EN

Annex 6

Horizon Europe

Work Programme 2023-2024

6. Civil Security for Society

Table of contents

Destination - Better protect the EU and its citizens against Crime and Terrorism

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024: *"Crime and terrorism are more effectively tackled, while respecting fundamental rights, […] thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for police authorities […] including measures against cybercrime."*

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Modern information analysis for Police Authorities, allowing them to efficiently fight criminals and terrorists who use novel technologies;
- Improved forensics and lawful evidence collection, increasing the capabilities to apprehend criminals and terrorists and bring them to the court;
- Enhanced prevention, detection and deterrence of societal issues related to various forms of crime, including cybercrime, and terrorism, such as violent radicalisation, domestic and sexual violence, or juvenile offenders;
- Increased security of citizens against terrorism, including in public spaces (while preserving their quality and openness);
- Improved intelligence picture and enhanced prevention, detection and deterrence of various forms of organised crime;
- More secure cyberspace for citizens, especially children, through a robust prevention, detection, and protection from cybercriminal activities.

The following call(s) in this work programme contribute to this destination: [...]

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-FCT-01	43.00		23 Nov 2023
HORIZON-CL3-2024-FCT-01		37.00	
Overall indicative budget	43.00	37.00	

Call - Fighting Crime and Terrorism 2023

HORIZON-CL3-2023-FCT-01

Conditions for the Call

Indicative budget(s)[1]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[2]	Number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-FCT-01-01	IA	43.00	Around 5.00	1
HORIZON-CL3-2023-FCT-01-02	RIA		Around 5.00	1
HORIZON-CL3-2023-FCT-01-03	RIA		Around 3.00	1
HORIZON-CL3-2023-FCT-01-04	IA		Around 4.00	2
HORIZON-CL3-2023-FCT-01-05	IA		Around 3.00	1
HORIZON-CL3-2023-FCT-01-06	RIA		Around 3.00	2
HORIZON-CL3-2023-FCT-01-07	RIA		Around 4.00	1
HORIZON-CL3-2023-FCT-01-08	RIA		Around 3.00	1
HORIZON-CL3-2023-FCT-01-09	RIA		Around 3.00	2
Overall indicative budget		43.00		

General conditions relating to this call

[1] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

[2] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

FCT01 - Modern information analysis for fighting crime and terrorism

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-01: Processing of large, complex and unstructured datasets resulting from online activities, while reconciling big data analysis and data protection

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 43.00 million.[3]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

[3] This budget is shared with topic HORIZON-CL3-2023-FCT-01-02, HORIZON-CL3-2023-FCT-01-03, HORIZON-CL3-2023-FCT-01-04, HORIZON-CL3-2023-FCT-01-05, HORIZON-CL3-2023-FCT-01-06, HORIZON-CL3-2023-FCT-01-07, HORIZON-CL3-2023-FCT-01-08, HORIZON-CL3-2023-FCT-01-09

- Improved capabilities of European Police Authorities and other relevant security practitioners for a fast and flexible analysis of huge amounts of heterogeneous data through the application of robust and advanced tools, allowing them to efficiently fight criminals and terrorists who use novel technologies;

- Enhanced and modern analysis of heterogeneous data and training curricula that take into account legal and ethical rules of operation, cost-benefit considerations, as well as fundamental rights such as privacy and protection of personal data, providing reports that can be used in court;

- The work of European Police Authorities in the area of combatting fight and terrorism is supported by big data analysis that is in accordance with data minimisation principles and high privacy standards, with clearly identified challenges, adequate models and scientific options for tackling the challenge proposed and solutions developed that meet the challenge.

Scope: With the constant increase of technological developments, the processing of large datasets is inevitable for police work in today's digital world. As a wide range of products and services become digitalised and interconnected, Police Authorities need adequate technologies to properly detect and contain emerging threats. Big data analysis also provides invaluable opportunities to carry out investigations, identify suspects, reveal or anticipate crime patterns or links between previously unconnected events or actors. In particular, there is a continuous need for handling of large, complex and unstructured datasets resulting from online activities, in order to gather, normalise, process, transform, connect, prioritise, visualise the data (including text, image, audio and video) in ways that facilitate the extraction of actionable intelligence, while ensuring interoperability between existing systems and standards in different Member States. Solutions to perform temporal and geospatial analyses are also needed. The innovation efforts should provide support to web-based data analysis that can facilitate e.g. the detection of human trafficking, terrorism or child sexual exploitation in an online environment. The work should include surface, deep and dark web.

Examples of relevant techniques include: examination of digitally captured signatures, identification of voice cloning and of deepfakes; detection and recognition of persons/objects/logos; speaker diarisation and identification; speech recognition and transcription into text; automatic classification of text into risk factors; optical character recognition; named entity recognition; concept extraction, extraction of entities and relations between them in unstructured text; multimodal analytics, in order to discover insights and patterns in large volumes of data through clustering, as well as the identification of user communities and key actors in the social networks being formed online; automatic correlations among all available sources, as well as cross-checking, cross-matching and mapping information between different cases, i.e. cross-reference with existing records in databases of Police Authorities. Identification of perpetrators can also be enhanced by detecting their online behaviour and habits, e.g. which days/hours they are used to login/logout, patterns used in passwords.

Taking advantage of these modern technologies will require Police Authorities to move away from business models based on data input to data evaluation. It will require robust and reliable information management structures that encompass all aspects from data collection to handling, evaluation, exploitation and data security. In particular, key principles such as data minimisation should apply to ensure that Police Authorities conduct data analysis in full compliance with fundamental rights and EU privacy standards. For example, it may be necessary to filter and reduce large datasets to what is relevant for operational support activities and in investigations. Hence, all these efforts should also reconcile big data analysis and data protection, i.e.: explore challenges to conduct big data analysis in accordance with data minimisation principles and high privacy standards, propose possible models and scientific options to tackle the challenge, and develop solutions (digital tools) that meet the challenge, focusing on triage and clustering functions. The successful proposal should thus help framing the issue of big data analysis for Police Authorities, providing guidelines as well as operational tools to comply with EU data protection standards.

The successful proposal should build on the relevant previous works (such as the H2020 projects ASGARD, STARLIGHT, COPKIT, AIDA or MAGNETO) and create synergies with similar on-going security research projects from the Horizon Europe WP2021-2022 on secure societies in the area of modern information analysis, in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Possibilities of coordination with related activities funded through the Internal Security Fund (such as EACTDA) and the Digital Europe Programme should be analysed too.

HORIZON-CL3-2023-FCT-01-02: Mitigating new threats and adapting investigation strategies in the era of Internet of Things

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 43.00 million.[4]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Modern tools to explore new threats pertaining to the development of Internet of Things are provided to European Police Authorities and other relevant security practitioners,

[4] This budget is shared with topic HORIZON-CL3-2023-FCT-01-01, HORIZON-CL3-2023-FCT-01-03, HORIZON-CL3-2023-FCT-01-04, HORIZON-CL3-2023-FCT-01-05, HORIZON-CL3-2023-FCT-01-06, HORIZON-CL3-2023-FCT-01-07, HORIZON-CL3-2023-FCT-01-08, HORIZON-CL3-2023-FCT-01-09

mitigating measures are proposed and the capabilities are enhanced regarding reliable interception of attack plans, all in a lawful manner;

- Faster evaluation and targeted exchange of security-relevant information between Police Authorities, including improved action options;
- Lawful access and exploitation of digital evidences in the Internet of Things environment is fortified, taking into account legal and ethical rules of operation as well as fundamental rights such as privacy and protection of personal data;

Best practices (legal, organisational, technical) to access and exploit Internet of Things in the course of investigation are strengthened, including by proposing standards and policy options as well as developing relevant tools and training materials.

Scope: Internet of Things (IoT) connects practically everything and makes everything more vulnerable as well. IoT devices increasingly benefit from the convergence and integration of technologies, such as machine learning, real-time analytics as well as 5G that will provide faster and more reliable connections for all devices.

There are a number of implications particular to IoT devices, which have been consistently highlighted by researchers and Police Authorities. IoT devices allow for the proliferation of attack vectors. Insecure IoT devices may become an easier target for criminals aiming to distribute attacks, infiltrate or infect networks - e.g., Distributed Denial of Service (DDoS) attacks originating from botnets of compromised Internet of Things (IoT) devices or malware-infected IoT devices, which exploit software vulnerabilities or weak authentication settings. Malevolent actions against connected devices with direct physical impact (e.g. car-to-car communication) are also a growing concern.

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 mitigate the emerging threats that this may pose.

At the same time, IoT proliferation will provide opportunities for the Police Authorities and other relevant security practitioners to collect a new range of data in relation with criminal activities. 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 European 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 secured and used for deriving indicators of an imminent threat.

The research should assess legal, organisational and technical implications of IoT development in the context of digital investigations, and propose strategies, including policy options, best practices, training materials, tools and path to standards that would foster “by design” a lawful access to relevant evidences.

The successful proposal should build on the relevant previous works and create synergies with similar on-going security research projects from the Horizon Europe WP2021-2022 on secure societies in the area of modern information analysis and digital security, in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Possibilities of coordination with related activities in the Digital Europe Programme should be analysed too.

FCT02 - Improved forensics and lawful evidence collection

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-03: 3D printing of weapons, including of energetic materials

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 43.00 million.[5]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Police Authorities and forensic institutes are provided with innovative methods of tracing of devices for 3D printing of weapons, including of energetic materials (explosives, pyrotechnics and propellants);
- Enhanced evidence collection due to a robust establishment of links between different cases, which takes into account legal and ethical rules of operation, the traceability of forensic evidence, cost-benefit considerations, as well as fundamental rights such as privacy and protection of personal data;
- Increased understanding and preparedness of Police Authorities and Forensic Institutes for future developments and possible investigations in this area, such as programmable matter or 4D technology;

Improved shaping and implementation of regulation related to the fight against malicious use of 3D printing of weapons, including of energetic materials.

[5] This budget is shared with topic HORIZON-CL3-2023-FCT-01-01, HORIZON-CL3-2023-FCT-01-02, HORIZON-CL3-2023-FCT-01-04, HORIZON-CL3-2023-FCT-01-05, HORIZON-CL3-2023-FCT-01-06, HORIZON-CL3-2023-FCT-01-07, HORIZON-CL3-2023-FCT-01-08, HORIZON-CL3-2023-FCT-01-09

Scope: 3D printing of weapons, including of energetic materials, i.e. materials with large amounts of stored or potential energy that can produce an explosion (explosives, propellants and pyrotechnics), is a topic of increasing concern to the law enforcement community. Police Authorities and forensic institutes would benefit from a better understanding and solutions that facilitate the tracing of printing devices, as well as the establishment of links between different cases. This is particularly relevant in the fields of serious and organised crime and drugs trafficking. The outcomes of this analysis may feed policy-making towards the adoption/updating of legal framework.

The successful proposal should not only focus on addressing the current issues but should also anticipate the likely evolutions. Notably, possible criminal abuses of 3D printing technology can become even more complex with the development of programmable matter (PM) technology and its use in 4D printing, with the 4th dimension being the time-dependent shape change after the printing. Namely, PM would enable 3D printed objects to be modified by the user or programmable for post-fabrication changes in function and shape, such as adapting to changing environments. PM technology, and its use in 4D printing, has a huge disruptive potential for security. Police Authorities and forensic practitioners need to keep track of developments in 3D printing, PM and 4D printing technology in order to better asses their disruptive capacity, potential misuse by criminals or terrorists, and, consequently, forensics challenges in investigating such cases.

HORIZON-CL3-2023-FCT-01-04: A harmonized European forensics approach on drugs analysis

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 43.00 million.[6]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- European Police Authorities, Forensic Institutes and other relevant security practitioners are equipped by modern means of chemical analysis (composition) in drugs aimed at facilitating the cross-matching of seized drugs to labs and the establishment of links

[6] This budget is shared with topic HORIZON-CL3-2023-FCT-01-01, HORIZON-CL3-2023-FCT-01-02, HORIZON-CL3-2023-FCT-01-03, HORIZON-CL3-2023-FCT-01-05, HORIZON-CL3-2023-FCT-01-06, HORIZON-CL3-2023-FCT-01-07, HORIZON-CL3-2023-FCT-01-08, HORIZON-CL3-2023-FCT-01-09

between cases, including by developing protocols to quickly exchange information on new substances;

- Improved and uniform EU-wide approach for the collection of evidence regarding illicit drugs-related overdoses, that would allow for choosing adequate responses in countering the drug-related problems;

- Improved collection and availability of forensic evidence, that could be used in court by the authorities, in direct violence, kidnapping or human trafficking cases, as well as reinforced prevention of such cases thanks to sensors/kits that are reliable, lawful, fast and easy-to-use;

Enhanced perception of citizens in public and private spaces that Europe is an area of freedom, justice and security.

Scope: Proposals are expected to address one of the following options:

Option A: A harmonised European approach is needed on the study of chemical analysis (composition) in drugs, to

1) facilitate the cross-matching of seized drugs to labs and the establishment of links between cases, including by developing protocols to quickly exchange information on new substances;

2) tackle forensic challenges related to illicit drugs-related overdoses.

The production of synthetic drugs in the EU is continuously expanding. The laboratories producing synthetic drugs are becoming more professional and versatile, resulting in an increased production and a greater flexibility in terms of which substances are produced and how they are produced.

On the one hand, criminal networks and criminals active in the production of synthetic drugs display a particularly high degree of specialisation. Thus, a modern and harmonised European approach to the analysis of the drugs composition would help to cross-match seized drugs to labs and make the links between cases, allowing a cross-border exchange of such evidence.

On the other hand, choosing appropriate responses that are likely to be effective in dealing with a particular drug-related problem requires a clear understanding of the problem, supported by the strongest available evidence. However, an obstacle in this process is the very limited or fully absent evidence, as it is the case in finding responses aimed at reducing overdose-related deaths. Namely, autopsies with full toxicology are underdeveloped in many Member States, making comparison at EU level difficult and aggregated numbers on overdose deaths not fully representative. Member States called to make this issue more comparable EU-wide. To this end, a modern chemical analysis of the drugs composition and a unified EU-wide approach would provide a significant support, also in view of commitments of the EU Drugs Strategy 2021-2025.

Option B: A reliable and easy-to-use detection of chemical submission drugs in beverages and urine.

GHB (Gamma-hydroxybutyrate) is one of the drugs known as "club drugs" or "date rape drugs". Notably when mixed with alcohol, it has a depressant effect and causes drowsiness, rendering the person defenceless and unable to remember what happened. Sexual assaults facilitated by chemical submission drugs have a growing tendency in Europe. Thus, Police Authorities and forensic practitioners need modern methods and technologies that enable better prevention against and investigation of different forms of violence and assault supported by these drugs. To this end, the successful proposal should aim at developing sensors and/or kits that would be fast and easy to use by Police Authorities in the field (i.e., in places where citizens are more at risk of ingesting GHB drugs through drinks and beverages). Furthermore, such solutions should provide results that are reliable, safe and simple to interpret when looking for and collecting evidence of such drugs that can be used in court. Legal and ethical challenges of such solutions should be fully considered in the development process.

Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

FCT03 – Enhanced prevention, detection and deterrence of societal issues related to various forms of crime

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-05: New technologies in service of community policing and transferable best practices

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 43.00 million.[7]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Strengthened resilience of local communities against crime, lowered feeling of insecurity and improved law enforcement;

[7] This budget is shared with topic HORIZON-CL3-2023-FCT-01-01, HORIZON-CL3-2023-FCT-01-02, HORIZON-CL3-2023-FCT-01-03, HORIZON-CL3-2023-FCT-01-04, HORIZON-CL3-2023-FCT-01-06, HORIZON-CL3-2023-FCT-01-07, HORIZON-CL3-2023-FCT-01-08, HORIZON-CL3-2023-FCT-01-09

- Early identification of negative factors in local communities, detection of possible threats, and better crime reporting;
- Better recognition for community diversity within neighbourhoods, and tailored approaches to majorities including communities traditionally not engaging with statutory authorities resulting in comprehensive community empowerment;
- Identification and EU wide dissemination of validated community policing best practices;
- Development of new methodologies, tools and adoption of technological support;
- Development of training curricula for Police Authorities on community policing in non-homogenous local milieus with social complexities, including balancing of majority needs while recognising expectations of minorities and/or sub-groups.

Scope: Community policing (CP) is an integral part of policing focusing on cooperation with local community for better understanding given group needs and meeting them. From both a theoretical and a practical point of view, three ways of delivering CP may be outlined: reactive, proactive, and co-active - based on community consultations and common actions[8]. While performing such actions, police provides information, initiates and participates in programs to prevent crime and ensure the protection of citizens in cooperation with other institutions. CP aims to create opportunities for positive, mutually respectful interactions between civilians and the police, to increase citizens` trust and enhance the ability of police to enforce the law.

