HORIZON EUROPE CLUSTER 3 AKTUÁLIS FELHÍVÁSAI

Schultheisz Máté (mate.schultheisz@nkfih.gov.hu)
Nemzeti Kapcsolattartó Pont (NCP)

2024. augusztus 27.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal

3. klaszter – Polgári biztonság a társadalomért

- 6 desztináció
- A **3. klaszter** munkaprogramja az EU **biztonsági, kiberbiztonsági, katasztrófa-kockázat csökkentési és ellenálló képesség növelési prioritásait** támogatja.
- Cél:
  - megelőzés, felkészültség és válságkezelés erősítése;
  - hozzájárulás egy **ellenálló, biztonságos és demokratikus társadalom** kialakításához, valamint a digitális technológiák biztonságához.
- A projektek új tudást, technológiákat és megoldásokat fejlesztenek.
- A polgárok és közösségek bevonása szükséges a biztonsági technológiák társadalmi hatásainak értékeléséhez, a közbizalom növeléséhez és a társadalmi innovációk integrálásához.

1. Desztináció – Az EU és polgárai hatékonyabb védelme a bűnözéssel és a terrorizmussal szemben

- A javasolt témák hozzájárulhatnak az alábbi hatások eléréséhez:
  - modern **információelemzés** a rendőrség számára, a bűnözők és terroristák elleni küzdelemhez;
  - fejlettebb **kriminalisztika** és jogszerű bizonyítékgyűjtés, a bűnözők elfogására és bíróság elé állítására;
  - a **bűncselekmények**, beleértve a kiberbűnözést és a terrorizmust, **megelőzésének, felismerésének és elrettentésének javítása**;
  - a **polgárok biztonságának növelése** a terrorizmus ellen, különösen nyilvános helyeken;
  - jobb hírszerzés és szervezett bűnözés elleni védelem;
  - **biztonságosabb kibertér** a polgárok, különösen a gyermekek számára.
- A javaslatoknak magukban kell foglalniuk a rendőrségi hatóságok bevonását, gyors alkalmazkodási stratégiákat, moduláris eszközöket, a gyakorlati igényekhez igazított fejlesztéseket, előző projektekre építést, a polgárok és közösségek aktív részvételét, oktatási és képzési elemeket, valamint az eredmények átvételének stratégiáját.
- 8 felhívás; 41,7 millió EUR

Fighting Crime and Terrorism

- Mitigating new threats and adapting investigation strategies in the era of Internet of Things – link
- Open Topic – link
  - Proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive forensic solutions for fighting crime and terrorism
- Lawful evidence collection in online child sexual abuse investigations, including undercover – link
- Radicalisation and gender - link
- Combating hate speech online and offline - link
- Open Topic – link
  - Proposals are welcome to address both existing and upcoming challenges in fighting crimes strongly influenced by cultural and/or societal issues
- CBRN-E detection capacities in small architecture - link
- Tracing of cryptocurrencies transactions related to criminal purposes - link

2. Desztináció – Az EU külső határainak hatékony védelme

- A javaslatoknak az alábbi hatások eléréséhez kell hozzájárulniuk:
  - az EU **határbiztonságának javítása**, költség- és energiahatékonyabb kezelés mellett, beleértve a tengeri környezetet és az infrastrukturális tevékenységeket, valamint a polgári biztonságot a balesetek, természeti katasztrófák és biztonsági kihívások ellen;
  - **határátlépési élmény javítása** az utazók és a hatóságok számára, miközben fenntartják a biztonságot, támogatva a schengeni térséget, csökkentve az illegális mozgásokat és védve az utazók alapvető jogait;
  - **vám- és ellátási lánc biztonságának javítása** az illegális tevékenységek megelőzésével, felismerésével és elrettentésével, valamint a kereskedelmi zavarok minimalizálásával.
- 5 felhívás; 29 millió EUR

