual-Progress-Report-2024.PDF [accessed: 2.01.2025].

Kieslich K., Lünich M., *Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations*, preprint, https://arxiv.org/abs/2401.13605v3 [accessed: 7.02.2025]. https://doi.org/10.48550/arXiv.2401.13605

NATO and European Union release final assessment report on resilience of critical infrastructure, NATO, 29.06.2023, https://www.nato.int/cps/en/natohq/news_216631.htm [accessed: 6.01.2025].

NBSINFRA, https://nbsinfra.eu/ [accessed: 17.01.2025].

Resilient Infrastructures, https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/resilient-infrastructures_en [accessed: 10.01.2025].

Strategic plan, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/strategic-plan_en [accessed: 3.01.2025].

Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe, European Commission, https://cordis.europa.eu/project/id/101168007 [accessed: 17.01.2025].

Szymański P., *Towards greater resilience: NATO and the EU on hybrid threats*, Ośrodek Studiów Wschodnich, 24.04.2020, https://www.osw.waw.pl/en/publikacje/osw-commentary/2020-04-24/towards-greater-resilience-nato-and-eu-hybrid-threats [accessed: 7.02.2025].

TESTUDO, https://testudo-project.eu/ [accessed: 15.01.2025].

The Commission calls on 23 Member States to fully transpose the NIS2 Directive, European Commission, 28.11.2024, https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive [accessed: 29.01.2025].

The cybersecurity challenges of legacy OT and how to manage them, Control Engineering, 21.03.2024, https://www.controleng.com/the-cybersecurity-challenges-of-legacy-ot-and-how-to-manage-them [accessed: 7.02.2025].

TRANSCEND, https://www.transcend-logistics.eu/ [accessed: 17.01.2025].

Transport resilience against Cyber and Non-Cyber Events to prevent Network Disruption, European Commission, https://cordis.europa.eu/project/id/101168023 [accessed: 17.01.2025].

Vigilant Maritime Surveillance of Critical Submarine Infrastructure, European Commission, https://cordis.europa.eu/project/id/101168016 [accessed: 14.01.2025].

VIGIMARE, https://vigimare.eu/ [accessed: 15.01.2025].

Legal acts

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 (NIS 2 Directive) – (Official Journal of the EU L 333/164 of 27.12.2022).

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 – (Official Journal of the EU L 333/80 of 27.12.2022).

Council Recommendation of 25 June 2024 on a Blueprint to Coordinate a Response at Union Level to Disruptions of Critical Infrastructure with Significant Cross-Border Relevance (Official Journal of the EU C 2024/4371 of 5.07.2024).

Małgorzata Wolbach

Senior Project Officer in the Polish Platform for Homeland Security (PPBW). Master's degree in Homeland Security and Bachelor's degree in Criminology in the Police Academy in Szczytno. At PPBW she is responsible for the implementation and realisation of projects funded by EU programmes, with a particular focus on projects addressing hybrid threats and the security of public spaces.

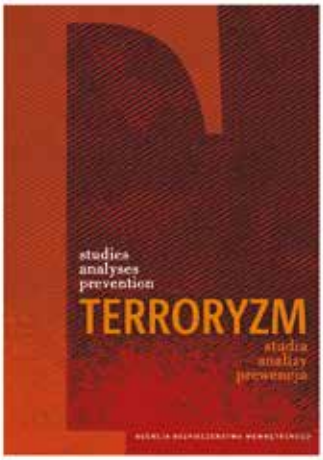
Contact: malgorzata.wolbach@ppbw.pl

Rashel Talukder

Managing Director of the Polish Platform for Homeland Security (PPBW). Since 2009 he has been actively involved in security research and development in Poland and Europe, including as coordinator of European projects. He was also involved in local community affairs as a municipal councillor of Stęszew (2018–2024).

Contact: rashel.talukder@ppbw.pl

INTERNAL SECURITY AGENCY
PUBLISHING HOUSE



The Publishing House of the Internal Security Agency, launched in 2009, issues peer-reviewed scientific monographs devoted to, inter alia, the history of Polish secret services and broadly understood legislative matters as well as publications concerning statutory tasks of the Internal Security Agency. It is also the publisher of two scientific journals: "Internal Security Review" and "Terrorism – Studies, Analyses, Prevention".

The biannual "Internal Security Review" is a scientific journal published since 2009 with a focus on interdisciplinary issues related to the protection of the constitutional order of the state. The topics of the articles cover a wide range of areas related to national security, e.g. legal issues, activities of institutions and organizations responsible for the protection of the constitutional order of the state as well as analyses of current and projected security status in the national and international perspectives.

The biannual "Terrorism – Studies, Analyses, Prevention" is a scientific journal established in 2021, devoted to interdisciplinary issues related to anti-terrorist protection and building resilience to terrorist threats in the national and international perspectives. It is meant to be a platform for the exchange of scientific ideas and experience, connecting the academic world and representatives of institutions and services that cooperate with each other within the Interministerial Team for Terrorist Threats, which is the coordination centre of the anti-terrorist system of the Republic of Poland.

Authors of the articles are officers of the Internal Security Agency and other uniformed services of the Republic of Poland, academics from universities, scientific institutions and research centers as well as specialists in fields related to the history of special services and the protection of national security.

Since July 2021, the Publishing House of the Internal Security Agency has been included in the Polish ministerial list of publishers issuing peer-reviewed scientific monographs. Number of points – 80 (LEVEL I).

For further information concerning the Publishing House of the Internal Security Agency, including terms of cooperation, please visit: www.abw.gov.pl/pub/.