Nowadays, Police Authorities, while caring out their duties to provide community security, are faced with numerous economic and demographic challenges. As a consequence, more efficient solutions, tools and methodologies are sought. First responders cope with growing communities, tighter budgets, and diverse quickly evolving milieus in their neighbourhoods, regularly facing challenges that initial professional training could not prepare them for. Moreover, rapidly changing social, economic and political environment, both domestically and internationally, complicates these problems and fuels new tensions. New approaches should also cover internal review of Police Authorities' personnel training, possible change of attitudes, or countering existing misconceptions and biases. Exchange of internationally validated best practices should be also coupled with adoption of new technologies in support to planning and carrying out the daily CP routines. Some examples of already introduced technologies are social media, Geographic Information System (GIS) or Open Source Intelligence (OSINT). Proposals should build on achievements and findings of related EU-funded projects such as UNITY, INSPEC2T, ICT4COP, CITYCoP or TRILLION. Activities proposed within this topic should address both technological and societal dimensions of CP in a balanced 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, in order to produce meaningful and significant effects enhancing the societal impact of the related innovation activities.

[8] Community Policing - A European Perspective - https://link.springer.com/book/10.1007/978-3-319-53396-4?page=1#toc"

FCT04 – Increased security of citizens against terrorism, including in public spaces

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-06: Exploring the risk of non-state actor development and deployment of a bioterrorist attack

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 43.00 million.[9]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Security practitioners and policy makers are provided with an improved intelligence picture of available and affordable substances and techniques with misuse potential including their threat levels and impact factors;
- Assessment of the probability of biohacking and weaponising of biological agents, including availability of necessary equipment, level of knowledge and skills of the perpetrators;
- Recommendations on open access and security policies towards protection of human and non-human genomic information databases, including legitimate access and remote exploitation;
- Development of case scenarios of homemade bioterrorism attack based on research conducted and recommendation of countermeasures including possible monitoring activities;
- Review and improved shaping of related future EU regulations.

Scope: Biological weapons in terms of their effectiveness are equal to the nuclear ones, thus growing influx of information from public media and professional scientific journals concerning availability, and affordability of gene editing knowledge and equipment raises significant security questions. In the past years, professional scientists has lost their exclusive license to DNA engineering, and home-grown biohackers have started their independent

[9] This budget is shared with topic HORIZON-CL3-2023-FCT-01-01, HORIZON-CL3-2023-FCT-01-02, HORIZON-CL3-2023-FCT-01-03, HORIZON-CL3-2023-FCT-01-04, HORIZON-CL3-2023-FCT-01-05, HORIZON-CL3-2023-FCT-01-07, HORIZON-CL3-2023-FCT-01-08, HORIZON-CL3-2023-FCT-01-09

experiments based on their own education, knowledge, online resources and commercially available components and tools. As the equipment becomes cheaper, DNA fragments can be purchased online from legally operating companies, and the expertise in gene-editing techniques available online, the potential for abuse is growing. Moreover, it is anticipated that genome printers will also soon be available for at-home applications strengthening the biohackers workbench. Even the more expensive techniques are not beyond reach of nonprofessional experimenters because while academic researchers undergo strict scrutiny when seeking federal funding, there are other non-governmental sources like private funding or crowdfunding websites, which may provide sufficient resources and minimum supervision. Furthermore, there are also already information that individuals affiliated to terrorist organisation are exploring this sphere. Among substances possible to weaponise are ones made from toxins such as botulism, or salmonella bacteria, Ebola virus, or bubonic plague virus from infected animals. Using these pathogens, one could attack municipal water systems and reservoirs, or air conditioning systems in mass gatherings. Doubts connected with possible rogue modification of living organisms` DNA raises also questions about establishing the necessary balance between open information sharing of research databases and requirements for their protection. The European Union and its Member States must consider, and prepare for the possibility of such an attack on their citizens. Possibility of home-made bioweapon to be used against civil population could appeal for a monitoring activities of certain substances and equipment at the state and/or EU level. Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

FCT05 – Organised crime prevented and combated

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-07: Organized Property Crime

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 43.00 million.[10]
Type of Action	Research and Innovation Actions

[10] This budget is shared with topic HORIZON-CL3-2023-FCT-01-01, HORIZON-CL3-2023-FCT-01-02, HORIZON-CL3-2023-FCT-01-03, HORIZON-CL3-2023-FCT-01-04, HORIZON-CL3-2023-FCT-01-05, HORIZON-CL3-2023-FCT-01-06, HORIZON-CL3-2023-FCT-01-08, HORIZON-CL3-2023-FCT-01-09

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Security practitioners and policy-makers are provided with improved and complete intelligence picture of organised property crime, including cross-border dimension, analysis and recommendations for possible improvement in data collection;
- Identification and review of most efficient international cooperation schemes in tackling organised property crime including lessons learned from Joint Investigation Teams and liaison officers;
- Fortified ability of Police Authorities and other relevant security practitioners to detect and prevent the emergence of networks involved in organised property crimes, and improved response to the threat of existing organisations;
- Recommendations and further improvement of security-by-design approach to urban areas development and management;

Identification and dissemination of best practices to be introduced in community policing strategies.

Scope: Organised property crime is a complex criminal phenomenon with dynamic range from organised robberies, through pick-pocketing, cargo crimes, motor vehicles theft, burglaries and thefts to fencing with ever-changing *modus operandi,* which contributes to the feeling of insecurity amongst European citizens and thus being a major concern to EU law enforcement. According to Eurostat, more than one million cases related to burglary are reported in the EU each year. Organised property crime, being likely the most visible type of organised crime, with a direct impact on people and the private and public sector, is one of the EU's priorities in the fight against serious and organised crime as part of EMPACT 2022 - 2025. Perpetrators are early adapters of new technological developments and quickly embrace changing operational environment, such as Covid-19 pandemics. Organised crime groups make use of various online services to facilitate their actions including social media platforms for checking whether individuals are away from targeted residences, scouting targeted neighbourhoods using free online navigation tools and fencing goods via online marketplaces. Activities proposed within this topic should address both technological and societal dimensions of organised property crime in a balanced way, taking care of the applicable legislation. International dimension should be analysed as well, such as networking and smuggling processes. Thus, both police, border guards and customs authorities should be involved in the consortia, in order to tackle effectively all aspects of this crime. One of the main challenges here is high mobility of organised crime groups, while majority of the Member States investigate these crimes at the local or national level. Proposals are expected to build on finding and achievements of earlier EU funded projects such as SPECTRE - Struggling against and Pursuing Experienced Criminal Teams Roaming in Europe (ISF).

HORIZON-CL3-2023-FCT-01-08: Crime as a service

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 43.00 million.[11]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- European Police Authorities and policy makers are provided with a robust analysis of the evolution of the contemporary organised crime, its structure, role of hierarchy, membership in the organisation and subcontracting of specialised criminal services.
- Policy makers benefit from an analysis of legal framework utilised for countering organised crime, in terms the validity of the legal definitions and penal provisions adopted and their impact on the effectiveness of judicial verdicts.
- Identification of the means of advertising, communication, marketing and money flows while offering criminal services on the underground market and development of methodology for their identification and set of respective countermeasures.
- Improved knowledge within European security institutions regarding developments in the field of organised crime and prospects for the future.

Scope: The Crime-as-a-service (CaaS) model proliferates and becomes a prominent feature not only for the cybercriminal underground, but also for traditional criminals hiring specialised digital and financial services. Thus, availability of exploit kits and other services not only serves cybercriminals with low technical skills, but also makes the operations of mature and organised threat actors more efficient. In 2021, Malware-as-a-service (MaaS) offerings on the Dark Web increased, of which ransomware affiliate programs seem to be the most prominent. These programs are an evolution of the Ransomware-as-a-Service (RaaS) model in which the operators share profits with partners who can breach a target network and either harvest all the information required to launch an attack or deploy the malware themselves. The shape of the organised crime evolves, investigators apart from traditionally closed, clandestine criminal structures, are increasingly confronted with modern, flexible, specialised and "multi-ethnic" organisations with a global operational range. As these groups seem not to work within

[11] This budget is shared with topic HORIZON-CL3-2023-FCT-01-01, HORIZON-CL3-2023-FCT-01-02, HORIZON-CL3-2023-FCT-01-03, HORIZON-CL3-2023-FCT-01-04, HORIZON-CL3-2023-FCT-01-05, HORIZON-CL3-2023-FCT-01-06, HORIZON-CL3-2023-FCT-01-07, HORIZON-CL3-2023-FCT-01-09

permanent multi-layered structures but with various actors delivering on demand services, some of the organised crime characteristics might be subject for a review. The shadow economy, like the official one, seeks for maximising the profit, and criminals take advantage of new ways of working in order to make their trade more effective and efficient, thus resulting in these entities leveraging technology, and underground market oriented to achieve their mission. Observed trend may be a challenge for the codified laws and definitions of organised crime as supposedly sealed off to outsiders and characterised by fixed and permanent cooperation. In order to enhance the fight against organised crime at the European level, it is a distinct research need to gain greater insight into the internal workings of modern organised crime structures. Coordination among the successful proposal from this topic as well as with the successful proposals under topic HORIZON-CL3-2024-FCT-01-08: *Tracing of cryptocurrency transactions* should be envisaged to avoid duplication, and to exploit complementarities as well as opportunities for increased impact.

FCT06 – Citizens are protected against cybercrime

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-FCT-01-09: Enhancing prevention and deterrence of advanced forms of cyber threats and cyber-dependent crime

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 43.00 million.[12]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Development of modular toolbox for Police Authorities, facilitating gathering and processing of data relevant for cybercrime and cyber - enabled crime investigations;
- Development of training curricula for Police Authorities, prosecutors, as well as judicial actors on major contemporary cybercriminal activities;

[12] This budget is shared with topic HORIZON-CL3-2023-FCT-01-01, HORIZON-CL3-2023-FCT-01-02, HORIZON-CL3-2023-FCT-01-03, HORIZON-CL3-2023-FCT-01-04, HORIZON-CL3-2023-FCT-01-05, HORIZON-CL3-2023-FCT-01-06, HORIZON-CL3-2023-FCT-01-07, HORIZON-CL3-2023-FCT-01-08

- Identification of best practices of international law enforcement and judicial cooperation networks;

- Development of multi-stakeholders strategies, including novel investigation schemes and information sharing mechanisms.

Scope: While cyber-attacks, notably ransomware and distributed denials or services, are getting more sophisticated, law enforcement officers need to develop strategies to gain a comprehensive knowledge of the numerous elements contributing to the attack (Virtual Private Networks - VPNs, Bulletproof Hosting – BPH, Remote Access Trojans – RATs, botnets, Dark Web platforms, cryptoransomware, Criminal Phone Banks, Pseudonyms, Advanced Persistent Threat groups – APTs, etc.). Having in mind that these are offered today in form *Crime-as-a-service* for anyone willing to pay, there is growing number of cases where advanced investigation have to be launched and conducted. Investigators need timely access to relevant data and expertise of a different nature and belonging to different categories of stakeholders (e.g. other Police Authorities or Internet service providers). As geographical boundaries become irrelevant in the commission of crime, criminal investigations have to become more cooperative. Comprehensive investigation of contemporary organised crime does not seem feasible to conduct by a single investigator or even a single force. This technical and organisational complexity together with the cross-border nature of cyberattacks requires cutting-edge investigative approaches, gathering a large range of expertise as well as trusted information sharing mechanisms across communities (including secured platforms). In addition, it is necessary to enhance cybercrime intelligence picture notably by enhancing reporting mechanism of cyber-dependent criminal activities. Enhancing prevention and deterrence of these forms of cyber and cyber-dependent crime takes development of multi-stakeholders strategies, including novel investigation schemes and information sharing mechanisms. Coordination among the successful proposals from this topic as well as with the successful proposal under topic HORIZON-CL3-2023-FCT-01-03 should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

Call - Fighting Crime and Terrorism 2024

HORIZON-CL3-2024-FCT-01

Conditions for the Call

Indicative budget(s)[13]

[13] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[14]	Number of projects expected to be funded
		2024		
Opening: na				
HORIZON-CL3-2024-FCT-01-01	IA	37.00	Around 4.00	1
HORIZON-CL3-2024-FCT-01-02	RIA		Around 3.00	1
HORIZON-CL3-2024-FCT-01-03	RIA		Around 5.00	1
HORIZON-CL3-2024-FCT-01-04	RIA		Around 3.00	2
HORIZON-CL3-2024-FCT-01-05	IA		Around 5.00	1
HORIZON-CL3-2024-FCT-01-06	RIA		Around 3.00	2
HORIZON-CL3-2024-FCT-01-07	RIA		Around 3.00	1
HORIZON-CL3-2024-FCT-01-08	IA		Around 4.00	1
Overall indicative budget		37.00		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.

[14] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

FCT01 - Modern information analysis for fighting crime and terrorism

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-01: Lawful interception: facing upcoming challenges

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 37.00 million.[15]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to all of the following outcomes:

- Challenges (legal, ethical and technical) for the police and the judiciary, posed by new technologies, are identified in the field of lawful interception, possible advanced solutions analysed and proposed, effective training materials created for Police Authorities and standardization activities fostered;
- Effective cooperation fortified among European Police Authorities and innovation community in the area of lawful interception, resulting, among others, in innovative solutions for targeted lawful access and evidence collection for legitimate law enforcement purposes.

Scope: Lawful interception is a key investigation and search tool in all fields of fighting crime, especially when it comes to combatting international terrorism, organized crime and cybercrime. As such, it is of utmost importance for Police Authorities that this instrument remains a key tool in future, despite further technical progress.

Recent developments, including the roll out of 5G networks, together with the shift to application level communications, privacy oriented protocols (notably end-to-end encryption and VPN connections), high speed networks, machine to machine communication and edge computing poses significant challenges to Police Authorities to carry on their duty.

[15] This budget is shared with topic HORIZON-CL3-2024-FCT-01-02, HORIZON-CL3-2024-FCT-01-03, HORIZON-CL3-2024-FCT-01-04, HORIZON-CL3-2024-FCT-01-05, HORIZON-CL3-2024-FCT-01-06, HORIZON-CL3-2024-FCT-01-07, HORIZON-CL3-2024-FCT-01-08

Alongside with the policy work conducted by the European Commission and the Council on encryption and data retention, it is instrumental to explore innovative solutions that preserve the ability of the European Police Authorities to access relevant information while ensuring at the same time the highest level of privacy of communications and cybersecurity standards. In order to reinforce networking and develop uniform methods and technical analysis standards, as well as ensure the sustainability of lawful interception in the Member States, EU-funded technical solutions for secure lawful interception capabilities in Europe are needed.

The work of the successful proposal should be focused on

1. identifying new challenges pertaining to lawful interception in the context of 5G and beyond, Internet of Things, temper-proof communications, edge computing, high bandwidth networks, loss of geolocalisation, etc.;

2. exploring innovative paradigms to perform lawful interception e.g. through the exploitation of metadata (social graphs, traffic analysis), data mining, behavioural analysis, in compliance with fundamental rights and data protection principles;

3. developing best practices, tools and standardisation activities to mitigate the identified challenges.

This analysis should not only focus on addressing the current obstacles but should also anticipate the likely evolutions in the field (e.g., of encryption and decryption technologies).

The successful proposal should build on related works, such as of the predecessor project funded in the scope of the previous WP.

FCT02 - Improved forensics and lawful evidence collection

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-02: Lawful evidence collection in online child sexual abuse investigations, including undercover

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 37.00 million.[16]
Type of Action	Research and Innovation Actions

[16] This budget is shared with topic HORIZON-CL3-2024-FCT-01-01, HORIZON-CL3-2024-FCT-01-03, HORIZON-CL3-2024-FCT-01-04, HORIZON-CL3-2024-FCT-01-05, HORIZON-CL3-2024-FCT-01-06, HORIZON-CL3-2024-FCT-01-07, HORIZON-CL3-2024-FCT-01-08

Expected Outcome: Projects' results are expected to contribute to all of the following outcomes:

- Development of safer justice outcomes through an increased understanding of the EU-wide legal aspects of online investigations, including undercover, in the area of child sexual abuse;
- Improved understanding of the EU-wide legislative hurdles that impact (undercover) investigations in this area;
- Modern and robust methods at the European level are proposed at all steps of an investigative process in this area, overcoming various types of biases and obstacles to the collection of evidence that is admissible in court and respects privacy, protection of personal data and anonymity of victims;
- Forensic practitioners, Police Authorities and other relevant security practitioners active in online (including undercover) child sexual abuse investigations benefit from innovative guidelines, manuals, education and training curricula.

Scope: The use of online undercover investigation techniques is an important asset for Police Authorities in infiltrating the networks of sexual abusers of children. These methods have proven very effective in understanding offender behaviour and interaction on online service providers, and have ultimately facilitated the shutting down of communication channels used by these offenders, as well as their prosecution. An increasingly important need for Police Authorities' activity in these spaces is the ability to effectively infiltrate particularly dangerous online groups of offenders, while making sure that the evidence obtained will be admissible in court. EU values and fundamental rights shall stay in the core of any future measures. Research in this area should tackle legislative hurdles 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 more effectively target these offenders. The results of this research topic (training, manuals guidelines) should be shared via CEPOL, provided that the Agency opts out from applying. The successful proposal should build on the relevant previous works (such as the H2020 projects GRACE, RAYUELA, CC-DRIVER and HEROES) and create synergies with similar on-going security research projects from the Horizon Europe WP2021-2022 in the area of digital forensics and countering child sexual abuse, in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Special care needs to be given to ethics and fundamental rights protection throughout the research and the solutions proposed. 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, in order to produce meaningful and significant effects enhancing the societal impact of the related innovation activities.

