Tools and processes to support stress tests of critical infrastructure

HORIZON-CL3-2026-01-INFRA-01

Program:	**Horizon Europe Cluster 3**
Típus:	**Innovation Action**
TRL szint:	**6-8**
Támogatás projektenként:	**4,835M EUR**
Támogatott projektek száma:	**2**
Pályázati felület megnyílik:	**6 May 2026**
Beadási határidő:	**5 November 2026**
Felhívás linkje:	LINK

The objective of this topic is to facilitate the stress testing of critical infrastructure by providing specialized tools and methodologies and support validation.
The proposed solutions may, among others, support simulation and modelling, multi-hazard and multi-threat scenario building, data analytics, including geospatial information, assessment of risks and adaptive capabilities, as well as impact of human factors. These solutions should be designed to be inclusive and accessible, considering the needs of diverse users and stakeholders. Solutions should allow flexible configuration taking into account the evolving nature of threats and hazards. If feasible they should also be adaptable to different sectors and should support stress testing under diverse environmental and geographical conditions, including operation in harsh and remote environments. Moreover, they need to comply with the relevant legislative frameworks and allow application of the developed tools under the current regime taking into account the sensitivity and confidentiality of the processed information.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu

Security challenges of the green transition in urban und peri urban areas

HORIZON-CL3-2026-01-INFRA-02

Program:	**Horizon Europe Cluster 3**
Típus:	**Research & Innovation Action**
TRL szint:	**6-8**
Támogatás projektenként:	**4M EUR**
Támogatott projektek száma:	**1**
Pályázati felület megnyílik:	**6 May 2026**
Beadási határidő:	**5 November 2026**
Felhívás linkje:	LINK

Proposals submitted under this topic should investigate the integration of sustainable & environmentally friendly technologies into urban and peri-urban areas to identify and explore physical and cyber risks and vulnerabilities resulting from this phenomenon, including, but not limited to: battery fires, toxic leaks, electric shocks, structural integrity, toxic waste, data privacy, land management disruptions, including potential negative impacts on the natural environment, or social and community tensions. The proposed inquiry should also consider the threat of malicious access, software and data manipulation and misuse of managing systems potentially leading to harm to health, loss of life, environmental damage or economic damage, regardless of whether the intention is criminal, vandalism, hybrid attack or other.

The ultimate goal of this research is to inform operators, first responders and authorities on how to mitigate risks, enhance their preparedness and improve their response to potential incidents.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu

Targeted innovative capabilities for the resilience of critical entities to natural and human-induced disasters, including hybrid scenarios

HORIZON-CL3-2026-01-INFRA-03

Program:	**Horizon Europe Cluster 3**
Típus:	**Innovation Action**
TRL szint:	**6-8**
Támogatás projektenként:	**5M EUR**
Támogatott projektek száma:	**2**
Pályázati felület megnyílik:	**6 May 2026**
Beadási határidő:	**5 November 2026**
Felhívás linkje:	LINK

This topic aims to support the development and demonstration of targeted high-tech capabilities that address specific preparedness, operational, and recovery gaps in the resilience of critical entities under multi-hazard and NaTech+ conditions.

Proposals should be grounded in existing risk assessments and draw on lessons learned from recent disruptive events. They are expected to deliver measurable improvements in both technological and organisational resilience through the identification and prioritisation of critical capability gaps, especially where cascading and cross-sectoral risks are likely to arise.

Proposals should also demonstrate cross-border, multi-actor coordination mechanisms through simulations or testing in real operational environments, involving public authorities, emergency responders, and critical service operators or representative environments where critical infrastructure is particularly exposed to multi-hazard risks.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu

Enhancing physical protection of critical infrastructures

HORIZON-CL3-2027-01-INFRA-01

Program:	**Horizon Europe Cluster 3**
Típus:	**Innovation Action**
TRL szint:	**6-7**
Támogatás projektenként:	**6M EUR**
Támogatott projektek száma:	**2**
Pályázati felület megnyílik:	**5 May 2027**
Beadási határidő:	**4 November 2027**
Felhívás linkje:	LINK

Physical protection of critical infrastructure should keep up its advancement to match risks and hazards stemming from malicious use of new and emerging technologies, and evolving operational environment, as well as improve its safety and security measures against knowns and emerging threats.

Proposals submitted under this topic should identify and analyse possible new challenges for the physical security of the critical entities and develop adequate tools, recommendations, manuals and training programmes for relevant operators and authorities. Where relevant for their scope proposals should utilise the nature-based solutions and respect principles of biodiversity. Furthermore, solutions should take into account interdependencies in the context of supply chains and their impact on physical protection.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu

Impact of malicious use of Open-Source Intelligence on critical infrastructure business continuity

HORIZON-CL3-2027-01-INFRA-02

Program:	Horizon Europe Cluster 3
Típus:	Innovation Action
TRL szint:	8
Támogatás projektenként:	3,835M EUR
Támogatott projektek száma:	2
Pályázati felület megnyílik:	5 May 2027
Beadási határidő:	4 November 2027
Felhívás linkje:	LINK

Proposals submitted under this topic should analyse the type, amount and accessibility of publicly available information and their usefulness in planning hostile operations against critical entities and their services. They should also parse the role of OSINT for identification and recruitment of insiders, identity theft, impersonation, or launching a psychological operations such as propaganda, foreign information manipulation and interference or disinformation, moreover. Moreover, the implications of AI data processing to misuse OSINT potential should be addressed. Any potential OSINT sources should be covered including, but not limited to social media, online fora, cloud resources, public records and databases, lawfully accessible deep web and dark web data, geospatial information, as well as paper archives in the public domain with blueprints, emergency response plans or similar. Proposals should especially consider scenarios including hybrid threats and lone wolves and develop tools and awareness campaigns to mitigate such threats.

NKFIH Horizont Európa NCP Csapat

ncp@nkfih.gov.hu

Horizont Europa NCP Magyarország

horizonteuropa.nkfih.gov.hu