Effective management of EU external borders

- Open Topic – link
  - Proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions within this Destination
- Interoperability for border and maritime surveillance and situational awareness - link
- Advanced user-friendly, compatible, secure identity and travel document management - link
- Integrated risk-based border control that mitigates public security risk, reduces false positives and strengthens privacy - link
- Detection and tracking of illegal and trafficked goods - link

3. Desztináció – Ellenálló infrastruktúra

- A javaslatoknak az alábbi hatások eléréséhez kell hozzájárulniuk:
  - **nagyszabású összekapcsolt rendszerek infrastruktúrájának** és az azokat üzemeltető entitásoknak az ellenálló képességének **biztosítása** összetett támadások, járványok, természeti és ember okozta katasztrófák vagy a klímaváltozás hatásai esetén;
  - **frissített rendszerek** az üzemeltetők ellenállóképességéhez és **a kritikus infrastruktúra védelméhez**, lehetővé téve a gyors, hatékony, biztonságos és emberi beavatkozás nélküli reagálást összetett fenyegetések és kihívások esetén, valamint a kockázatok jobb felméréséhez, biztosítva az európai infrastruktúrák ellenálló képességét és nyitott stratégiai autonómiáját;
  - **ellenálló és biztonságos okos városok védelme**, a kritikus infrastruktúrák és rendszerek védelméből származó tudás felhasználásával, amelyek egyre összetettebbé válnak.
- 3 felhívás; 16 millió EUR

Resilient Infrastructure

- Open Topic – link
  - Proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for increasing the resilience of critical infrastructure
- Resilient and secure urban planning and new tools for EU territorial entities - link
- Advanced real-time data analysis used for infrastructure resilience - link

4. Desztináció – Fokozott kiberbiztonság

- A pályázatoknak hozzá kell járulniuk az alábbi hatások közül egy vagy több eléréséhez:
  - az EU kiberbiztonsági kapacitásainak és az Európai Unió szuverenitásának megerősítése a digitális technológiák terén;
  - **ellenállóbb digitális infrastruktúrák**, rendszerek és folyamatok;
  - **fokozott s**zoftver-, hardver- és **ellátási lánc-biztonság;**
  - biztonságosabbá váló, bomlasztó technológiák;
  - intelligens és számszerűsíthető biztonsági biztosíték és tanúsítás, amelyet az egész EU-ban megosztanak;
  - megerősített tudatosság, valamint közös kiberbiztonsági irányítás és kultúra.
- 2 felhívás; 60, 4 millió EUR

Increased Cybersecurity

- Approaches and tools for security in software and hardware development and assessment - link
- Post-quantum cryptography transition - link

5. Desztináció – Katasztrófákkal szemben ellenálló európai társadalom

- A javaslatoknak az alábbi hatások eléréséhez kell hozzájárulniuk:
  - a **legújabb tudományos eredmények és integrált technológiák jobb kihasználása** a katasztrófák megértésében és kezelésében;
  - a polgárok bevonása a kutatásokba, növelve az európai társadalom ellenállóképességét;
  - **fokozott együttműködés és párbeszéd** a tudományos közösség és az első és második válaszadók között, gyorsítva az eredmények gyakorlatba való átültetését;
  - **egységesített és interoperábilis irányelvek**, protokollok és eszközök támogatása a válságkezelésben;
  - **javított hatáselőrejelző képesség** és forgatókönyv-építés a kritikus entitások stressztesztelésére;
  - az intézmények és **szakemberek jobb felkészítése** a természeti katasztrófákra, amelyek gyakorisága és súlyossága nőtt a klímaváltozás miatt;
  - javított mentési és vészhelyzetkezelési képességek extrém éghajlati események és geológiai veszélyek esetén.
- 5 felhívás; 30 millió EUR