HORIZON-CL3-2024-FCT-01-03: CBRNE forensics – post-blast crime scene investigation

Specific conditions

Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 37.00 million.[17]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved European common investigation capabilities thanks to modern, robust and validated solutions used by forensic institutes and Police Authorities for analysing post-blast crime scenes in order to make fast and reliable assessments of charge weight and determine the point of origin of the detonation;
- Improved modelling capability of post-blast forensic investigators to assess damages after explosion;
- European common and lawful methods for forensic investigators to collect and sample traces as well as secure evidence for judicial purposes;

Police Authorities and other relevant security practitioners are provided with modern tools for a better assessment and prevention of explosions.

Scope: One of the main challenges of post-blast forensic investigations consists in identifying the properties/source of explosion (notably epicentre, composition, charge weight), based on the damage caused to surrounding buildings, such as crater size, fractures, extent of thrown debris, etc. Classical approaches in post-blast forensic investigation are mainly based on photos and videos, i.e. observed damage. However, in order to determine the properties of explosion, high-quality (high-resolution and high accuracy) low-cost 3D scene mapping and reconstruction techniques, including an automated transfer of reconstruction data, need to be developed. Furthermore, advanced user-friendly simulation/modelling tools, such as of various blasts in different settings, are needed for the development of a calibrated tool for assessment of detonation data (energy release, TNT equivalent, origin, etc.). Automated interpretation of recorded data should be included as well.

The proposal should aim to achieve results to be used for forensic purposes, while also envisaging preventive usages, i.e., to evaluate how to evacuate an area while minimising risks in case of an explosion. For these scenarios the same evaluation, simulations, etc. would be required. Selective on-site methods to determine the explosives used would provide improved knowledge on where to collect and secure samples for forensics investigations. The successful

[17] This budget is shared with topic HORIZON-CL3-2024-FCT-01-01, HORIZON-CL3-2024-FCT-01-02, HORIZON-CL3-2024-FCT-01-04, HORIZON-CL3-2024-FCT-01-05, HORIZON-CL3-2024-FCT-01-06, HORIZON-CL3-2024-FCT-01-07, HORIZON-CL3-2024-FCT-01-08

proposal should also tackle legal implications of different national procedures for CBRNE sampling collection and the legal implications for sampling analysis in different EU laboratories.

Proposed activities should build on previous EU-funded projects in this area, such as INHERIT and ODYSSEUS.

FCT03 – Enhanced prevention, detection and deterrence of societal issues related to various forms of crime

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-04: Radicalisation and gender

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 37.00 million.[18]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved understanding of women and girls motivation for the support of extremist ideologies, including grievances and stigmatisation elements;
- Development of strategies to enhance application of motivation factor in detection, prevention and de-radicalisation efforts;
- European Police Authorities, social care workers and teachers 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;

Design girls and women's empowerment approaches through legal, financial and/or cultural means aimed at tackling the root causes of radicalisation and extremism.

[18] This budget is shared with topic HORIZON-CL3-2024-FCT-01-01, HORIZON-CL3-2024-FCT-01-02, HORIZON-CL3-2024-FCT-01-03, HORIZON-CL3-2024-FCT-01-05, HORIZON-CL3-2024-FCT-01-06, HORIZON-CL3-2024-FCT-01-07, HORIZON-CL3-2024-FCT-01-08

Scope: Terrorism resulting from radicalisation and violent extremism is a serious threat to European security. Part of the complexity of these phenomena lies in the fact that there is neither a single pathway to radicalisation nor a single terrorist profile. Support of extremist is an effect of individual clusters of psychological, personal, social, economic and political reasons. From a gender perspective, women's radicalisation and involvement in violent extremist groups remains relatively under-researched and still characterized by misconceptions. This misconception shaped counter-terrorism strategies in the past, exacerbating women's exclusion from decision-making processes and their significant underrepresentation in bodies countering the phenomena. In situations of conflict and violence, women are unfairly seen as passive, victims, subordinate and maternal, while these are assumptions reinforcing gender stereotypes. A woman should not be assumed to be more or less dangerous, nor more prone to peace, dialogue, non-violence and co-operation than a male. In fact, the very image of the peaceful woman has been used by terrorist groups to recruit in their organisations [19]. Entry point for prevention and de-radicalisation efforts are local communities, which are both stakeholders and partners of the law enforcement in this process. Activities aimed at youngsters and adults have to be gender sensitive, and research has to deliver tailored advice and solutions adequately, and proportionately addressing all critical issues. Community policing with its multidisciplinary approach seeks the cooperation of local communities and the broad range of public authorities in its efforts of building safe environments, however this efforts should recognise not only cultural, social and economic diversity of the milieus, but mentioned above be gender sensitive. Proposals should build on past EU-funded projects such as ARMOuR, BRIDGE, DARE, D.RAD, RaP or YoungRes. Moreover the EU Counter-Terrorism Agenda adopted in 2020 outlines that Radicalisation Awareness Network (RAN) will identify best practices and approaches of community policing and engagement to build trust with and among communities, and research under this topic should also build upon the work done by RAN. 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, in order to produce meaningful and significant effects enhancing the societal impact of the related innovation activities.

FCT04 – Increased security of citizens against terrorism, including in public spaces

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-05: CBRN detection capacities in small architecture

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

19 https://www.europol.europa.eu/cms/sites/default/files/documents/women_in_islamic_state_propaganda_3.pdf

Indicative budget	The total indicative budget for the topic is EUR 37.00 million.[20]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved vulnerability assessments by law enforcement and local managers of public spaces by detection of chemical, biological, radiological and nuclear (CBRN) threats in the public spaces and flow of public transport, in order to provide broader situational awareness to practitioners in the field;
- Enhanced planning capabilities of security practitioners and policy-makers due to the access of new data and identification of potential vulnerabilities connected to the design/refurbishment and improvement of different public spaces;
- Recommendations for further improving safety and security-by-design approach to public spaces and mass transportation systems;
- Improved training of Police Authorities in collaboration with different public and private actors (e. g., crisis management and civil protection authorities, fire brigades, regulatory agencies, emergency health services, security managers, private security organisations, civil society groups etc.) to enhance their preparedness to attacks on public spaces;
- Enhanced modelling capabilities for security practitioners and policy-makers due to the identification of potential new vulnerabilities and data available, and improved support to planning of respective resources and activities.

Scope: Public spaces such as squares, sport venues, shopping districts, places of worship, and mass transport systems have been the target of terrorist attacks causing significant loss of lives and causing societal insecurity. The means to carry out such attacks from one or several attackers range from sophisticated and well-planned scenarios including several attackers using explosives and firearms, up to so called low-cost attacks making use of everyday goods. Today specific urban furniture like benches, bus shelters, flower boxes, etc. already have double functions controlling access to protected areas, which answers to some of the low cost attacks. The next logical step seems to expand their functions further and adopt new functionalities to better respond to the terrorist threats, such as for CBRN ones. Over the last several years numerous nationally and EU funded projects such as EU-SENSE, TERRIFFIC, PROACTIVE or ChemSniff developed scenarios and sensors capable of improving citizens safety and security. 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

[20] This budget is shared with topic HORIZON-CL3-2024-FCT-01-01, HORIZON-CL3-2024-FCT-01-02, HORIZON-CL3-2024-FCT-01-03, HORIZON-CL3-2024-FCT-01-04, HORIZON-CL3-2024-FCT-01-06, HORIZON-CL3-2024-FCT-01-07, HORIZON-CL3-2024-FCT-01-08

of existing sensors within the public spaces small architecture. Traditional sensors and surveillance systems like ANPR, cameras or image analysis systems are not in the scope of this topic unless their integration with new sensors is considered, and added value of networked systems demonstrated. Proposals should present relevant challenges and opportunities for future applications of CBRN detection capacities in small architecture, including prospects of scalability, real-time processing, and cooperation of networked systems.

FCT05 – Organised crime prevented and combated

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-06: Environmental impact of illicit drugs production

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 37.00 million.[21]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Assessment of the full impact of illicit drug production on the environment;
- Development of innovative tools and methodologies to detect and prevent environmental impact related to illicit drug production and trafficking;

Development of effective and cost efficient disposal of seized drugs precursors and other chemicals and equipment used in illicit drug production.

Scope: Negative impacts of illicit drug production and trafficking such as violent criminality, loss of human lives, addiction, or individual and/or community social costs are commonly known. However drug production has also a huge impact on the environment in forms of excessive carbon footprint and water stress, deforestation, use of herbicides while counter-fighting drug plantations, disposal of unprocessed hazardous chemicals (by-products of drugs synthesis) and pollution of air, soil and water. Having in mind that the market for illegal drugs in Europe is big and either stable (cannabis, heroin) or grows (cocaine, synthetic drugs)[22]

[21] This budget is shared with topic HORIZON-CL3-2024-FCT-01-01, HORIZON-CL3-2024-FCT-01-02, HORIZON-CL3-2024-FCT-01-03, HORIZON-CL3-2024-FCT-01-04, HORIZON-CL3-2024-FCT-01-05, HORIZON-CL3-2024-FCT-01-07, HORIZON-CL3-2024-FCT-01-08

[22] EMCDDA 2020, European Drug Report, Trends and Developments 2020, accessible at https://www.emcdda.europa.eu/publications/edr/trends-developments/2020_en

coupled with the fact that for example production of a kilo of pure MDMA, the main substance in ecstasy, results in some 10 kilos of toxic waste — or some 30 kilos in the case of amphetamines we are facing a serious environmental problem, directly effecting health of EU citizens. At the same time even legally produced drugs like cannabis have serious impact on local water and energy balance. Moreover, each year increasing tones of illicit drugs are being confiscated by law enforcement across the EU, together with the dismantling of labs for synthetic drugs. In this context, aspects related to the handling and destruction of seized illicit drugs, drug precursors and other chemicals and equipment used in illicit drug production, as well as the ecological disposal of the resulting waste need to be considered in the proposals[23]. Coordination among the successful proposals from this topic as well as with the successful proposal under topic HORIZON-CL3-2024-FCT-01-07: *Counterfeiting pharmaceutical products* should be envisaged to avoid duplication, and to exploit complementarities as well as opportunities for increased impact.

HORIZON-CL3-2024-FCT-01-07: Counterfeiting pharmaceutical products

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 37.00 million.[24]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Intelligence gathering on the scale of the phenomena and types of pharmaceutical products targeted;
- Identifications and analysis of modus operandi, effected markets and entry points for these markets;
- Gap analysis of mitigation measures towards major threat factors of the substandard and counterfeited pharmaceutical, including recommendations at policy, operational and societal level;
- Development of investigative techniques and methodologies for better detection and counteraction to production and proliferation of counterfeit medicines;

[23] EU Drugs Strategy 2021-2025

[24] This budget is shared with topic HORIZON-CL3-2024-FCT-01-01, HORIZON-CL3-2024-FCT-01-02, HORIZON-CL3-2024-FCT-01-03, HORIZON-CL3-2024-FCT-01-04, HORIZON-CL3-2024-FCT-01-05, HORIZON-CL3-2024-FCT-01-06, HORIZON-CL3-2024-FCT-01-08

Recommendation on prevention of misuse of easy entry points (e.g.: small parcels) into regulated markets like Europe.

Scope: Criminal involvement in the manufacture and distribution of counterfeit pharmaceutical products is driven by high profits, relatively low risks of detection and low penalties in case of prosecution. At the same time, specific consumers are vulnerable for deception. This phenomenon is of a significant relevance as it simultaneously threats a number of values: negatively impacting individuals (with adverse effects from incorrect active ingredients, failure to cure existing diseases, generate loss of confidence in health systems), producers (loss of income and reputation, the potential cost of managing the disposal of counterfeits), state economies (loss of tax revenues, jobs), additional stress on public health systems and environmental impact of chemical waste and other hazardous materials from substandard and falsified medical products. Recent data shows that distribution of pharmaceutical goods is increasingly shifting from physical to online markets including dedicated platforms such as online pharmacies as well as social media services. Most trading activity is believed to take place via official web services. However, some pharmaceutical products are also distributed via dark web platforms. There are known examples of legitimate companies served as a shield for trade in counterfeit pharmaceuticals. Coordination among the successful proposal from this topic as well as with the successful proposals under topic HORIZON-CL3-2024-FCT-01-06: *Environmental impact of illicit drugs production* should be envisaged to avoid duplication, and to exploit complementarities as well as opportunities for increased impact. 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, in order to produce meaningful and significant effects enhancing the societal impact of the related innovation activities.

FCT06 – Citizens are protected against cybercrime

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-FCT-01-08: Tracing of cryptocurrency transactions

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 37.00 million.[25]
Type of Action	Innovation Actions

[25] This budget is shared with topic HORIZON-CL3-2024-FCT-01-01, HORIZON-CL3-2024-FCT-01-02, HORIZON-CL3-2024-FCT-01-03, HORIZON-CL3-2024-FCT-01-04, HORIZON-CL3-2024-FCT-01-05, HORIZON-CL3-2024-FCT-01-06, HORIZON-CL3-2024-FCT-01-07

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Limiting the attractiveness of cryptocurrencies for illegal money transfers with better tractability of cryptocurrency transactions;
- Propose lawful tools and methods for Police Authorities to trace virtual currency transactions;
- Recommendations for better policies and regulation of the cryptocurrencies market;
- Development of training curricula for Police Authorities, Prosecutors, as well as judicial actors on tracing, seizing and handling cryptocurrencies in the course of investigation.

Scope: Cryptocurrencies are a widely used method by criminals to transfer funds due to their anonymity, ease of use and lack of international borders and restrictions, exactly these things that make use of traditional bank routes difficult. With the raise of crime-as-a-service market, and growth in the number of connected transactions, use of cryptocurrency as one of the money loundering typology better tracing of cryptocurrency transactions is crucial to keep the ground in the fight against crime. On top of it all, clandestine cryptocurrency activities are increasingly facilitated by new developments such as high privacy decentralised exchanges, which while used by perpetrators frustrate the efforts of Police Authorities to detect and recover criminal assets as well as to prevent fraudulent transactions. 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. It is key that innovation explores these options and proposes mitigation measures, from legal, organisational, and technical perspectives (including the development of tools and relevant trainings to trace decentralized and privacy-oriented currency). Proposals should build on finding and outcomes of former nationally and EU funded projects like TITANIUM, TRACE, and Anti-FinTer. Coordination among the successful proposal from this topic as well as with the successful proposals under topic HORIZON-CL3-2023-FCT-01-08: *Crime as a service* should be envisaged to avoid duplication, and to exploit complementarities as well as opportunities for increased impact.

Destination - Effective management of EU external borders

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024:

"Legitimate passengers and shipments travel more easily into the EU, while illicit trades, trafficking, piracy, terrorist and other criminal acts are prevented, due to improved air, land and sea border management and maritime security including better knowledge on social factors."

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Improved security (as well as better cost- and energy- efficient management) of EU land and air borders, as well as sea borders and maritime environment, infrastructures and activities, as well as for the EU external civilian security, against accidents, natural disasters and security challenges such as illegal trafficking, piracy and potential terrorist attacks, cyber and hybrid threats;
- Improved border crossing experience for travellers and border authorities staff (including customs, coast and border guards), while maintaining security and monitoring of movements across air, land and sea EU external borders, supporting the Schengen space, reducing illegal movements of people and goods across those borders and protecting fundamental rights of travellers, both EU citizens and Third Country Nationals;
- Improved customs and supply chain security though better prevention, detection, deterrence and fight of illegal activities involving flows of goods across EU external border crossing points and through the supply chain, as well as through better interoperability, minimising disruption to trade flows.

The following call(s) in this work programme contribute to this destination: [...]

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-BM-01	28.82		23 Nov 2023
HORIZON-CL3-2024-BM-01		29.00	
Overall indicative budget	28.82	29.00	

Call - Border Management 2023

HORIZON-CL3-2023-BM-01

Conditions for the Call

Indicative budget(s)[26]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[27]	Number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-BM-01-01	RIA	28.82	Around 3.00	2
HORIZON-CL3-2023-BM-01-02	RIA		Around 5.00	1
HORIZON-CL3-2023-BM-01-03	IA		Around 4.00	2
HORIZON-CL3-2023-BM-01-04	CSA		Around 1.30	1
HORIZON-CL3-2023-BM-01-05	IA		Around 5.00	1
HORIZON-CL3-2023-BM-01-06	IA		Around 3.00	1
Overall indicative budget		28.82		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.

[26] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

[27] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

BM01 – Efficient border surveillance and maritime security

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-BM-01-01: Capabilities for land border surveillance and situational awareness

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[28]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Increased land border surveillance capabilities, better performing and more cost-efficient, with data and fundamental rights protection by design.
- Better surveillance of land border areas, supporting fight against illegal activities across external borders, as well as safety of people and operators in the border areas, including favouring border crossings through border crossing points.

[28] This budget is shared with topic HORIZON-CL3-2023-BM-01-02, HORIZON-CL3-2023-BM-01-03, HORIZON-CL3-2023-BM-01-04, HORIZON-CL3-2023-BM-01-05, HORIZON-CL3-2023-BM-01-06

- More efficient and more flexible solutions, including relocation and rapid deployment capabilities, comparable to physical barriers to deter and monitor irregular border crossings outside border crossing points.

