EU-CIP Policy Brief

Kacper Murawa, PPHS
September, 2025

"Building the Resilience of Critical Infrastructure to Threats through Standardisation and Auditing – Conclusions from the EU-CIP project"

Based on a workshop of the same name organised on September 4th 2025 by Polish Platform for Homeland Security

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

General Conclusions

- Greater adaptability and flexibility

It is essential that critical infrastructure adapts more effectively to new types of threats, whether physical, digital or hybrid. Existing response schemes often fail to keep pace with the rate of change and require a thorough update.

- Shortening response Times

The speed of response to incidents and disruptions is one of the key weaknesses of the current system. Countries should improve their processes for detecting, reporting and responding to threats.

- Transparency and effective coordination

There is still too little information exchange between countries, sectors, operators and administrations. Common standards and an interoperable framework are needed to ensure a consistent approach to infrastructure protection and resilience.

- Modern technologies and tools

Solutions such as digital twins, anomaly detection, cascading effects analysis, machine learning and cyber-physical threat detection tools should be used to better secure infrastructure.

- Gaps in legislation and its implementation

The transposition of the CER Directive into national law continues to face delays. Differences in the identification and assessment of critical entities lead to varying levels of security in different countries.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

- Poor use of research and innovation results

EU projects generate valuable technologies and analyses, but these are rarely actually implemented in practice or transformed into new standards and policies. There is a lack of mechanisms to ensure the sustainability and usefulness of these results after the project has ended.

- Public-private partnerships (PPPs)

Operators, technology providers and the private sector should be actively involved in the development of policies and standards, rather than just being recipients of them. A clear legal and regulatory framework for this type of cooperation is essential.

- Resilience already at the design stage

Resilience to various threats – both physical and digital – should be taken into account when designing new infrastructure elements. The modernisation of older systems is also a priority, as they are often the weakest link.

- Better monitoring and evaluation mechanisms

Measurable performance indicators (e.g. response time, service availability, number of incidents) should be established and their achievement reported regularly, both at national and EU level. Greater publicity for research and innovation results is also desirable.

- Joint stress tests and exercises

Resilience tests and joint exercises should cover critical infrastructure of cross-border importance and involve different sectors. It is also worth developing scenarios and response plans involving several countries.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Conclusions for EU Member States

- Priority transposition of the CER Directive

Countries should ensure that national legislation is consistent with CER requirements and that the identification of critical entities is carried out in a timely and effective manner.

- Strengthening institutions

It is important to clarify competences and responsibilities at every level (central, local, private), as well as to ensure adequate resources and a clear division of roles in the event of an incident.

- Investment in new technologies and innovation

The development and implementation of modern infrastructure protection solutions should be supported – through subsidies, tax breaks and partnerships with the scientific sector.

- International cooperation and knowledge exchange

It is worth actively participating in networks such as EU-CIP, sharing good practices and taking part in joint exercises.

- Financial support and market incentives

Funding for modernisation, innovation and projects should be secured from both EU and national sources. Tax breaks, simplification of regulations and acceleration of procedures will also be helpful.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Conclusions for EU-CIP

- Focus on the real needs of users

It is essential to consult infrastructure operators and local and national authorities on project activities so that the solutions developed actually respond to real challenges.

- Pilots and demonstrators

It is worth presenting new solutions in practice to gain credibility and encourage their implementation.

- Standardisation and certification

Solutions developed within the project should comply with current and future EU standards. It is important to certify them and ensure their interoperability.

- Sustainability of project results

Already at the implementation stage, it is necessary to plan how to maintain the results achieved after the end of the project – e.g. through institutions, knowledge centres or permanent data platforms.

- Measuring results and communication

It is worth clearly defining what will be the measure of the project's success (e.g. the number of better protected entities, reduction in response time). It is also important to report transparently and share all results, including those that are less successful.

- Designing for resilience

New initiatives should take resilience into account from the outset – by anticipating possible disruptions, mitigating risks, building redundancy and ensuring system flexibility.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Consortium:

- Engineering – Ingegneria Informatica SPA (ENG), Italy
- Deutsches Zentrum für Luft und Raumfahrt EV (DLR), Germany
- GFT Italia SRL (GFT), Italy
- Inov instituto de engenharia de sistemas e computadores inovacao (INOV), Portugal
- Inlecom commercial pathways company limited by guarantee (ICP), Ireland
- SINTEF AS (SIN), Norway
- Steinbeis EU-VRI GMBH (EU-VRi), Germany
- Stowarzyszenie Polska Platforma bezpieczenstwa wewnetrznego (PPHS), Poland
- Laurea – Ammattikorkeakoulou oy (LAU), Finland
- Innov - Acts Limited (INNOV), Cyprus
- Norks Regnesentral (NRS), Norway
- European Organisation for Security (EOS), Belgium
- Katholieke Universiteit Leuven (KUL), Belgium
- Fstechnology SPA (FST), Italy
- Athens International Airport S.A (AIA), Greece
- Fundacion de la Comunidad Valenciana para la investigacion, promocion y estudios comerciales de Valenciaport (FV), Spain
- Orange Romania (ORO), Romania
- Electricité de France (EDF), France
- Association française de normalisation(AFNOR), France
- Leonardo Societa per Azioni (LDO), Italy

Join Us

https://www.eucip.eu/
@EUCIP_HorizonEu
@EU-CIP Project

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessary reflect those of the European Union or the European Commission. Neither the European Union no the granting authorities can be held responsible for them.