Disaster-Resilient Society

- Prevention, detection, response and mitigation of chemical, biological and radiological threats to agricultural production, feed and food processing, distribution and consumption - link
- Open Topic – link
  - Proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for enhanced interactions among the scientific community, practitioners, city's risk managers of major crises and citizens or local communities in the event of (natural or man-made) disasters
- Harmonised / Standard protocols for the implementation of alert and impact forecasting systems as well as transnational emergency management in the areas of high-impact weather / climatic and geological disasters - link
- Hi-tech capacities for crisis response and recovery after a natural-technological (NaTech) disaster – link
- Cost-effective sustainable technologies and crisis management strategies for RN large-scale protection of population and infrastructures after a nuclear blast or nuclear facility incident - link

6. Desztináció – Megerősített biztonsági kutatás és innováció

- A javaslatoknak az alábbi hatások eléréséhez kell hozzájárulniuk:
  - az **EU polgári biztonsági képességeinek hatékonyabb és eredményesebb**, bizonyítékokon és tudáson alapuló **fejlesztése**, amely egy erősebb és szisztematikusabb biztonsági kutatási és innovációs ciklusra épül;
  - a keresleti és kínálati piac szereplői közötti **fokozott együttműködés**, beleértve a más területek szereplőivel való együttműködést is, amely elősegíti a biztonsági kutatás sikeres eredményeinek gyors iparosítását, kereskedelmi forgalomba hozatalát, elfogadását és alkalmazását, valamint erősíti az EU biztonságtechnológiai és ipari bázisának versenyképességét és rugalmasságát, és biztosítja a kritikus biztonsági területeken az EU-termékek ellátásbiztonságát.
- 2 felhívás; 16,6 millió EUR

Support to Security Research and Innovation

- Demand-led innovation through public procurement - link
- Accelerating uptake through open proposals for advanced SME innovation - link

Hasznos linkek

- Partnerkeresés:
  - https://security-research-map.b2match.io/
- Munkaprogram:
  - 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

HORIZON-CL3-2024-FCT-01-01

Mitigating new threats and adapting investigation strategies in the era of Internet of Things

Research & Innovation Action | TRL 5-6 | 5M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The successful proposal should help Police Authorities understand the implications of the fast-developing IoT environment in order to keep pace with the evolution of its applications, recognise and tackle the emerging (digital and especially physical) threats that this may pose.
- New investigating schemes are needed for Police Authorities to access and exploit IoTs evidence, in compliance with EU values. To this end, the proposal should examine the extent to which, e.g., modern vehicle models, smart TVs, private surveillance systems, virtual assistants or voice control systems can be considered as sources of evidence for the collection and analysis of data, as well as how such data can be used for deriving indicators of an imminent threat.
- The research should assess legal, organisational and technical implications of IoT development in the context of investigations, including e.g. privacy issues, and propose strategies, including training materials, tools and path to standards that would foster "by design" a lawful access to relevant evidence.
- The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects as well as create synergies with similar ongoing security research projects from the Calls 2021-2022 on Fighting Crime and Terrorism and on Increased Cybersecurity.

HORIZON-CL3-2024-FCT-01-02

Open Topic

Research & Innovation Action | TRL 5-7 | 4,5M EUR/project | 2 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive forensic solutions for fighting crime and terrorism, that are not covered by the other topics of Horizon Europe Calls Fighting Crime and Terrorism 2021-2022, Fighting Crime and Terrorism 2023 and Fighting Crime and Terrorism 2024.
- Proposals should convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. Proposals should also delineate the plans to develop possible future uptake and upscaling at national and EU level for possible next steps after the research project.

HORIZON-CL3-2024-FCT-01-03

Lawful evidence collection in online child sexual abuse investigations, including undercover

Research & Innovation Action | TRL 5-6 | 3,7M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Research in this area should tackle legislative frameworks to collecting evidence in online, including undercover, investigations of child sexual abuse, leading to guidelines and manuals that would make the capability available across the EU to target these offenders more effectively.
- The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects as well as create synergies with similar on-going security research projects from the Calls 2021-2022 on Fighting Crime and Terrorism.
- Since the use of undercover agents online could be beneficial in other crime areas too, particularly in counter terrorism, analysis of possibilities for the developed approaches to be adapted to these other crime areas would be welcome.
- This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise.