Scope: External land borders of the European Union and of the Schengen area present some and different border surveillance challenges, ranging from those closer to the Mediterranean, to the Nordic Countries external land borders, which may lead to difficulties in efficiently monitor them, deterring illegal activities across the external borders, as well as trafficking of human beings and exploitation of irregular migration that avoid border crossing points.

Furthermore, the border surveillance capabilities needs along land borders may change in time, often just within a year or a season, and/or need to respond and adapt with relatively short notice. Solutions must hence allow to re-orient capacity and resources accordingly (through physical portability and/or other approaches).

Cooperation for surveillance along land borders require compatibility and interoperability among legacy and planned systems. Proposed solutions should allow higher interoperability cross-border among EU and Associated Countries practitioners, cross-systems and multi-authority.

Compatibility and integration with the European Border Surveillance System (EUROSUR) is needed, and compatibility and/or exploitation of other information sharing environments would be an additional asset.

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): networked deployable, and possibly mobile, semi-autonomous surveillance towers; IoT and advanced mesh connectivity; Virtual and Augmented Reality for enhanced C2 and situational awareness; integrated wide area RPAS management; passive, low-energy systems; artificial intelligence.

Equipment and technologies enabling land border surveillance need to contribute to cost and energy efficiency, limit their environmental impact and being more and more sustainable when they will be taken up in the future. This may be addressed, for example, by integrating opportunities of circular economy, self-sustained equipment, lower emissions and/or environmental footprints.

The proposed solutions should ensure secure data collection, access, encryption and decision support processes.

EU authorities should plan to take up the results of the research, should it deliver on its goals and compatibly with applicable legislation, with the support of the Border Management and Visa Instrument (BMVI).

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other Framework Programmes projects. In particular, proposals should build on achievements and findings or relevant recent EU-funded civil security research projects such as FOLDOUT, ROBORDER, ANDROMEDA and BorderUAS,

as well as projects from topic *HORIZON-CL3-2021-BM-01-01: Enhanced security and management of borders, maritime environment, activities and transport, by increased surveillance capability, including high altitude, long endurance aerial support*, and other relevant research.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals.

Proposals under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) starting from the design of their work, and engage with the Agency in the development of the project. Proposals should give a key role to Frontex in validating the project outcomes, with the aim of facilitating future uptake of innovations for the border and coast guard community.

Cross-community and cross-authority synergies within civil security can be an asset, for example with Fight Crime and Terrorism (regarding combating crime across external borders) and Disaster Resilience Societies (regarding natural hazards and disasters).

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-BM-01-02: Identify, inspect, neutralise Unexploded Ordnance (UXO) at sea

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[29]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Increased capabilities to map, detect, classify, inspect, assess and neutralise UXO at sea.
- Improved safety and security for maritime economic operators and for EU citizens.

Scope: A large amount of Unexploded Ordnance (UXO), as well as old mines, estimated by experts in the tens of thousands tons, lay in European seas and often close to European shores. Most of this material dates back to the World Wars. Estimates for the timing of material

[29] This budget is shared with topic HORIZON-CL3-2023-BM-01-01, HORIZON-CL3-2023-BM-01-03, HORIZON-CL3-2023-BM-01-04, HORIZON-CL3-2023-BM-01-05, HORIZON-CL3-2023-BM-01-06

corrosion suggest that much of this material is likely to be an increasing safety risk in the next 10 to 20 years. And this would happen while coasts, shores and seas have more and more value for economic and civilian activities, from communications to transport to trade to sustainable energy production. UXO hence represent a substantial safety risk for economic operators at sea, citizens, as well as for the environment.

UXO represent also a security risk, as some of this dangerous material is relatively easily retrievable and could be misused in illicit, including criminal and terrorist, acts. These security threats could be linked directly to maritime security and infrastructures (to deny or ransom a port, for example), or be moved towards other illicit acts.

Roles and responsibilities to map, identify, assess, inspect, retrieve and/or neutralise UXO vary among Member States, between private operators, local and regional governments, national governments, and the military that carry out civilian tasks.

Current capabilities on mapping, identifying, assessing, inspecting, retrieving and/or neutralising UXO still largely use human operators, and increased use of automated and/or unmanned systems would be desirable for efficiency and safety reasons.

The proposed project should improve capabilities on: a) enabling knowledge (mapping and integrating data from historical maps and more recent data, including reports from sea operators); comparative analysis of legislation, roles and responsibilities in Member States); b) detection (of UXO on and below the marine sediment/seabed, being able to detect also buried objects); c) identification, classification, assessment (identifying chemical and material aspects; sensing levels of corrosion). Proposals that include solutions also on one or more of the following aspects would be desirable: a) inspection and handling (grab and manipulate UXO under water, from intact shells to chunks to small parts; collect and recovery); b) neutralisation and disposal (containment of chemical spill-overs and possible explosions).

The involvement of civilian stakeholders, beyond civilian authorities, such as operators on sea, is strongly encouraged.

Proposed solutions should be compatible or interoperable with legacy and current systems, and propose or allow an interoperability between systems in use by different Member States.

Proposed solutions that would improve energy efficiency and environmental impact aspects of current UXO risk mitigation operations (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment) would be desirable.

Synergies with the topic on trustworthy AI for security applications (SSRI) should be taken into account.

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): sonars and other sensors; UxVs/AUVs; on-board analytical capabilities for material samples; hydroacoustic profiling; artificial intelligence for detection and classification; wing tows from ships; system of systems architecture.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other Framework Programmes projects and/or other EU projects such as BASTA and EXPLOTEC.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals.

Synergies within civil security can be an asset, for example with Fight Crime and Terrorism (regarding combating organised crime and terrorism) and Disaster Resilience Societies (regarding environmental contamination).

BM02 – Secured and facilitated crossing of external borders

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-BM-01-03: Beyond the state-of-the-art "biometrics on the move"

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[30]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Updated, European-based, knowledge and development on biometrics technologies that could be used for identification of travellers crossing external EU borders.
- Maximisation of travellers' experience and of security reassurances, minimizing false positives and handling of personal data.
- Contribute to capabilities that strengthen the Schengen area, by providing security at its external borders that also reassure on maintaining the free movement within its borders.

Scope: Biometrics are one of the most usable and most reliable ways to validate the identity of an individual. Biometrics that are traditionally used in the context of border controls include fingerprints and 2D facial images; other biometrics are also used for identity management

[30] This budget is shared with topic HORIZON-CL3-2023-BM-01-01, HORIZON-CL3-2023-BM-01-02, HORIZON-CL3-2023-BM-01-04, HORIZON-CL3-2023-BM-01-05, HORIZON-CL3-2023-BM-01-06

outside the European Union, or at national level, such as iris; and further others are used in other applications in the private sector and in consumer market.

As for many other technologies, applications of biometrics to improve capabilities in civil security, such as in the border management or law enforcement sectors, may have higher requirements than applications in the consumer market, in terms of reliability, usability, and strict minimization of risks to personal data protection and fundamental rights, as well as to risks of bias or discrimination.

Research should assess and develop the fit-for-purpose for border management of biometric identification modalities beyond fingerprints and facial images, and/or innovative modalities of acquisition of those and other biometrics. Proposed project(s) should particularly investigate biometrics modalities that currently do not offer satisfactory performance (in terms of reliability, usability data protection risk minimization, bias risk minimisation, etc.) for application in a border checks context.

Any biometric modality or acquisition modality innovation should imply improvements on acquisition, processing and validation, compared to the state-of-the-art, "on the move" (i.e. while the traveller is moving), contactless and at a distance of up to one meter, and/or of both travellers crossing borders inside or outside vehicles. The solution(s) should be compatible with different groups of (informed and voluntarily enrolled) travellers, EU/EES citizens and/or of Third Country National at border crossing points.

The proposed solution(s) must include data protection, fundamentals rights protection and privacy by design. Developed solutions should indeed help to minimizing the need and use of biometric data to achieve an acceptable reliability of identification, including by acquiring and using less personal data compared to the state-of-the-art.

The project should also study if and how it would be possible securely and privacy-friendly "re-use" collected biometrics.

The proposed solution(s) should foresee modular integration with health checks – such as in the case of pandemics – as temperature, which can be performed by border staff.

The proposed solution(s) should include automated decision support system for the biometric recognition business process that suggest the end-users (border checks operators) which procedure, technology or database can be used without infringing rights of travellers.

Synergies with the topic on trustworthy AI for security applications (SSRI) should be taken into account.

EU authorities should plan to take up the results of the research, after the project and should it deliver on its goals and compatibly with applicable legislation, with the support of the Border Management and Visa Instrument (BMVI).

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): palm vein, 3D facial images, periocular biometrics, other biometrics modalities, sensors, artificial intelligence.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other recent EU Framework Programmes projects on security research such as iMARS, D4FLY, and projects funded under *HORIZON-CL3-2021-BM-01-03: Improved border checks for travel facilitation across external borders and improved experiences for both passengers and border authorities' staff* and *HORIZON-CL3-2022-BM-01-02: Enhanced security of, and combating the frauds on, identity management and identity and travel documents*.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals.

Proposals under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) starting from the design of their work, and engage with the Agency in the development of the project. Proposals should give a key role to Frontex in validating the project outcomes, with the aim of facilitating future uptake of innovations for the border and coast guard community.

HORIZON-CL3-2023-BM-01-04: Reliability of age assessments in a border management context

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 1.30 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[31]
Type of Action	Coordination and Support Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved adaptation, preparedness and cooperation of border and police authorities in the fight against human trafficking.
- Expanded knowledge base on reliability and efficiency of methods of age assessment.

[31] This budget is shared with topic HORIZON-CL3-2023-BM-01-01, HORIZON-CL3-2023-BM-01-02, HORIZON-CL3-2023-BM-01-03, HORIZON-CL3-2023-BM-01-05, HORIZON-CL3-2023-BM-01-06

- Improved protection of minors, including by more reliable assessment and by minimising the use of medical and invasive age assessment methods
- Improve the exchange and alignment of practices among European authorities.

Scope: Many unaccompanied children and young people arriving at the external EU borders and seeking asylum, lack official documents showing their identity and age. Age assessment is important as it determines where an individual will be initially housed and what services, supports, and legal processes they will receive to ensure protection and child protection.

The number of unaccompanied children, which has exploded in the last five years, confronts border management practitioners with new problems and accentuates existing ones.

Currently there is no age assessment process, medical or non-medical, with a 100% reliability. Furthermore, there is considerable variation in practices and methods of age assessment in a border management context in Member States. Non-medical approached may include interviews, phychological assessments and other holistic approaches; medical approaches may include X-rays, DNA methylation or other analyses. EU regulations, and guidelines by EASO[32] or documents by the European Migration Network, include safeguards and recommendations, such as that the least invasive methods should be used, and that medical methods should be used as a last resort.

This Cooperation and Support Action should do research, include literature review and research with practitioners, on current and potential practices for age assessment in a border management context. It should assess and compare scientific reliability and specificity of different methods, as well as their risks for fundamental rights and for invasiveness. While the research results would not necessarily imply any legislative or policy decision on age assessment methods in the border management context, the research will develop evidence-based results on options for more (compared to the state-of-the-art) child-sensitive models of age assessment in the context of border management, that protect fundamental rights.

Synergies within civil security can be an asset, for example with Fight Crime and Terrorism.

BM03 – Better customs and supply chain security

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-BM-01-05: Interoperability of systems and equipment at tactical level; between equipment and databases; and between databases of threats and materials

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately.

[32] EASO. Age assessment practices in EU+ countries: updated findings (europa.eu)

	Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[33]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Increased interoperability of existing (and foreseeable upcoming) customs control equipment at tactical level, multi-supplier, multi-authority and cross-border.
- More efficient and quicker availability, for EU customs practitioners, of reference data (spectra etc.) on threats and materials.
- Building capabilities for a more harmonised European application of customs controls based on risk management and trade facilitation.

Scope: European customs, as all operators and citizens, also work in our increasingly digitalised and interconnected world of equipment, systems, and data. On the one hand, this opens opportunities to harness their capacity and information to improve trade facilitation while protecting the security and safety of citizens as well as the EU's economy. On the other hand, the proliferation of equipment, system and data, often from different suppliers and in different bases, may also present challenges in terms of interoperability and an efficient management of flows of goods across the external borders of the Custom Union. Furthermore, the strategy of the "European custom union acting as one" implies that equipment are used by other authorities beyond customs; that equipment, including mobile one, is shared among Member States to increase cooperation and collaboration on checking flows of goods across European borders, and that standards and technical specifications for customs control equipment are harmonised.

Another challenge for European customs control capabilities is the rapid availability of, and rapidly shared, data references for (new) threat and illicit materials.

All this calls for research and innovation for solutions that prepare and increase the interoperability of customs control equipment and data at "tactical" level, in terms of multi-authority, cross-border, multi-supplier interoperability as well as linkages among Member States and Commission systems, and the more rapid availability and sharing of libraries of reference data for target substances or materials. There is room for innovation to improve access to updated spectra (or other formats or references) of target substances and materials when they appear; easily make them available to customs' devices; and improve data for libraries.

The solution(s) proposed under this topic should define the requirements and way forward to enable and enhance the interoperability of customs control equipment and of data used in

[33] This budget is shared with topic HORIZON-CL3-2023-BM-01-01, HORIZON-CL3-2023-BM-01-02, HORIZON-CL3-2023-BM-01-03, HORIZON-CL3-2023-BM-01-04, HORIZON-CL3-2023-BM-01-06

different Member States and/or by different authorities at national level, as well as Commission systems.

The proposed solution(s) should address how to make libraries of data references on target substances and materials more rapidly available and shared to authorities; to update and share them faster, though securely; to enable quicker tackling of illegal substances and materials, either innovating current approaches or designing altogether new approaches for reference libraries.

The results of the research should be taken up by EU customs authorities in the framework of the Customs Union "acting as one", with the support of the Customs Control Equipment Instrument (CCEI). The CCEI will enable not only the possibility to establish harmonisation through common standards and technical specifications but will offer access to actively fund equipment across the Member States to fulfil these common standards.

The proposed solution must include privacy enhancing techniques to allow the sharing of tools without the sharing of data beyond what is strictly necessary. Leakage or compromising of personal data must be avoided in the transfer of tools or models.

Synergies with the topic on trustworthy AI for security applications (SSRI) should be taken into account.

Improving energy efficiency and environmental impact aspects of new security technologies for this capability (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment).

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): blockchain/DLT, artificial intelligence; spectroscopy, data fusion.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other recent EU Framework Programmes projects on security research such as PROFILE.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals.

Proposals under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) starting from the design of their work, and engage with the Agency in the development of the project. Proposals should give a key role to Frontex in validating the project outcomes, with the aim of facilitating future uptake of innovations for the border and coast guard community.

HORIZON-CL3-2023-BM-01-06: Increased security for air cargo

Specific conditions

Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[34]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Increased security of air cargo, including hold baggage and larger cargo clusters, to accidental or intentional explosion, noxious chemicals, or other material degradation.

Scope: The importance and reliability of air cargo for international trade further increased in the last years, and it is likely to remain critical after the COVID-19 pandemic. Air cargo can also represent continuity assurances to cope, at least in the short term and for critical lines, with supply chain and/or distribution crises. The context however presents security challenges as well as high potential consequences of threats, primarily but not limited to explosives.

Equipment and technologies enabling increased security of air cargo need to contribute to cost and energy efficiency, limit their environmental impact and being more and more sustainable when they will be taken up in the future. This may be addressed, for example, by integrating opportunities of circular economy, self-sustained equipment, lower emissions and/or environmental footprints. An increased security of air cargo, furthermore, should not be regarded as an incentive to use air transport when this has a higher environmental and emissions impact, but prioritised on critical supply lines and/or situations.

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): blast containment and other passive technology, smart active defuse systems, sensors, artificial intelligence.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other recent EU Framework Programmes projects on security research such as EUROSKY, FLY-BAG, FLY-BAG2, CORE.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals.

Synergies within civil security can be an asset, for example with Fight Crime and Terrorism and Resilient Infrastructures.

[34] This budget is shared with topic HORIZON-CL3-2023-BM-01-01, HORIZON-CL3-2023-BM-01-02, HORIZON-CL3-2023-BM-01-03, HORIZON-CL3-2023-BM-01-04, HORIZON-CL3-2023-BM-01-05

Call - Border Management 2024

HORIZON-CL3-2024-BM-01

Conditions for the Call

Indicative budget(s)[35]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[36]	Number of projects expected to be funded
		2024		
Opening: na				
HORIZON-CL3-2024-BM-01-01	IA	29.00	Around 6.00	1
HORIZON-CL3-2024-BM-01-02	IA		Around 3.00	1
HORIZON-CL3-2024-BM-01-03	IA		Around 5.00	1
HORIZON-CL3-2024-BM-01-04	IA		Around 5.00	1
HORIZON-CL3-2024-BM-01-05	IA		Around 4.00	2
Overall indicative budget		29.00		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.

35 The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

36 Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

BM01 – Efficient border surveillance and maritime security

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-BM-01-01: Interoperability for border and maritime surveillance and situational awareness

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[37]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Increased border surveillance capability, better performing and more cost-efficient, with data and fundamental rights protection by design.
- Improved surveillance and situational awareness of sea borders, but also of maritime infrastructures as harbours and commercial/civilian maritime security along sea lines of communication.
- Improved multi-level, multi-authority and cross-border (among EU/AC practitioners) collaboration thanks to better interoperability of sensing, analysis and C2 systems.