HORIZON-CL3-2024-FCT-01-04

Radicalisation and gender

Research & Innovation Action | TRL 5-6 | 3M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Projects' results are expected to contribute to some or all of the following outcomes:
  - Improved understanding of motivation of women and girls for supporting extremist ideologies, such as grievance and stigmatisation;
  - Improved understanding of the role of masculinity in men and boys' motivation for the support of extreme ideologies;
  - Better understanding of the group dynamics at play during processes of radicalisation, including factors for factionalism and potential splinters in terrorist organisations;
  - Development of strategies aimed at enhancing the use of motivation factor in detection, prevention and de-radicalisation efforts;
  - European Police Authorities, Prison Authorities, social care workers, teachers and other P/CVE practitioners benefit from modern and validated tools, skills and training curricula to identify early symptoms of radicalisation;
  - Identification and assessment of best practices that are transferable across Member States improving and developing modules and trainings, strengthening adaption of local community policing in diverse communities; and
  - Design girls and women's empowerment approaches through legal, financial and/or cultural means aimed at tackling the root causes of radicalisation and extremism.

HORIZON-CL3-2024-FCT-01-05

Combating hate speech online and offline

Innovation Action | TRL 6-7 | 3M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The successful proposal is expected to reinforce hate crime training and capacity building for Police Authorities and other relevant security practitioners, in particular to enhance their tools and methods for lawful detection, reporting and data/evidence collection and analysis of the hate speech related activities that are considered as crime or could lead to a crime, notably the ones supported by advanced digital technologies, such as in emerging cyber environments.
- The successful proposal is expected to build on previously developed tools for related applications (such as text and image matching).
- The successful proposal should also support the implementation of the voluntary Code of Conduct on countering illegal hate speech online that the European Commission initiated in 2016 with IT companies.
- The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects.
- This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise.

HORIZON-CL3-2024-FCT-01-06

Open Topic

Research & Innovation Action | TRL 5-6 | 3M EUR/project | 2 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Projects' results are expected to contribute to all of the following outcomes:
  - Building Police Authorities' capabilities to identify, prevent and investigate major contemporary and/or emerging criminal activities;
  - Development of tools, methods or manuals for Police Authorities, improving their effectiveness in detecting crimes, collecting evidence and investigating cases of major contemporary and/or emerging criminal activities;
  - Development of training curricula, for Police Authorities, prosecutors, as well as judicial actors on major contemporary and/or emerging criminal activities, raising their awareness about impact of cultural and societal issues on the categories of crime and/or violence under consideration.
- Proposals are welcome to address both existing and upcoming challenges in fighting crimes strongly influenced by cultural and/or societal issues that are not covered by the other topics of Horizon Europe Calls Fighting Crime and Terrorism 2021-2022, Fighting Crime and Terrorism 2023 and Fighting Crime and Terrorism 2024.
- This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise.

HORIZON-CL3-2024-FCT-01-07

CBRN-E detection capacities in small architecture

Innovation Action | TRL 6-8 | 6M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects, as well as seek to exploit potential synergies with the successful proposal(s) funded under HORIZON-CL3-2024-BM-01-05.
- In recent years, in some pilot actions some street furniture, including bins and bus shelters have become smart as they have been equipped with environmental sensors, wireless modules, or microcontrollers becoming part of the IoT infrastructure, and one of the components of the future smart cities. Proposals should focus on exploitation and integration of existing sensors within the public space small architectures. Traditional sensors and surveillance platforms like the Automatic Number-Plates Recognition (ANPR), cameras or image analysis systems are not in the scope of this topic unless their integration with new sensors is considered, and the added value of networked systems demonstrated.
- Proposals should present relevant challenges and opportunities for future applications of CBRN-E detection capacities in small architecture, including prospects of scalability, real-time processing, and cooperation of networked systems.