Scope: Authorities performing surveillance of maritime borders and maritime wide areas use a range of technologies, and receive a range of information, to monitor wide areas, detect threats or crises, and respond to them. However, these inputs are not always merged into common command-and-control (C2) systems that can inform rapid decision-making.

[37] This budget is shared with topic HORIZON-CL3-2024-BM-01-02, HORIZON-CL3-2024-BM-01-03, HORIZON-CL3-2024-BM-01-04, HORIZON-CL3-2024-BM-01-05

The proposed solution(s) should allow improved interoperability (at both back-end and front-end levels), independently of the supplier of the equipment, and ideally interchangeability that enables exchange of information among authorities that use different systems.

The proposed solution(s) can include the design of open architecture C2 systems, including open standards for APIs and data models.

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, 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).

While the project will mainly focus on enabling capabilities through interoperability and interchangeability, proposals that in the process aim at advancing certain technological components, and integrating them into the solution, are welcome.

EU authorities should plan to take up the results of the research, after the project and should it deliver on its goals and compatibly with applicable legislation, with the support of the Border Management and Visa Instrument (BMVI).

Proposed solution(s) should improve energy efficiency and environmental impact aspects of new security technologies for this capability (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment).

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): open architecture, standardisation, user interface and experience, artificial intelligence, UxV or fixed sensors, vessels-as-sensors, IoT (beyond vessels), advanced mesh connectivity, automated analysis of abnormal or non-cooperative vessels' behaviour, Virtual and Augmented Reality, integrated wide area RPAS management, over-the-horizon detection technologies.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other recent EU Framework Programmes projects on security research such as CAMELOT, COMPASS2020, EFFECTOR, PROMENADE, NESTOR.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals.

Proposals under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) starting from the design of their work, and engage with the Agency in the development of the project. Proposals should give a key role to Frontex in validating the project outcomes, with the aim of facilitating future uptake of innovations for the border and coast guard community.

Synergies within civil security can be an asset, for example with Disaster Resilient Societies and Fight Crime and Terrorism.

HORIZON-CL3-2024-BM-01-02: Prevent and mitigate piracy, hijacking, attacks, or kidnapping of crew, for ships

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[38]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Increased security of ships, vessels, crews and passengers to threats of piracy, kidnapping, hijacking or attacks.
- Increased deterrence to criminal or terrorist acts against commercial ships
- Mitigated safety and security risks on seafarers, passengers, economy and the environment.

Scope: Improved capabilities are needed to help protecting fleets and maritime lines from criminal acts and harassment. Protecting seafarers, merchant shipping and cruise ships and securing Europe's maritime trade and supply lines need updated and cost effective solutions.

This topics aims at improving civilian capabilities for the protection of European civilian passengers and merchant ships from piracy, hijacking of vessels and/or kidnapping of crew, and for mitigating the consequences of such threats.

The proposed solution(s) should be able to both detect and defuse cyber-attacks against ships' operating systems, and to provide passive physical security and safety systems.

[38] This budget is shared with topic HORIZON-CL3-2024-BM-01-01, HORIZON-CL3-2024-BM-01-03, HORIZON-CL3-2024-BM-01-04, HORIZON-CL3-2024-BM-01-05

Proposed solution(s) should be compatible or interoperable with legacy and current systems, and propose or allow an interoperability between systems in use by different Member States.

Proposed solution(s) should improve energy efficiency and environmental impact aspects of new security technologies for this capability (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment).

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): counter-RPAS for ships, security "citadels", sirens and emergency or alarm technologies.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other recent EU Framework Programmes projects on security research such as SECTRONIC, PROMERC, iPATCH, ISOLA.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals.

Synergies within civil security can be an asset, for example with Fight Crime and Terrorism.

BM02 – Secured and facilitated crossing of external borders

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-BM-01-03: Advanced user-friendly, compatible, secure identity and travel document management

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[39]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved capabilities to validate breeder and identity documents as well as Type 1 and Type 2 digitalised travel documents.

[39] This budget is shared with topic HORIZON-CL3-2024-BM-01-01, HORIZON-CL3-2024-BM-01-02, HORIZON-CL3-2024-BM-01-04, HORIZON-CL3-2024-BM-01-05

- Improved compatibility among tools while guaranteeing not sharing (beyond what's strictly necessary) or compromising personal data.
- Enhanced integration with EU current or planned architecture(s) for digital wallets.
- Contribute to capabilities that strengthen the Schengen area, by providing security at its external borders that also reassure on maintaining the free movement within its borders.

Scope: Facilitation of crossing borders (for the European Union, the external Schengen borders), and of travel across those borders went and is further going through remarkable developments thanks to subsequent technological generations, and updated procedures and regulatory frameworks. From automated border control gates, to "no gate" solutions, to "seamless travel", from secure documents, to digitalised travel documents to "dematerialised travel documents" and "digital wallets". All to ease border crossing for travellers, while maintaining border security against illicit or irregular crossings and protecting privacy and fundamental rights. This topic aims at exploring and developing capabilities for the security of digitalised identity documents used for travel across external borders.

The proposed solution must 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 legacy and current systems, and propose or allow an interoperability between systems in use by different Member States.

The operational applicability focus should be on highly digitalised documents and "digital identity management" used for travel across external borders. However, the research should not forget the security of breeder documents, which risk to be "weak links" when they are used to obtain genuine, secure travel documents.

Authentication of documents is relevant for border management, immigration or visa applications. Furthermore, it could also be relevant to combat other illicit activities, such as financial fraud.

The proposed solution must include privacy enhancing techniques to allow the sharing of tools without the sharing of data beyond what is strictly necessary. Leakage or compromising of personal data must be avoided in the transfer of tools or models.

The proposed solution 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.

The proposed solution should include an automated decision support system that suggest the end-users such as border authorities staff which process and database/tool can be legally used with or by a certain technology or database.

The developed solutions need to comply with the Ethics Guidelines on Trustworthy AI (2019).

EU authorities should plan to take up the results of the research, should it deliver on its goals and compatibly with applicable legislation, with the support of the Border Management and Visa Instrument (BMVI).

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other Framework Programmes projects. In particular, proposals should build on achievements and findings or relevant recent EU-funded civil security research projects such as iMARS and project(s) funded under *HORIZON-CL3-2022-BM-01-02: Enhanced security of, and combating the frauds on, identity management and identity and travel documents*.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals.

Proposals under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) starting from the design of their work, and engage with the Agency in the development of the project. Proposals should give a key role to Frontex in validating the project outcomes, with the aim of facilitating future uptake of innovations for the border and coast guard community.

Cross-community and cross-authority synergies within civil security can be an asset, for example with Fight Crime and Terrorism (regarding combating crime involving identity misrepresentation).

HORIZON-CL3-2024-BM-01-04: Integrated risk-based border control that enhance public security risk mitigation while reducing false positives and strengthening privacy

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[40]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved border crossing assisted control systems, coordinated between border, customs and security controls.

[40] This budget is shared with topic HORIZON-CL3-2024-BM-01-01, HORIZON-CL3-2024-BM-01-02, HORIZON-CL3-2024-BM-01-03, HORIZON-CL3-2024-BM-01-05

- Allocate more efficiently border check resources, maintaining security while minimise time and hassle for crossings and false positives.
- Being able to flexibly allocate border check resources, when and where needed, depending on changing needs (for example seasonally).
- Contribute to capabilities that strengthen the Schengen area, by providing security at its external borders that also reassure on maintaining the free movement within its borders.

Scope: Growth of international travel and mobility, which will catch up and likely increase to the pre-COVID-19 pandemic levels, the scarcity of resources, and the need to ease border crossings while maintaining security of the Schengen area, make reliable risk assessments and border checks prioritisation important. Border practitioners in some Member States are assessing feasibility, reliability and acceptability of optimising border controls using risk-based management.

The solution(s) proposed under this topic must allow easier and more flexible allocation and change of resources in border checks, for example basing on seasonal peaks. A possible use case of focus is that of roll-on-roll-off ferries. That situation may generate long queues for border and security checks, while often being seasonal. A proposed solution should help performing border checks, as well improving speed to detecting threats in vehicles, especially weapons and explosives, without people coming out of vehicles and without slowing down (dis)embarkment onto and off roll-on-roll-off ferries.

In any case, the proposed solution(s) should consider both the travellers and the goods accompanying them.

Higher leveraging of risk management in border crossing practices has the potential to also decrease and minimise the use of personal data and the risks for privacy and fundamental rights. However, the project should integrate strong ethical, legal and acceptability assessment to ensure that, on the other hand, the risks of bias and discrimination of risk mitigation is minimised.

Collaboration with international stakeholders in the field of transport and transport safety in the air, maritime and rail contexts is encouraged.

EU authorities should plan to take up the results of the research, after the project and should it deliver on its goals and compatibly with applicable legislation, with the support of the Border Management and Visa Instrument (BMVI).

Synergies with the topic on trustworthy AI for security applications (SSRI) should be taken into account.

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.

The system should include automated decision support system that suggest the end-users which process and database/tool can be legally used with or by a certain technology or database.

Solutions should be compatible or interoperable with legacy and current systems, and propose or allow an interoperability between systems in use by different Member States.

Proposed solution(s) should improve energy efficiency and environmental impact aspects of new security technologies for this capability (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment).

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): risk assessment methods, data fusion, sensors, artificial intelligence.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other recent EU Framework Programmes projects on security research such as TRESSPASS, or XP-DITE

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals.

Proposals under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) starting from the design of their work, and engage with the Agency in the development of the project. Proposals should give a key role to Frontex in validating the project outcomes, with the aim of facilitating future uptake of innovations for the border and coast guard community.

Synergies within civil security can be an asset, for example with Fight Crime and Terrorism.

BM03 – Better customs and supply chain security

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-BM-01-05: Detection and tracking of illegal and trafficked goods

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[41]

[41] This budget is shared with topic HORIZON-CL3-2024-BM-01-01, HORIZON-CL3-2024-BM-01-02, HORIZON-CL3-2024-BM-01-03, HORIZON-CL3-2024-BM-01-04

Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Contributing to development of fully automated customs control checkpoints.
- Enhancing detection capabilities for customs security, while facilitating trade.

Scope: European customs need improved capabilities that allow bettering and automatically detecting from traces, interpreting images from scanned cargo, interpreting data, tracking goods, and/or identifying anomalies that support the detection of threats, smuggling or illicit trade eliminating or minimizing disruption to the trade flow. The proposed system should hence advance and/or combine as much as possible the components of detection, tracking and risk-based anticipation.

The proposed solution(s) could include trustworthy algorithms for recognition that minimise false positives and biases.

On detection, proposed research could include image (shape) recognition and interpretation, and/or a tracking approach.

The proposed solution(s) should 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.

The research can also propose and explore technologies for the improved traceability of goods and items that could be illicitly trafficked using non-invasive markings.

The research project can test one or more specific use cases, such as (non-exhaustive examples): art, cultural goods, waste and other environmentally-risky material, valuables, dangerous items either assembled or disassembled.

Proposed solution(s) should improve energy efficiency and environmental impact aspects of new security technologies for this capability (e.g. low environmental footprint, low emissions, circular economy aspects and/or self-sustained equipment).

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): scanning (vision), detectors (traces), nanotechnology, blockchain/DLT, artificial intelligence.

Research projects should consider, build on (if appropriate) and not duplicate previous research, including but not limited to research by other recent EU Framework Programmes projects on security research such as ENTRANCE, SilentBorder, MULTISCAN3D.

Proposals should delineate the plans for further development to subsequent TRLs as well as uptake (industrialisation, commercialisation, acquisition and/or deployment) at national and EU level, should the research deliver on its goals. The results of the research should be taken up by

EU customs authorities in the framework of the Customs Union "acting as one", with the support of the Customs Control Equipment Instrument (CCEI).

Synergies within civil security can be an asset, for example with Fight Crime and Terrorism.

Destination - Resilient Infrastructure

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024: *"[…] resilience and autonomy of physical and digital infrastructures are enhanced and vital societal functions are ensured, thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for […] infrastructure operators […]"*

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Ensured resilience of large-scale interconnected systems infrastructures in case of complex attacks, pandemics or natural and man-made disasters;
- Upgraded infrastructure protection systems enable rapid, effective, safe and secure response and without substantial human intervention to complex threats and challenges, and better assess risks ensuring resilience and strategic autonomy of European infrastructures;
- Resilient and secure smart cities are protected using the knowledge derived from the protection of critical infrastructures and systems that are characterised by growing complexity.

The following call(s) in this work programme contribute to this destination: [...]

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-INFRA-01	15.04		23 Nov 2023 (First Stage)
HORIZON-CL3-2024-INFRA-01		15.00	
Overall indicative budget	15.04	15.00	

Call - Resilent Infrastructure 2023

HORIZON-CL3-2023-INFRA-01

Conditions for the Call

Indicative budget(s)[42]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[43]	Number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-INFRA-01-01	CSA	15.04 [44]	Around 3.00	1
HORIZON-CL3-2023-INFRA-01-02	IA		Around 6.00	2
Overall indicative budget		15.04		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.

42 The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

43 Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

44 Of which EUR 15.04 million from the 'na' budget.

Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

INFRA01 – Improved preparedness and response for large-scale disruptions of European infrastructures

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-INFRA-01-01: Resilient Plans and next generation tools for Risk Assessments and Incident Notification

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 15.04 million.[46]
Type of Action	Coordination and Support Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Provide common European guidance in order to meet all the provisions of the CER-Directive and support the upgrading of Critical entities in the EU;
- Development of guidelines for critical entities, for the drafting of their resilience plans according to the proposal of CER Directive: risk analysis, domino effects, cross-sector and cross-border analysis, standardised plans, educational and training tools;
- Creation of an all-hazards framework to support Member States in ensuring improved concepts and instruments for the anticipation of risks to critical entities;
- Development of concrete tools to support all-hazard analysis by integrating domain specific risk assessment for critical entities and allowing to manage interdependencies phenomena among different sectors and countries;

[46] This budget is shared with topic HORIZON-CL3-2023-INFRA-01-02

- Improved preparedness and response for disruptions of European critical entities and enhanced resilience of the EU internal market.

Scope: The livelihoods of European citizens and the good functioning of the internal market depend on the reliable provision of services fundamental for societal or economic activities in many different sectors. Critical entities are essential for the functioning of modern societies. With the new Directive on the Resilience of Critical Entities (CER-Directive) the Commission intends to create an all-hazards framework to support Member States. The main goal is to help Member States in ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents, no matter if they are caused by natural hazards, accidents, terrorism, insider threats, or public health emergencies like the one the world faces today.

This Directive reflects the priorities of the Commission's EU Security Union Strategy[47], which calls for a revised approach to critical infrastructure resilience that better reflects the current and anticipated future risk landscape, the increasingly tight interdependencies between different sectors, and also the increasingly interdependent relationships between physical and digital infrastructures. The CER-Directive aims to ensure that competent authorities designated under this directive and those designated under the new NIS 2 Directive[48] take complementary measures and exchange information as necessary regarding cyber and non-cyber resilience, and that particularly critical entities in the sectors considered to be 'essential' per the proposed NIS 2 Directive are also subject to more general resilience-enhancing obligations to address non-cyber risk

In the CER-Directive, it is expected that the critical entities should:

- have a comprehensive understanding of all relevant risks to which they are exposed and analyse those risks. To that aim, they should carry out risks assessments, that should be based on the risk assessment carried out by Member States.
- develop a resilience plan or equivalent document(s), according to outcomes of the risk assessments.

The proposals should focus on the development of improved concepts and instruments for the anticipation of risks to critical entities. A risk assessment analysis method, addressing the relevant natural and man-made risks, including accidents, natural disasters, public health emergencies, hybrid threats or other antagonistic threats, including terrorism is needed. In addition, there is a need for improved methodologies of assessments related to risk, vulnerability, complexity, and resilience of interconnected critical entities. A cross-sector and cross-border analysis of interdependencies both by authorities, but notably also entities should be included as part of this work.

Proposals should also focus on the development of a more effective resilience plan conception method, which shall support critical entities to draft their resilience plans according to the provisions of the CER Directive. The resilience plan conception method should include risk

47 Communication from the Commission on the EU Security Union Strategy. COM (2020) 605
48 Reference to NIS 2 Directive, once adopted.

analysis, domino effects analysis, cross-sector and cross-border analysis, standardised plans etc. In addition, this method should include measures on adequate protection of critical entities, measures on prevention, response, mitigation, and recovery from the consequences of incidents, protection of sensitive information and measures that ensure adequate employee security management.

It is recommended that proposals should develop concrete tools to support all-hazard analysis by integrating domain specific risk assessment and allowing to manage interdependencies phenomena among different sectors and countries. Possible examples are virtual reality tools, dashboards, or other instruments to be used and that currently do not exist on such scale.