HORIZON-CL3-2024-FCT-01-08

Tracing of cryptocurrencies transactions related to criminal purposes

Innovation Action | TRL 6-7 | 6M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The future of cryptocurrencies and the extent to which criminals and terrorists will use them will depend on factors such as anonymity, future regulation, law enforcement activities and security of the systems. Innovation should explore these considerations and propose mitigation measures, from legal, organisational, and technical perspectives (including the development of tools and relevant trainings to enhanced tractability of cryptocurrencies transactions. Proposals should also propose cooperation model(s) and tools for the exchange of information between relevant authorities.
- The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects. Coordination among the successful proposal from this topic as well as with the successful proposals under topic HORIZON-CL3-2023- FCT-01-06.

HORIZON-CL3-2024-BM-01-01

Open Topic

Research & Innovation Action | TRL 4-6 | 3M EUR/project | 2 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions within this Destination that are not covered by the other topics in Horizon Europe Calls Border Management 2021-2022, Border Management 2023 and Border Management 2024.
- Adapted to the nature, scope, type and target TRL of proposed projects, proposals should convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions.
- Proposals should be convincing in explaining the methods they intend to use for demonstrating, testing or validating the proposed tools and solutions.
- Proposals should also delineate the plans to develop possible future follow-up research and development and/or uptake and upscaling at national and EU level for possible next steps after the research project.

HORIZON-CL3-2024-BM-01-02

Interoperability for border and maritime surveillance and situational awareness

Innovation Action | TRL - | 6M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The proposed solution(s) should allow improved interoperability (at both back-end and frontend levels), independently of the supplier of the equipment, and ideally interchangeability that enables exchange of information among authorities that use different systems. Compatibility and integration with other information sharing environments, including the Common Information Sharing Environment (CISE) is essential in order to support the cross-sectoral and cross-border exchange of information.
- The proposed solution(s) should enable simultaneous connection of different sensors (or of different data, or of different assets, depending by the module) by different suppliers, the flexible tasking and monitoring of surveillance assets like RPAS, and the visualization and manipulation of the data in a single user interface in a seamless way. This will support practitioners to exploit their technology stack in an agnostic way.
- The proposed solution(s) should allow for seamless connectivity between C2 systems from different authorities, and at different coordination levels; include cybersecurity measures and information access segregation capabilities; include concepts of operation, standard operating procedures and common lexicon for joint operations using interoperable systems through the proposed solution(s).

HORIZON-CL3-2024-BM-01-03

Advanced user-friendly, compatible, secure identity and travel document management

Innovation Action | TRL - | 6M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- This topic aims at exploring and developing enhanced capabilities for securely managing digitalised travel documents used for travel across external borders. The proposed solution should be compatible with planned or possible future EU highly digitalised travel documents formats and travel facilitation systems, and with applicable ICAO current and upcoming schemes.
- The proposed solutions should be compatible or interoperable with relevant existing digitalised travel documents systems. The proposed solutions should also respect fundamental rights such as privacy and protection of personal data, apply privacy by design of the application and use privacy-enhancing technologies.
- The operational applicability focus should be on highly digitalised travel documents and "digital identity management" used for travel across external borders. However, the research should include enhancing the security of breeder documents, which risk being "weak links" when they are used to obtain genuine, secure travel documents.

HORIZON-CL3-2024-BM-01-04

Integrated risk-based border control that mitigates public security risk, reduces false positives and strengthens privacy

Innovation Action | TRL - | 5M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The solution(s) proposed under this topic should allow easier and more flexible allocation and change of resources in border checks, for example to meet seasonal peaks. A proposed solution should help perform border checks, as well improve the speed for detecting threats in vehicles, such as weapons and explosives, without people coming out of vehicles and without slowing down (dis)embarkment off or onto roll-on-roll-off ferries.
- The proposed system should ensure secure data collection, access, encryption, and decision support processes. Full encryption at transit and rest should be ensured, while enabling fuzzy searches on all metrics of the documents' data.
- In any case, the proposed solution(s) should consider both the travellers and the goods accompanying them.