HORIZON-CL3-2023-INFRA-01-02: Supporting critical infrastructures against cyber and non-cyber threats to reinforce the EU resilience of critical entities

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 15.04 million.[49]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Support the resilience of EU critical entities against cyber and non-cyber threats in specific sector;
- A reliable state-of-the-art analysis of physical/cyber detection technologies and risk scenarios, in the context of a critical entity in a specific sector;
- Improved cooperation against natural or man-made threats and subsequent disruptions of infrastructures in Europe, allowing for operational testing in real scenarios or realistic simulations of scenarios with specific regard to disruptions in specific sector of critical entities;
- Improvement situational awareness and governance by the implementation of effective solutions that enhance detection and anticipated projection of a determined threating situation, as well as implementation of prevention, preparedness/mitigation, response, and recovery types of intervention;

[49] This budget is shared with topic HORIZON-CL3-2023-INFRA-01-01

- Significant reduction of risks and exposures to anomalies or deliberate events on cyber-physical systems, or on complex and critical infrastructures/systems;

Enhanced preparedness and response by definition of operational procedures of critical entities as well as public authorities considering citizens involvement and societal impact in case of disruption of critical entities in a specific sector.

Scope: The operational environment in which critical entities operate has changed significantly in recent years. Security research and innovation related to infrastructure resilience has been following a sectorial approach in order to increase the resilience of critical entities. The approach to critical infrastructure resilience is needed that better reflects the current and anticipated future risk landscape, the increasingly tight interdependencies between different sectors, and also the increasingly interdependent relationships between physical and digital infrastructures.

A disruption affecting the service provision by one operator in one sector has the potential to generate cascading effects on service provision in other sectors, and also potentially in other Member States or across the entire EU.

With more and more infrastructure systems being interconnected, a stronger focus on the systemic dimension and complexity of attacks and disruptions by cyber or physical means needs to be applied. As such, not only interdependencies within one type of infrastructure (or closely related types) can be taken into account. The risk landscape is more complex in the recent years, involving today natural hazards (in many cases exacerbated by climate change), state-sponsored hybrid actions, terrorism, insider threats, pandemics, and accidents (such as industrial accidents).

The proposals for both the CER-Directive and the NIS2-Directive include an Annex on sectors that should be covered under new EU rules. Some of those sectors or sub-sectors have not yet, or not yet fully, been addressed in projects of the last years. This is true notably for: Public Administration, financial market infrastructure, Road Transport, District Heating and Cooling, Financial Markets and Banking, lines of communication as well as Hydrogen, included in the proposals for CER and NIS-2. Such disruptions in critical entities have possibly serious negative implications for citizens, business, governments, in the environment and endanger the smooth functioning of the internal market.

Another important issue is to have in place efficient cybersecurity measures to block the access to critical infrastructures. A possible project focusing on the protection of critical infrastructures against such threat should be considered as gaps and vulnerabilities need to be identified and overcome (e.g. protection of drinking water supply systems from high chemical levels, nuclear facilities, etc.).

Therefore, the successful proposal, following a sector-based approach and identifying a specific priority sector, should work on how to increase cyber and physical resilience of critical entities. It should also align with the list of sectors described in the Annexes of CER and NIS-2 proposals

and contribute to the implementation of both directives, in line with the EU Security Union Strategy.

The proposal should orient itself on the policy shift from protection towards resilience and thus focus on entities providing essential service in the internal market, rather than on physical or digital assets. The main practitioners in this topic should come from critical entities, as well as competent authorities of MS in charge of resilience of infrastructures.

Call - Resilient Infrastructure 2024

HORIZON-CL3-2024-INFRA-01

Conditions for the Call

Indicative budget(s)[50]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[51]	Number of projects expected to be funded
		2024		
Opening: na				
HORIZON-CL3-2024-INFRA-01-01	IA	15.00	Around 6.00	1
HORIZON-CL3-2024-INFRA-01-02	RIA		Around 5.00	1
HORIZON-CL3-2024-INFRA-01-03	IA		Around 4.00	1
Overall indicative budget		15.00		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.

[50] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

[51] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

INFRA02 – Resilient and secure urban areas and smart cities

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-INFRA-01-01: Resilient and secure urban planning and new tools for EU territorial entities

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 15.00 million.[52]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Evaluation of the resilience of an urban and rural environment, identify weaknesses and recommend changes to organizational 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;

[52] This budget is shared with topic HORIZON-CL3-2024-INFRA-01-02, HORIZON-CL3-2024-INFRA-01-03

- Improvement of the efficiency of the security forces and emergency services (police, firefighters, paramedics ...) for the benefit of the European citizens;

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, in order to coordinate efficient responses of emergency services and to improve interventions and overall security.

Scope: European territories are developing into more connected and complex systems of different services and infrastructures empowered by technologies and growing digitisation. This change in urban areas in Europe, brings new opportunities but also new threats for the authorities and their relationship with the citizens. It is therefore critical for the resilience of our urban areas and for their citizens' wellbeing that those services are trusted and secure.

The classical large-scale infrastructures have a long tradition of implementing the principles of Safety-by-design and Security-by-design when planning their assets. However, with more and more infrastructures on the local level becoming vulnerable, security research can support their protection with new approaches in 'Security-by-design'. In view of limited budgets of many local administrations, improved knowledge as well as innovative security upgrades and processes for existing urban infrastructures equipped with advanced connectivity technologies and cooperative systems could be explored.

EU territories, despite their size and location, suffer from a lack of dedicated EU sovereign and trusted tools in order to enhance the coordination of local first responders and to improve security coverage, such as the preparation of operational staff, field intervention and predictive tools. Even though some complicated tools already exist, it is clear that there is no generic, cost effective and easy to use solutions for local authorities. Therefore, there is a need for creation of new tools that are designed in a simple manner and deployed in an effective way.

Resilient and secure urban planning tools for the development of holistic approaches that network the different organizational levels, sensor and communication levels and data rooms are very pertinent. These tools should assess the resilience of urban and rural territories, identify weaknesses and recommend changes to organizational processes, sensors and communication infrastructure. The secure urban and rural living spaces, technical solutions, organizational levels, and data rooms must be more closely linked. There is a clear need for a development of tools for recovery strategies and proactive foresight for urban and rural environments. The tactical tools should include modelling of urban centers and rural areas (e.g. digital twins), predictive tools (e.g. natural risks, daily delinquency, open-source information), improved global situational awareness and day-to-day planning and crisis management (e.g. decision support, simulation, training).

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 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.

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.

HORIZON-CL3-2024-INFRA-01-02: Advanced real-time data analysis used for infrastructure protection

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 15.00 million.[53]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved capabilities for risk 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, 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;

[53] This budget is shared with topic HORIZON-CL3-2024-INFRA-01-01, HORIZON-CL3-2024-INFRA-01-03

Improved ability to map in real-time the source(s) of risk factors that could endanger the networked infrastructure.

Scope: Today's society is more interconnected than ever before. Telecommunication networks, transport networks, aviation, the energy grid, finance are the backbone of today's society. Due to their exceptional complexity and size, infrastructure networks pose a specific challenge when it comes to identifying different risks, either cyber or physical. Especially in the cyber-domain, many intrusions or attacks remain unnoticed or are detected relatively late. Technological developments in areas like machine learning for analytics, user interfaces as well as storage applications have the potential to improve related capabilities.

Modern urban environments and interconnected infrastructures create constantly big amounts of data. In addition, other sources can be exploited to support the identification and analysis of risks to infrastructures. Therefore, research on enhanced risk anticipation through real-time data analysis has the potential to lead to useful tools to enhance preparedness (contingency plans, scenario-based exercises, allocation of resources, etc.).

Resilience of smart cities is marked by a set of specific requirements taking into account most notably aspects from the integration considering user centre approaches as well as social and ethical aspects of Industrial Internet of Things (IIoT), AI/ Machine Learning approaches for real-time data analytics, ensuring transparency, sufficient knowledge and their operational challenges in this area.

While the availability of larger amounts of data from different sources offers potential to improve the identification of possible risks to infrastructures, it increases also 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 cyber-attacks 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 of hazardous agents and contaminants inside the infrastructure networks is a key to allow for quick response, inform and involve citizens 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.

HORIZON-CL3-2024-INFRA-01-03: Climate proofing of critical entities and impact of climate change on critical infrastructure

Specific conditions

Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 15.00 million.[54]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Development of new concepts for the resilience of critical entities incorporating climate proofing and updating existing integrated risk management plans for cities and urban areas with a view of complementing existing methods for protection and resilience;
- Improved forecast methods, mitigation concepts and methods and new modelling techniques;
- Development of new tools and solutions in real environment, in order to increase the resilience of critical infrastructures, validate multi-hazard scenarios, create interactive hazard maps;
- Enhancement of the capacity of critical entities to be more resilient on potential damages with testing of different scenarios on how climate change will influence different types of hazards, including storms, wildfires, floods, landslides and heatwaves in the operation of pre-existing and planed critical infrastructures.

Scope: Urban environments are facing several challenges in green and economic growth enabling and supporting a high quality of life in resilient of EU territories. Proposed measures to support resilient infrastructure against climate change and adaptation measures for climate proofing are necessary.

The aim of the topic is to increase climate-proofing infrastructure that integrate climate change mitigation and adaptation measures into the development of infrastructures and also to help mainstream climate considerations and develop resilient critical entities in respect to Paris Agreement and EU climate objectives.

The impacts of climate change are already having repercussions for critical assets and infrastructure with long lifetimes such as railways, bridges or power stations, and these impacts are set to intensify in the future. In areas affected by sea level rise, the development of critical entities requires particular attention. Similarly, heat tolerance for railway tracks and needs to account for the projected higher maximum temperature rather than historical values. Wildfires could affect water availability but also to cause significant disruptions on the operation of

[54] This budget is shared with topic HORIZON-CL3-2024-INFRA-01-01, HORIZON-CL3-2024-INFRA-01-02

critical infrastructures. Landslides are particularly important in mountainous countries causing billions of euros in damages each year. Natural and man-made disasters can adversely affect infrastructure such as high- and railway lines, reservoir dams, pressure pipes, pipelines, and settlements due to differential and localised displacements of the ground surface and subsurface. For all the above cases, the damages can be considerable, and the lifecycle of man-made structures can be reduced, accompanied with a great economic loss. It is therefore essential to clearly identify – and consequently invest in – critical entities that are prepared for a climate-neutral and climate-resilient future.

Proposals should focus on stress tests of critical infrastructure, improved forecast methods, mitigation concepts and methods and new modelling techniques, in the light of climate proofing of critical infrastructure such as highways, railway lines, bridges, power lines, pipelines for gas and oil, reservoir dams for water supply and power generation.

The testing and/or piloting of the tools and solutions developed in a real setting with one or more relevant 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.

Increased Cybersecurity

Proposals for topics under this Destination should set out a credible pathway contributing to the following impact of the Strategic Plan 2021-2024: "Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats".

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies
- More resilient digital infrastructures, systems and processes
- Increased software, hardware and supply chain security
- Secured disruptive technologies
- Smart and quantifiable security assurance and certification shared across the EU
- Reinforced awareness and a common cyber security management and culture.

The following call(s) in this work programme contribute to this destination: [...]

Call	Budgets (EUR million)	Deadline(s)
	2023	
HORIZON-CL3-2023-CS-01	70.25	23 Nov 2023
HORIZON-CL3-2024-CS-01		
Overall indicative budget	70.25	

Call - Increased Cybersecurity 2023

HORIZON-CL3-2023-CS-01

Conditions for the Call

Indicative budget(s)[55]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[56]	Number of projects expected to be funded
		2023		
Opening: na Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-CS-01-01	IA	70.25 [57]	2.00 to 4.00	Not relevant
HORIZON-CL3-2023-CS-01-02	RIA		2.00 to 4.00	Not relevant
HORIZON-CL3-2023-CS-01-03	RIA		2.00 to 4.00	Not relevant
Overall indicative budget		70.25		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.

55 The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

56 Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

57 Of which EUR 70.25 million from the 'na' budget.

Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

CS01 - Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-CS-01-01: Secure distributed platforms (IoT, Edge, Cloud, Dataspaces)

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 2.00 and 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 70.25 million.[60]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Tools to support cybersecurity resilience, preparedness, and awareness within critical infrastructures and across supply chains, including.
- Cloud infrastructures vulnerabilities mitigation.
- Secure integration of untrusted IoT in trusted environments.
- Trust & Security for massive connected IoT ecosystems & lifecycle management.
- Secure interoperability of systems.
- Secure infrastructure and secure Identities for a security chain that secure communication, data collection, data transport, and data processing.

[60] This budget is shared with topic HORIZON-CL3-2023-CS-01-02, HORIZON-CL3-2023-CS-01-03

Scope: The evolution of our interconnected society brings multiple layers of cloud, edge computing, and IoT platforms that continuously interact with each other. Yet this always-connected ecosystem populated with potentially vulnerable entities requires advanced, smart and agile protection mechanisms that to manage the security and privacy of individual components through their lifecycle and of overall systems. The complexity of such interconnected environments underlines the need for the proactive and automated detection, analysis, and mitigation of cybersecurity attacks in cloud, edge computing and IoT deployment. Integrating end-to-end security and user-centric privacy in complex distributed platforms requires research to address security threats and vulnerabilities over the entire platform ecosystem.

CS02 –Privacy-preserving and identity technologies

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-CS-01-02: Privacy-preserving and identity technologies

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 2.00 and 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 70.25 million.[61]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved scalable and reliable privacy-preserving and identity technologies for federated processing of personal and industrial data and their integration in real-world systems.
- Improving privacy-preserving technologies for cyber threat intelligence and data sharing solutions.
- Contribution to promotion of GDPR compliant European data spaces for digital services and research (in synergy with DATA Topics of Horizon Europe Cluster 4). Also, contribution to the promotion of eID Regulation compliant European solutions.
- Research and development of self-sovereign identify technologies and solutions.
- Strengthened European ecosystem of open source developers and researchers of privacy-preserving solutions.

[61] This budget is shared with topic HORIZON-CL3-2023-CS-01-01, HORIZON-CL3-2023-CS-01-03

Scope: Using big data for digital services and scientific research brings about new opportunities and challenges. For example, machine- learning methods process medical and behavioural data for finding causes and explanations for diseases or health risks. However, a large amount of this data is personal data. Leakage or abuse of this kind of data, potential privacy risks (e.g. attribute disclosure or membership inference) and identity compromises pose threats to individuals, society and economy, which hamper further developing data spaces involving personal data. Likewise, there are similar challenges for the exploitation of non-personal/ industrial data assets that may compromise the opportunities offered by the data economy. Advanced privacy-preserving technologies such as homomorphic encryption, secure multiparty computation, and differential privacy have the potential to address these challenges. However, further research is required to ensure and test their applicability in real-world use case scenarios.

The security of any digital service or the access to data is based on secure digital identities. The eID Regulation provides the legal framework on which to build technological solutions that address the user needs concerning their digital identity. With regards to personal data, it is also important to develop self-sovereign identity solutions that give users complete control on their personal data and use.

Consortia should bring together interdisciplinary expertise and capacity covering the supply and the demand side, i.e. industry, service providers and end-users. Participation of SMEs is strongly encouraged. Legal expertise should also be added to assess and ensure compliance of the technical project results with data regulations and the GDPR.

CS03 - Secured disruptive technologies

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-CS-01-03: Security of robust AI systems

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 2.00 and 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 70.25 million.[62]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Security-by-design concept and resilience to adversarial attacks

[62] This budget is shared with topic HORIZON-CL3-2023-CS-01-01, HORIZON-CL3-2023-CS-01-02

- Inclusion of context awareness in machine learning in order to boost resiliency.

Scope: Artificial Intelligence (in particular Deep Learning and Machine Learning), together with advances in computing capacity, enable users to process very large amounts of data. As such, AI techniques have been successfully applied to tackle many cybersecurity problems via advanced methods for threat detection, prediction, and response. For example, AI mechanisms have the ability to combat the spread of digital fake assets, which are abused for misinformation and miseducation within our societies. The use of robust AI as a technology for building system monitoring techniques and anomaly detection should be developed further. At the same time, concerns have been raised over the security and stability of the AI algorithms used in cybersecurity applications. Thus, it is important to ensure that only certified, fair, and security-compliant AI algorithms are used to enhance cybersecurity.

Call - Increased Cybersecurity 2024

HORIZON-CL3-2024-CS-01

Conditions for the Call

Indicative budget(s)[63]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[64]	Number of projects expected to be funded
Opening: na				
HORIZON-CL3-2024-CS-01-01	IA		2.00 to 4.00	Not relevant
HORIZON-CL3-2024-CS-01-02	RIA		2.00 to 4.00	Not relevant
Overall indicative budget				

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.

63 The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

64 Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

CS01 - Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-CS-01-01: Approaches and tools for security in software and hardware development and assessment

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 2.00 and 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 0.00 million.[65]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved hardware and software security engineering; resilient systems design.
- Systematic study of vulnerabilities; software analysis, vulnerability discovery and dynamic security assessment.

[65] This budget is shared with topic HORIZON-CL3-2024-CS-01-02

- Trustworthy certifiable hardware and software.
- AI-based security services e.g. predictive security, advanced anomaly and intrusion detection, system health checks.
- Robust AI-based fake detection e.g. audio, video, images and speech.

Scope: 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 Europe, 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 evolves, which was by factored in compliance approaches.

The use of AI as a technology for building system monitoring techniques and anomaly detection should be developed further. At the same time, concerns have been raised over the security and stability of AI algorithms used in cybersecurity applications. Thus, it is important to ensure that only certified, fair, and security-compliant AI algorithms are used to enhance cybersecurity.