HORIZON-CL3-2024-BM-01-05

Detection and tracking of illegal and trafficked goods

Research & Innovation Action | TRL - | 3M EUR/project | 2 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The proposed system should hence advance and/or combine as much as possible the components of detection, tracking and risk-based anticipation.
- On detection, the proposed solution(s) could include trustworthy algorithms for recognition that minimise false positives and biases. Proposed research could include, for example, image (shape) recognition and interpretation, and/or a trace detection approach.
- On tracking, the research can propose and explore, for example, technologies for improved traceability of goods and items that could be illicitly trafficked using non-invasive markings.
- On risk-based anticipation, the proposed solution(s) can leverage automated image recognition and interpretation capability coupled with data analytics, such as using advance cargo information in order to anticipate and detect security risks prior to goods' arrival at the EU external borders

HORIZON-CL3-2024-INFRA-01-01

Open Topic

Innovation Action | TRL 6-8 | 5M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for increasing the resilience of critical infrastructure, that are not covered by the other topics of Horizon Europe Calls Resilient Infrastructure 2021-2022, Resilient Infrastructure 2023 and Resilient Infrastructure 2024.

HORIZON-CL3-2024-INFRA-01-02

Resilient and secure urban planning and new tools for EU territorial entities

Innovation Action | TRL 6-8 | 6M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The proposals should include a high level of confidence in data management and sharing, provide solutions on cybersecurity issues and take on board new type of threats. The proposed solutions should suggest trusted shared architectures, trusted data collection, secure computation on the data and management processes, modelling capabilities, hypervisor supporting global situational awareness with open and trusted API's, trusted data processing engines and, e.g., artificial intelligence tools. If the tools include processing of personal data, it should consider including a risk assessment or privacy impact of individuals and society.
- The testing and/or piloting of the tools and solutions developed in a real setting and the participation of one or more relevant local authorities is an asset; regardless, actions should foresee how they will facilitate the uptake, replication across setting and up-scaling of the capabilities - i.e. solutions, tools, processes et al. – to be developed by the project.
- This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise.

HORIZON-CL3-2024-INFRA-01-03

Advanced real-time data analysis used for infrastructure resilience

Research & Innovation Action | TRL 5-6 | 5M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- While the availability of larger amounts of data from different sources offers potential to improve the identification of possible risks to infrastructures, it also increases the demand for fast and resilient analytical tools. There is a need to filter information to identify data that is relevant as an indicator for risks and - given the large number of different forms of cyberattacks or intrusions - also a need to prioritise and decide according to the degree of danger they present. This implies the need for matching data in the appropriate context and verifying the source with a view of ensuring that only relevant data is analysed, thus avoiding false results.
- Faster identification and localisation of hazardous agents and contaminants inside the infrastructure networks is a key to allow for quick response, inform and involve citizens and residents as well as avoid large-scale damage of any incident. Such identification capabilities can be deployed as part of the infrastructure and integrate with the systems public authorities use to make sure information is available as soon as possible. Furthermore, it is crucial to develop methods for better cooperation between different actors to ensure a common understanding and interpretation of data and to provide interactive tools for exchange and visualisation for decision support. Cooperation between different public and private actors is essential in this regard.
- This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise.

HORIZON-CL3-2024-CS-01-01

Approaches and tools for security in software and hardware development and assessment

Innovation Action | TRL - | 4-6M EUR/project | 6 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Software is at the foundation of all digital technologies and, as such, at the core of IT infrastructures, services, and products. Current software development prioritises fast deployment over security, which results in vulnerabilities and unsecure applications. Security engineering, both at the software and hardware levels, must be integrated in their development. Whilst a great portion of the software and hardware used in the EU is developed outside the European Union, it should comply with the security requirements within the EU.
- The EU should be able to rely on software and hardware that can be verified and audited as to their security. In particular, the potential security implications of using open-source software and hardware, and security auditability in that context, should be further explored. Software is subject to continuous update, so the security posture cannot be assessed once and for all, hence methods and tooling to perform continuous assessments of security are needed. In addition, security and privacy regulations also evolve, having to be factored in compliance approaches.

HORIZON-CL3-2024-CS-01-02

Post-quantum cryptography transition

Research & Innovation Action | TRL - | 4-6M EUR/project | 4 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The advent of large-scale quantum computers will compromise much of modern cryptography, which is instrumental in ensuring cybersecurity and privacy of the digital transition. Any cryptographic primitive based on the integer factorization and/or the discrete logarithm problems will be vulnerable to large-scale quantum-powered attacks. The digital data/products/systems that derive their security ultimately from the abovementioned primitives will be compromised and must be upgraded - including their replacement when needed- to quantum-resistant cryptography. The massive scale of this foreseen upgrade shows that preparations are needed today in order to widely implement the relevant mitigations in the future. Many companies and governments cannot afford to have their protected communications/data decrypted in the future, even if that future still seems distant. There is a need to advance swiftly in the transition to quantum-resistant cryptography.
- Post-quantum resistant cryptographic algorithms should be deployable in a dynamic manner in order to quickly react to new quantum computer developments. Recommendations for postquantum cryptography have already been published, but have to be maintained up-to-date. Proposals received under this topic should contribute to developing coordinated European recommendations for the transition to post-quantum cryptography across the EU.

HORIZON-CL3-2024-DRS-01-01

Prevention, detection, response and mitigation of chemical, biological and radiological threats to agricultural production, feed and food processing, distribution and consumption

Research & Innovation Action | TRL - | 4M EUR/project | 2 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The EU institutions have to start to consider the agri-food chain as a critical infrastructure which can suffer from attacks and which need to be protected. The most effective way to accomplish this goal is through international cooperation by a multisectorial approach combing different expertise, such as from law enforcement, the feed and food sector and health emergency services.
- The main challenge is to increase the resilience of European agricultural production, feed and food processing and distribution chain in case of sudden shocks. It is also crucial to address the interrelations between the food chain shocks and different types of critical entities with the objective of developing tools and methods to minimize cascading effects and allow rapid recovery of service performance levels after incidents. In the new context also the interaction with climate change, global trade and internet trade (spreading often plant material not controlled at all and of low quality) need to be taken into consideration. Artificial intelligence provides new tools for better coping with many of the most important challenges.
- This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise.

HORIZON-CL3-2024-DRS-01-02

Open Topic

Research & Innovation Action | TRL - | 3M EUR/project | 2 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for enhanced interactions among the scientific community, practitioners, city's risk managers of major crises and citizens or local communities in the event of (natural or man-made) disasters, that are not covered by the other topics of Calls Disaster-Resilient Society 2021-2022, Call Disaster-Resilient Society 2023 and Call Disaster-Resilient Society 2024.
- Proposals may address situational awareness of disaster-related risks by citizens, near-to-real-cases exercises (demonstrations simulating real cases) involving citizen volunteers, municipal authorities and first responders, advisory dissemination materials, highlighting good practices of interactions among citizens, municipal authorities and first and second responders in the event of (natural or man-made) disasters, addressed to European public in different EU languages, etc.

HORIZON-CL3-2024-DRS-01-03

Harmonised / Standard protocols for the implementation of alert and impact forecasting systems as well as transnational emergency management in the areas of high-impact weather / climatic and geological disasters

Innovation Action | TRL - | 3M EUR/project | 2 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Knowledge transfer (cross-border and cross-sectoral) about natural hazards-related risks and emergency management is essential to increase the resilience of societies. A vital dialogue and exchange of good practice examples among scientific and technical communities, stakeholders, policymakers and local communities is needed. In particular, the level of awareness of EU citizens for local risks can be increased by new approaches to visualise risks, vulnerability and exposure through e.g. impact forecasting data and mapping including satellite data and information.
- Currently, there are no harmonised / standardised European methods for identifying vulnerability and exposure on the basis of which alert and impact forecasting systems are established, allowing this information to be used by civil protection authorities in a timely manner to improve disaster preparedness, communication to local authorities and population, evaluation logistics etc.
- This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise.