CS02 - Cryptography

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-CS-01-02: Post-quantum cryptography transition

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 2.00 and 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 0.00 million.[66]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

[66] This budget is shared with topic HORIZON-CL3-2024-CS-01-01

- Easy-to-use implementation tools for the large-scale implementation of post-quantum cryptographic algorithms, based on state of the art standards.
- Increasing the maturity of current post-quantum cryptographic algorithms and contribution to further standardisation.
- Secure and efficient transition from pre- to post-quantum encryption through tools implementing a hybrid approach combining recognised pre-quantum public key algorithms and additional post-quantum algorithms.

Scope: 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 is a few decades away. There is a need to advance in the transition to quantum-resistant cryptography.

Destination - Disaster-Resilient Society for Europe

Proposals involving earth observation are encouraged to primarily make use of Copernicus data, services and technologies.

Proposal are encouraged also to coordinate with ESA relevant activities, especially those undertaken under the Science for Society element of the FutureEO programme (https://eo4society.esa.int).Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024:

"Losses from natural, accidental and man-made disasters are reduced through enhanced disaster risk reduction based on preventive actions, better societal preparedness and resilience and improved disaster risk management in a systemic way."

More specifically, proposals should contribute to the achievement of one or more of the following impacts

- Enhanced collaboration, interactions and cross-discipline dialogue and networking between the scientific community, research institutions and programmes (e.g., H2020, ESA scientific activities, national science programmes, FutureEarth RIS-KAN) and first and second responders through dedicated networking and collaboration actions fostering a fasters transfer of results from science into practice.

- Enhanced exploitation of the latest scientific results (e.g., from research programmes and institutions) and integrated technologies (e.g. Earth observation, in situ data collection, advanced modelling, AI) into enhanced understanding of high-impact hazards and complex compound and cascade events and improved prevention, preparedness to mitigation, response, and recovery tools.

- Enhanced understanding and improved knowledge and situational awareness of disaster-related risks by citizens, empowered to act and consider innovative solutions, thus raising the resilience of European society;

- More efficient cross-sectoral, cross-disciplines (including SSH), cross-border coordination of the disaster risk management cycle and governance (from scientific research to prevention, preparedness to mitigation, response, and recovery, including knowledge transfer and awareness of innovative solutions) from international to local levels.

- Support of harmonised and/or standardised and interoperability of guidelines / protocols / tools / technologies in the area of crisis management and CBRN-E.

- Strengthened capacities of first responders in all operational phases related to any kind of (natural and man-made) disasters so that they can better prepare their operations, have access to enhanced situational awareness, have means to respond to events in a faster,

safer and more efficient way, and may more effectively proceed with victim identification, triage and care;

- Improved impact forecasting capability and scenario building for enhanced stress testing of critical entities and adaption of protection and resilience-enhancing activity accordingly;

- Improved ability to rescue and manage the first phases of emergencies that take into account extreme climatic events and/or geological hazards that may threaten urban areas (e.g. interface fires, floods, volcanic eruption etc.).

The following call(s) in this work programme contribute to this destination: [...]

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-DRS-01	28.82		23 Nov 2023
HORIZON-CL3-2024-DRS-01		29.00	
Overall indicative budget	28.82	29.00	

Call - Disaster-Resilient Society 2023

HORIZON-CL3-2023-DRS-01

Conditions for the Call

Indicative budget(s)[67]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[68]	Number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-DRS-01-01	RIA	28.82	Around 3.00	1
HORIZON-CL3-2023-DRS-01-02	IA		Around 3.00	1
HORIZON-CL3-2023-DRS-01-03	RIA		Around 3.00	1
HORIZON-CL3-2023-DRS-01-04	IA		Around 4.00	1
HORIZON-CL3-2023-DRS-01-05	IA		Around 3.00	1
HORIZON-CL3-2023-DRS-01-06	IA		Around 4.00	1
HORIZON-CL3-2023-DRS-01-07	RIA		Around 3.00	1
HORIZON-CL3-2023-DRS-01-08	IA		Around 6.00	1
Overall indicative budget		28.82		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.

[67] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

[68] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

DRS01 - Societal Resilience: Increased risk Awareness and preparedness of citizens

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-DRS-01-01: Innovative concepts to enhance cooperation and use of available knowledge across disaster and crisis management-related disciplines and administrative levels

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[69]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to the following outcomes:

- Analysis of the influence of operational and organisational structures in disaster risk reduction on knowledge sharing, both across different thematic disciplines and administrative levels.

[69] This budget is shared with topic HORIZON-CL3-2023-DRS-01-02, HORIZON-CL3-2023-DRS-01-03, HORIZON-CL3-2023-DRS-01-04, HORIZON-CL3-2023-DRS-01-05, HORIZON-CL3-2023-DRS-01-06, HORIZON-CL3-2023-DRS-01-07, HORIZON-CL3-2023-DRS-01-08

- Development of concrete knowledge-sharing and knowledge management tools and platforms to enhance the situational awareness and foster cooperation across relevant thematic disciplines usable on different administrative levels (local, regional, national as well as European and international), taking into account the specificities of classified information.

- Development and scale-up of innovative solutions to overcome language, cultural and organisational barriers (e. g. in cross-border cooperation) like collaborative platforms for knowledge exchange including a neutral machine translation engine, which uses machine learning to improve and fine-tune its output. This would help the exchange as authorities could easily translate documents using DRR jargon on the platform

- Concepts to mainstream disaster prevention work and knowledge available in prevention into preparedness and response.

Scope: Innovative solutions are required to use relevant knowledge available across risk reduction-related disciplines and administrative levels for enhancing cooperation in the case of (natural or man-made) disaster and crisis events, taking into account multiple language aspects. This goes along with needs related to the fostering of cross-sectoral cooperation at different levels (from international to local) between different security-related actors in preparedness and response, prevention, and recovery efforts. Possible actions include cross-sectoral / disciplines networking, information exchanges among existing networks, synergy building among different types of research and innovation, capacity-building, education and training programmes, standardization, deployment of innovative disaster risk financing instruments including risk transfer mechanisms and disaster risk insurance.

The importance of prevention as a field of action in security overall and for disaster-resilient societies is still not well enough understood. This is largely because actors in prevention (e.g. administrative departments and offices such as environment, agriculture, marine, health, consumer protection, economy, energy etc.) are often different from actors in preparedness and response (e.g. civil protection units, fire services, law enforcement agencies, emergency health services etc.) as well as in recovery. Organisational or public management research could be undertaken to find innovative solutions for better cooperating and using relevant knowledge available across disciplines and administrative levels. The specificities of working with classified information that cannot be shared easily should also be considered in this context.

[**References to be added on international cooperation, involvement of SSH, societal engagement and/or social innovation**].

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-DRS-01-02: Improving social and societal preparedness for disaster response and health emergencies

Specific conditions

Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[70]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to the following outcomes:

- Maintaining basic services through improved local cooperation in preparedness and prevention, transformation of workplaces, e.g., regarding protective gear, digital transformation, and home office, and specific measures to better address first responders' (e.g., health care workers) retention and ability to work during long-term crisis situations
- Identification of different factors in inequality and ways to communicate with vulnerable groups, of individual, organisational, and systemic resilience factors and pathways to support these, and of ways to address vulnerabilities in acute crisis as well as during prevention, in order to elaborate an interconnectedness of resilience and vulnerability
- Improved crisis communication through increased awareness and risk perception regarding bio security, identification of challenges for and limits of communication strategies and interventions regarding different vulnerable groups and approaches to address these, elaborating of ways for resolving barriers for crisis communication: interlinguality, interculturality, intersemiotics
- Putting the citizen at the centre of the crisis management process, analysing behaviours regarding unpopular measures (e.g., quarantine) and vaccination attitudes and identification and relieving of barriers for vaccination readiness: Trust, risk appraisal, barriers for registration for vaccination, information, collective responsibility
- Incorporation of information technology and data processing into crisis management through improved information processing in transformative governance, illustrating possibilities, challenges, and limits of digitalisation and enabling usage of data for political decision making.
- Incorporation of machine learning and artificial intelligence in governance and political decision making based on interdisciplinary discussions on definitions on problems; areas of application; and definition of responsibilities and competences in data governance
- Strengthening of the One Health approach including not only human physical health but also environmental and animal health, and understanding of the biological risks posed by

[70] This budget is shared with topic HORIZON-CL3-2023-DRS-01-01, HORIZON-CL3-2023-DRS-01-03, HORIZON-CL3-2023-DRS-01-04, HORIZON-CL3-2023-DRS-01-05, HORIZON-CL3-2023-DRS-01-06, HORIZON-CL3-2023-DRS-01-07, HORIZON-CL3-2023-DRS-01-08

environmental changes such as climate change and preparedness for impacts on human health.

Scope: The COVID-19 pandemic illustrated the specific challenges of health emergencies and the necessity to be prepared not only on a material and physical level but also from a social and societal perspective. Challenges during the pandemic included missing bsl3 laboratories and research on pathogens due to low acceptance and support; difficulties of working with protective gear such as insecurities and usage mistakes; additional disadvantages for vulnerable groups among others due to communication issues; and lack of local cooperation and prevention regarding equipment, stocks, and coordination. These challenges were largely due to deficiencies in the inclusion of social sciences in disaster research. The COVID-19 pandemic poses an opportunity to analyse successes and difficulties during a global health crisis and thereby preparing for future health crises.

Currently, different groups are not reached equally by public communication efforts. Risk communication especially fails to contact vulnerable groups. Social inequalities are present in different forms and on different levels. For communication strategies and interventions, it should be considered how they are affected by different groups, localities, and cultural factors. In different crises, different vulnerability factors can be more pronounced and different groups can be more vulnerable. On the other hand, resilience can protect against negative effects of crises. Resilience can be supported on an individual, organisational, or systemic level. All should be considered in preparation for crisis as well as in acute situations.

Information technology and digital data processing are becoming increasingly important in public health. Processing large datasets and automated analyses can open new possibilities in understanding health and illness on a population level and for deriving prevention strategies. However, the implementation of information technology poses several challenges and research on how to effectively use the results in political decision-making. Data security is another challenge when large amounts of personalized (health) data are processed automatically. Concerns about data security and general scepticism about digital information processing in the population need to be taken seriously and addressed.

Health encompasses several aspects and levels. Human health incorporates both physical and psychological health which are interconnected and mutually dependent. At the same time, humans are embedded in their environment so human and environmental health cannot be approached in isolation from each other. According to the One Health approach, health of humans, animals, and environment are intertwined. This is illustrated by the current health crisis of COVID-19 which is attributed to SARS-CoV-2 jumping over from wild animals to humans. Another illustration of the interconnectedness are health impacts of climate change. These interdependencies make an interdisciplinary approach to health necessary that incorporates all aspects of health and their interconnectedness.

[**References to be added on international cooperation, involvement of SSH and societal engagement and/or social innovation**].

DRS02 - Improved Disaster Risk Management and Governance

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-DRS-01-03: Design of crisis prevention and preparedness actions in case of digital breakdown (internet, electricity etc.)

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[71]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Development of prevention/preparedness actions based on the (existing) analysis of interdependencies between critical infrastructures and possible cascading effects;
- Analysis of existing communication systems and assessment/development of alternative communication tools for Civil Protection and Crisis Management security authorities, including the communication with private sector and actors responsible for critical infrastructures.

Scope: The modern societies are highly dependent on the (unlimited) availability of electricity and digital infrastructures. A digital breakdown with loss of electricity and IT infrastructures would have severe impacts on various infrastructures and areas critical for the functioning of societies. Assessment of the consequences of possible digital breakdown (internet, electricity etc.) would require focused research in order to design appropriate crisis prevention and preparedness actions taking into account cascading effects. This includes analysis of interdependencies between different critical infrastructures, the assessment of different scenarios and conditions like duration and extent of the digital breakdown as well as possible cascading effects.

Assess also the advantage of using satellite broadcast in case of unavailable terrestrial systems (disseminate instructions and guidance to populations, to rescue teams, to authorities, etc.)

[71] This budget is shared with topic HORIZON-CL3-2023-DRS-01-01, HORIZON-CL3-2023-DRS-01-02, HORIZON-CL3-2023-DRS-01-04, HORIZON-CL3-2023-DRS-01-05, HORIZON-CL3-2023-DRS-01-06, HORIZON-CL3-2023-DRS-01-07, HORIZON-CL3-2023-DRS-01-08

[**References to be added on international cooperation, involvement of SSH and societal engagement and/or social innovation – Cross-reference to INFRA**].

HORIZON-CL3-2023-DRS-01-04: Augmented reality solutions for improved situational awareness for public safety in case of cross-border emergency situations

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[72]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Innovative Artificial Intelligence tools to process large amounts of data (both operational and open sources) in real-time or near real-time patterns in audio or video streams, identifying abnormal or suspicious situations, people or behaviours, measuring and mitigating the lack of real data in sufficient volume and quality for the implementation of large-scale pilot projects to test the effectiveness of prototypes.
- Systems to identify relevant information (for missions) in open source analysis, with specific attention to fake news and correlation with field information filtered by Mission Critical Services platforms.
- Improved reporting tools to reduce repetitive and procedural activities.
- Location means for (first and second) responders, vis-à-vis their proximity to threats and hazards in real time.

Enhanced communication and cooperation between citizens, experts and practitioners.

Scope: Public Safety end users are faced with large amounts of multimedia contents regarding any kind of events. These data can be aggregated and analysed to build and provide a rich common operational picture and enhanced situational awareness services to first and second responders. Nonetheless, the huge amounts of date produced, on the one hand, from the management control itself and, on the other hand, from multiple sources of data, cannot be processed by human beings, thus limiting the potential benefits for Public Safety users. Innovative solutions are therefore needed to use information from different sources for

[72] This budget is shared with topic HORIZON-CL3-2023-DRS-01-01, HORIZON-CL3-2023-DRS-01-02, HORIZON-CL3-2023-DRS-01-03, HORIZON-CL3-2023-DRS-01-05, HORIZON-CL3-2023-DRS-01-06, HORIZON-CL3-2023-DRS-01-07, HORIZON-CL3-2023-DRS-01-08

command operations, exploiting Artificial Intelligence to analyse various digital streams (real time audio / video or data) related to an incident or a mission in order to support Public Safety end users while respecting legal frameworks and responsibilities. As such, they can provide actionable intelligence that exploits different data sources and enhance their situational awareness while facilitating their mission management (e.g. mission workflow, reporting, inter-agencies and cross-border cooperation).

[**References to be added on involvement of SSH and societal engagement and/or social innovation**].

DRS03 - Improved harmonisation and/or standardisation in the area of crisis management and CBRN-E

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-DRS-01-05: Operability and standardisation in response to biological toxin incidents

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[73]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved European crisis management in case of an incident with biological toxins through the development of a pan-European network of security practitioners
- New and existing portable devices, technologies and methods for responders to perform on-site detection of biological toxins are brought to the market
- Recommendations of effective decontamination measures for personnel, equipment and facilities exposed to biological toxins are provided based on solid experimental testing
- Development of an operational European response network of specialised and forensic laboratories and harmonised procedures/guidelines for forensic analysis of biological toxins applicable to a range of relevant technologies and toxins

[73] This budget is shared with topic HORIZON-CL3-2023-DRS-01-01, HORIZON-CL3-2023-DRS-01-02, HORIZON-CL3-2023-DRS-01-03, HORIZON-CL3-2023-DRS-01-04, HORIZON-CL3-2023-DRS-01-06, HORIZON-CL3-2023-DRS-01-07, HORIZON-CL3-2023-DRS-01-08

- The risks for responders from exposure to biological toxins in the hot-zone are assessed and recommendations of protective equipment for working with biological toxins in the hot-zone are developed

- Building on existing initiatives and networks, a consolidated platform is established providing support for standardisation efforts in the analysis of biological toxins.

Scope: Recent incidents in Europe and worldwide have highlighted the current threat posed by several biological toxins falling under the Chemical and Biological Weapons Convention. The incidents demonstrated the urgency for countries individually and collectively to improve crisis management capabilities, to advance standardisation efforts and to interconnect security practitioners such as first responders, law enforcement agencies as well as specialised and forensic laboratories across Europe. In order to ensure cross border interoperability, existing and new national procedures need to be developed and implemented in an operational and coherent European crisis response network capable of addressing the threats posed by biological toxins.

To properly manage and minimise the effects of an attack with biological toxins, fast and reliable detection and identification of the used agent is critical. Portable devices, technologies and methods for responders to perform on-site detection of a panel of biological toxins remain to be developed. There is a need for evaluation, training and advancement of on-site detection methods for responders, as well as the integration of emerging detection technologies into marketable solutions.

The safety of responders relies on correct risk assessment and the use of appropriate protective equipment. The risks from exposure to biological toxins in the hot-zone are largely unknown. In order to recommend appropriate protective equipment for first responders and to guide the use of effective decontamination measures, the risks from exposure need to be assessed.

Following an attack, exposed personnel, equipment and facilities needs to be decontaminated and declared safe as quickly as possible, in order limit the effects on society. Most decontamination procedures are developed for chemical or biological (i.e. organisms and viruses) agents, but based on their characteristics, biological toxins are at the interface of classical biological and chemical agents. Therefore, the efficiency of existing decontamination procedures should be evaluated for the decontamination of biological toxins.