HORIZON-CL3-2024-DRS-01-04

Hi-tech capacities for crisis response and recovery after a natural-technological (NaTech) disaster

Research & Innovation Action | TRL 5-7 | 4M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- The confluence of incidents in recent years has brought renewed concerns over our systemic resilience to external shocks arising from natural-technological (NaTech) disasters. The main focus on NaTech risks lies on a thorough understanding of the vulnerability of industrial sites and critical infrastructure, and the potential impact natural hazards can have on such technological resources. This entails the identification of both physical (safety of building facilities and structures) and operational vulnerabilities, often addressing multi-hazard conditions. Innovative methods are required for analysing worst-case scenarios, and informing decision-makers about the crosscutting and shared responses to different crises given available resources.
- Research involving multiple fields of expertise, including spatial information (to be specified), is also required to improve hi-tech capacities for operational response systems to better cope with natural and/or technological disasters occurring in Europe (and in overseas territories) in an integrated manner. This will rely on a knowledge sharing among natural and technological risks communities to develop a holistic vision for an integrated operational crisis management of NaTech disasters.
- This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise.

HORIZON-CL3-2024-DRS-01-05

Cost-effective sustainable technologies and crisis management strategies for RN large-scale protection of population and infrastructures after a nuclear blast or nuclear facility incident

Research & Innovation Action | TRL 6-8 | 6M EUR/project | 1 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Research on large-scale protection of population and infrastructure in the event of a nuclear explosion need to be undertaken both separately as well as in a RN-perspective. Research activities aimed at updating EU's possibilities for large-scale protection of population and infrastructure in the event of a nuclear explosion would benefit from being carried out in close cooperation with other EU-members. Research activities should also pertain to improved understanding of the radioactive fallout and assessment of dose rates to the population following a nuclear explosion in order to enable use of cost-effective sustainable technologies in protection of population and infrastructures.
- In a situation after a RN-incident the time consuming and laborious decontamination procedures for the population must be reduced to a minimum. Therefore, the possibility to identifying the need for decontamination, and above all to assess that there is no need for decontamination would be beneficial as well as the possibility to enter a shelter or other protected area in a safe way.
- This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise.

HORIZON-CL3-2024-SSRI-01-01

Exploration of critical raw materials in deep land deposits

Pre-commercial Procurement| TRL 6-8 | 5,25M EUR/project | 2 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Projects' results are expected to contribute to some or all of the following outcomes:
  - An identifiable community of EU civil security authorities with common user/functional needs for innovative technology solutions;
  - Tested and validated capacity of EU technology and industrial base to develop and produce technology prototypes that meet the needs of the EU user community;
  - Improved delineation of the EU market (including demand and supply) for innovative civil security systems that can articulate alternative options for uptake in function of different industrialisation needs, commercialisation needs, acquisition needs, deployment needs and additional funding needs (beyond R&I funding).

HORIZON-CL3-2024-SSRI-01-02

Exploration of critical raw materials in deep land deposits

Innovation Action | TRL 6-7 | 1,5M EUR/project | 4 to be funded | Deadline 20 Nov 2024

Link to the topic: click here

- Projects' results are expected to contribute to some or all of the following outcomes:
  - Development of a mature technological solution addressing EU security policy priorities in the areas addressed by the Cluster 3 work programme;
  - Facilitated access to civil security market for small innovators;
  - Improved cooperation between public buyers and small supply market actors for a swifter uptake of innovation in response to short to mid-term needs;
  - Stronger partnerships between small and medium EU security industry and technology actors to ensure the sustainability of the EU innovation capacity in the civil security domain and reduce technological dependencies from non-EU suppliers in critical security areas.

Köszönöm megtisztelő figyelmüket!