Previous initiatives have initiated standardisation efforts for lab-based detection and identification of biological toxins. Analytical tools and reference materials are available and comprehensive training and proficiency-testing programs were organised, however, the need for further technical and operational improvement was demonstrated. Building on existing initiatives and networks, a consolidated platform should be established providing analytical tools, training and intercomparisons among laboratories. Following the initial detection of the used biological toxin, a more detailed analysis is needed in order to link the agent to confiscated materials. In support of criminal investigations, new procedures and guidelines for comprehensive forensic analysis of biological toxins are needed. The developed methods and procedures should be shared among specialised and forensic laboratories.

[**References on involvement of SSH and societal engagement and/or social innovation – Cross-reference to FCT**].

HORIZON-CL3-2023-DRS-01-06: Strengthened networking of training centres for the validation and testing of CBRN-E tools and technologies

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[74]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Better coordinated and validated test and training capacity in Europe. Compilation of Training and testing centres including POCs in Europe
- Improved cooperation and method development. Round robin tests for comparisons and development of testing methodologies and protocols
- Inter-cooperation and synchronizing in filling in gaps in test and validation techniques.

Scope: In case of a CBRN-E incident, it is of outmost importance that personnel involved in handling the situation, i.e., rescue services and polices, are well educated and trained and that they are using equipment and tools that are reliable with validated capabilities. It can be the difference between a well-functioning management and a disaster. To achieve a more robust and consistent opportunity to practice, test and evaluate CBRN-E tools and technologies within Europe, it is necessary to create a network of facilities and centres. A screening of the existing training and test centres in Europe can identify gaps where training and testing opportunities are lacking but can also be a possibility to highlight weaknesses in that there may be dependencies on one or a few actors. This will indicate what type of facilities are necessary to develop to strengthen the testing end exercise capabilities in Europe to be better prepared in the event of a CBRN-E incident. It will also give the existing centres a possibility to network and cooperate to compare, enhance, develop and extend the palette of tests, exercises and training to achieve a robustness that will benefit the whole European CBRN-E community.

The goal is to create a more robust and consistent opportunity to develop, practice, test and evaluate CBRN-E tools and technologies in Europe. A screening of training and test centres in

[74] This budget is shared with topic HORIZON-CL3-2023-DRS-01-01, HORIZON-CL3-2023-DRS-01-02, HORIZON-CL3-2023-DRS-01-03, HORIZON-CL3-2023-DRS-01-04, HORIZON-CL3-2023-DRS-01-05, HORIZON-CL3-2023-DRS-01-07, HORIZON-CL3-2023-DRS-01-08

Europe create a possibility to identify gaps where training and testing opportunities are lacking, but also a possibility to identify weaknesses in that there may be dependencies on one or a few actors.

It will also give the existing centres a possibility to network and cooperate to compare, enhance, develop and extend the palette of tests, exercises and training to achieve a robustness that will benefit the whole European CBRN-E community.

The work would build on the results achieved from the eNOTICE project (https://cordis.europa.eu/project/id/740521) but focus on further development of tools, tests and training methods.

DRS04 - Strengthened capacities of first and second responders

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-DRS-01-07: Hi-tech capacities for cross-border crisis response and recovery after a natural-technological (NaTech) disaster

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[75]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Development of a holistic vision of crisis management after telluric (e.g. volcanic, seismic, tsunami) or extreme climate events (e.g. floods, storms, storm surges, fires, droughts) producing impacts on critical assets (e.g. infrastructures, industries) and creation of new management framework for handling NaTech crises.

- Enhanced existing crisis management tools to develop a common platform (shared among public and private operators) allowing cross-border exchanges and decision-making, while respecting legal frameworks and responsibilities.

- Demonstrated operational protocols and development of standard operating procedures able to respond to NaTech crises in cross-border configurations, including comprehensive

[75] This budget is shared with topic HORIZON-CL3-2023-DRS-01-01, HORIZON-CL3-2023-DRS-01-02, HORIZON-CL3-2023-DRS-01-03, HORIZON-CL3-2023-DRS-01-04, HORIZON-CL3-2023-DRS-01-05, HORIZON-CL3-2023-DRS-01-06, HORIZON-CL3-2023-DRS-01-08

risk modelling of worst-case scenarios taking into account cascading effects and future impacts of climate change, and taking into consideration spatial information and data.

- Improvement of our understanding and capabilities to identify and mitigate risks associated with interdependencies across infrastructures and other human (social and economic) systems.

Scope: The confluence of incidents in recent years has brought renewed concerns over our systemic resilience to external shocks arising from natural-technological (NaTech) disasters. This is particularly acute in the event of disruption in the transport, power, water supply and communication sectors in highly populated and industrialised areas, or when such events raise the likelihood of cascading effects with severe impacts on communities and the economy that are hard or impossible to predict. 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, 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 oversea 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 is part of a coordination initiative between ESA and the EC on Earth System Science. Under the EC-ESA Earth System Science Initiative both institutions aim at coordinating efforts to support complementary collaborative projects, funded on the EC side through Horizon Europe and on the ESA side through the ESA FutureEO programme. Proposals should include a work package, means and resources for coordination with complementary projects funded under the ESA FutureEO initiative.

[**References to be added on the Convention on the Transboundary Effects of Industrial Accidents (TEIA) / Implementation of natural hazard-triggered technological accident principles, and to the Sendai Framework for Action + Involvement of SSH and societal engagement and/or social innovation – Cross-reference to INFRA**].

HORIZON-CL3-2023-DRS-01-08: Robotics: Autonomous systems to supplement skills for use in hazardous environments

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 6.00 million would allow these outcomes to be addressed appropriately.

	Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.82 million.[76]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Broad acceptance of autonomous systems by first responders and affected people in civil protection.
- Higher safety and security standards for operational forces working in hazardous environments.
- Get ahead of future shortcomings of trained first responder personnel by increasing first responder efficiency (less personnel do more work in shorter time).
- Increased ability to conduct on-scene operations remotely without endangering first responders.
- Hyperspectral sensing can provide new data for robots as it is capable of identifying remotely, in real-time and at long distances, different materials or harmful substances.
- Advanced gas sensing methods based on laser spectroscopy can also provide information about volatile hazardous substances.
- European robotics industry is strengthened through engagement in the civil protection research as well as an economic and political advantage through building up know-how for innovative technologies.

Scope: Robotics and automation are key technologies that help increase productivity and efficiency to prevent, prepare, and/or respond to natural and man-made disasters. Demographic change and lifestyle changes, such as shifting several time centre of one's life, build up lots of pressure, especially on volunteer-based first responder organizations, which need long training to be mission ready. First responders supported by robotics will be able to fulfil more work within a shorter amount of time and with less personnel. In this industry, cheaper, more capable, and more flexible technologies are accelerating the growth of fully automated production facilities. It is necessary to bring this innovation also into saving lives. Fundamental changes (procedures, tactics and strategies) in the civil protection traditional way of working is needed. Robotic systems with and without autonomous functionalities are not entirely new in disaster relief. But still, there is no continuous and decisive step towards bringing this innovation into

[76] This budget is shared with topic HORIZON-CL3-2023-DRS-01-01, HORIZON-CL3-2023-DRS-01-02, HORIZON-CL3-2023-DRS-01-03, HORIZON-CL3-2023-DRS-01-04, HORIZON-CL3-2023-DRS-01-05, HORIZON-CL3-2023-DRS-01-06, HORIZON-CL3-2023-DRS-01-07

the first responders' daily work. In order to be successful in this process, various aspects must be considered.

Firstly, there is a need to identify the fields and domains that will benefit from (autonomous) robotic systems. For a start, there is an urgent need to look into the deployments in hazardous environments or where the danger for first responders and citizens is the highest. What kind of technologies can be replaced with robotic solutions to complete the task more efficiently? What are the situations which cause the most significant danger to human life during a disaster situation? Also, it is essential to look into options where robotic systems might be more effective than humans. Extensive technology inventory is needed. Altogether this first step can be considered as the exhaustive requirements and gaps analyses which is an inevitable step bringing robotics closer to the civil protection.

Secondly, the identified gaps and needs should be the basis for proof-of-concept research and development studies. Proof of concept studies can either focus on autonomous systems based on artificial intelligence algorithms or semi- automatic systems. The latter enables managers and practitioners to immerse themselves in what is happening on- site from a great distance and make decisions or even actively intervene in what is happening. To this end, new sensing capabilities should be developed to enhance robotic capabilities and provide more information about the hazards in the environment they operate. They should be adapted in a compact system to be mounted on robots. Human-machine interaction technologies that enable an overlapping control of the robotic systems between the artificial Intelligence entity and the operator need to be developed. The interaction between the user and the robotic system has to be intuitive and should work without extended training.

Thirdly, first responders' training, preparedness, and mindset must be considered when bringing new technologies into the field. This is necessary in order to reach a required paradigm shift. This is a long-term process and therefore has to be strategical and well planned.

Fourthly, the relevant infrastructure needs to be put in place. Robotic systems must be seen as an integral part of first responder ecosystems and not as a single technology. Further research is needed to define the basic physical and organisational structures and facilities required for the operation of robotic solutions and integration to the current operational infrastructure. Therefore, adapted standard operational procedures have to be developed.

Overarching topics like ethics, legal and societal implications are highly relevant in the robotics context. They form the basis for the societal acceptance of artificial intelligence in control and decision-making. As robotics become a new resource for the application in hazardous environments (but not only), their acceptance has to be ensured from the perspectives of emergency services, just as the people to be rescued.

In summary, the scope of this topic is not only to develop new robotic solutions for specific tasks but address it more holistically considering also the surrounding environment and factors that impact civil protection on a larger scale (urbanisation, ageing, climate change, increased complexity in the area of critical infrastructure protection etc.). There are many research and engineering challenges that need to be addressed in the framework of this topic. First responders

play a vital role in ensuring that the robotics solutions are based on the needs and are valuable assets for the civil protection ecosystem. Therefore at least five first or second responder organisations have to be involved in the research consortia.

[**Reference to be added to legacy of past EU-Research, involvement of SSH and societal engagement and/or social innovation**].

Call - Disaster-Resilient Society 2024

HORIZON-CL3-2024-DRS-01

Conditions for the Call

Indicative budget(s)[77]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[78]	Number of projects expected to be funded
		2024		
Opening: na				
HORIZON-CL3-2024-DRS-01-01	IA	29.00	Around 3.00	2
HORIZON-CL3-2024-DRS-01-02	IA		Around 3.00	2
HORIZON-CL3-2024-DRS-01-03	CSA		Around 2.00	1
HORIZON-CL3-2024-DRS-01-04	IA		Around 4.00	2
HORIZON-CL3-2024-DRS-01-05	IA		Around 3.00	1
HORIZON-CL3-2024-DRS-01-06	IA		Around 4.00	1
Overall indicative budget		29.00		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.

[77] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

[78] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

DRS01 - Societal Resilience: Increased risk Awareness and preparedness of citizens

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-DRS-01-01: Better integration of citizen volunteers in field validation of risk management approaches

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[79]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to the following outcomes:

- Better integration of spontaneous volunteers in public hazard management systems, and enhanced training of first responders and volunteers in operational tasks of disaster response and via digital training platforms (including virtual and augmented reality formats)

[79] This budget is shared with topic HORIZON-CL3-2024-DRS-01-02, HORIZON-CL3-2024-DRS-01-03, HORIZON-CL3-2024-DRS-01-04, HORIZON-CL3-2024-DRS-01-05, HORIZON-CL3-2024-DRS-01-06

- Lessons learnt from near-to-real-cases exercises (demonstrations simulating real cases) involving citizen volunteers, local authorities and first responders, with recommendations to be delivered to Member States authorities in charge of management of different types of risks on how to integrate citizen volunteers in the disaster preparedness and response actions and how to coordinate them on site in the disaster area.

- Advisory dissemination materials, highlighting good practices of interactions among citizens, local authorities and first and second responders in the event of (natural or man-made) disasters, addressed to European public in different EU languages.

Scope: Building a common culture for improving societal resilience closely relies not only on the understanding of risks by citizens but also on their engagement in preparatory actions and inclusion of their knowledge. Among them, demonstrations and field validation of risk management approaches, as well as training actions addressing first responders, may have a strong impact on the risk awareness and engagement of citizens in the case of disaster events, supporting citizens in acting efficiently by themselves. This engagement of citizens in disaster and crisis management will also benefit from their involvement in field validation of different approaches / methods used by local authorities and first and second responders, in representative urban and non-urban environments.

An unresolved issue is how spontaneous helpers can be involved systematically in major hazard management by the Government. In the past, such situations revealed that previously unknown helpers were available spontaneously, unexpectedly and in appreciable numbers and that the respective local authorities or officials on site were overwhelmed by this lack of organisation as there were no concepts for equipping, deploying and controlling these helpers. Recent disasters like the covid-19-crisis or in particular the aftermath of the heavy rain events in Summer 2021 have proved again the need for a more efficient and controlled integration of spontaneous volunteers in disaster response. A better preparedness and training of both potential volunteers and first and second responders is therefore needed. On the basis of past experiences built-up by large-scale demonstration projects in the field of natural hazards and CBRN sectors, near-to-real-cases exercises should involve citizen volunteers, local authorities and first and second responders to enhance the understanding of risks and the interactions among different actors (policy-makers and implementers, scientists, practitioners and citizens). Dissemination efforts should be ensured so that experiences with citizens can be widely shared in Europe via social networks and other means.

Furthermore, the demands of the authorities and organisations with security responsibilities change when they have to manage a situation with a large number of spontaneous helpers. Assuming a coordinating role becomes increasingly important. The effects on the established structures as well as the organisational implementation needs to be explored. This also applies to the present role of the professional helpers, for which new aspects might need to be included in their role, for example how to deploy spontaneous helpers. This includes training the staff of volunteer and professional fire services to act as coaches for the spontaneous helpers.

[**References to be added on SSH and societal engagement and/or social innovation**].

DRS02 - Improved Disaster Risk Management and Governance

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-DRS-01-02: Prevention, detection, response and mitigation of biological and chemical threats to agricultural production, forestry and to food processing, distribution and consumption

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[80]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Increase EU capabilities to assess risks, detect, alert, mitigate and respond to food intentional contamination from CBRN agents, through the entire food chain/s (agro-production, food industry, transporting, retail and HO.RE.CA., public catering);
- Increase the understanding on food terrorism threats and on food chain vulnerabilities to intentional and accidental contaminations;
- Raise awareness among big food companies and authorities to CBRN threats arising from malicious use of hazardous agents that pose danger to public health. This should be done under the premises of food as a critical infrastructure and risks pertaining therein;
- Increase the understanding on water supply terrorism threats and vulnerabilities to intentional and accidental contaminations, heighten quality control monitoring systems so the presence of biochemical agents posing a risk to public health are identified faster;
- Create an "*EU food chain protection practitioner network* " and increase their capability to react to intentional contaminations acts and to unforeseen crisis (catastrophic incidents, climate changes crisis);
- Define guidelines of an *European Food Protection Policy* and of an *Urban Food Resilience Plan*, targeting all those European municipalities that want to develop an

[80] This budget is shared with topic HORIZON-CL3-2024-DRS-01-01, HORIZON-CL3-2024-DRS-01-03, HORIZON-CL3-2024-DRS-01-04, HORIZON-CL3-2024-DRS-01-05, HORIZON-CL3-2024-DRS-01-06

integrated approach to profile and secure urban food supply chains, particularly in times of crises.

Scope: Plant and animal health is of global importance for sustainable agriculture and competitive agriculture and forestry, as well as for the protection of biodiversity and ecosystems. Globally, between 10 and 28 percent of crop production is lost to pests and contamination of food and feed by mycotoxins can severely threaten the health of humans and livestock. The International Year of Plant Health (IYPH) 2020, established by the United Nations, raised public and political awareness of the importance of plant health and a recent study (IPPC, 2021) calls the attention of policy makers to the main effects of climate change on plant health, helping governments and the international community addressing plant health challenges. Also the food chain, from harvest of agricultural products, throughout processing, distribution and until consumption can be challenged by several (hybrid) threats, which are increasingly taking non-conventional forms and possibly targeting the agriculture and food chain with severe consequences.

The Word Health Organisation identified intentional agriculture attack with biological weapons and food contamination as one of the main global public health threats of the 21st century. The potential for terrorist attacks or other criminal actions against agri-food targets is increasingly recognised as a threat to international security. The population's health could be jeopardised by the manipulation of communicable diseases or the contamination of food, soil, air and drinking water by CBRN agents. These risks have been studied and documented by a Network of excellence (Plant and Food Biosecurity) funded by the European Commission under the 7th Framework Programme, which addressed the threat of and damage from biological incidents of accidental, natural or intentional origin, including bioterrorism acts (intentional release of harmful biological agents such as bacteria, viruses or toxins to cause fear, illness or death of people, animals or plants and/or disrupt social, economic or political stability). The project tackled the overall risk management cycle, from preparedness, prevention, detection and surveillance to response and recovery in the topic areas of plant biosecurity and food safety, taking also into account the need to ensure a proper transfer and implementation of research outputs, including practical tools to user (producers, policy makers, scientists, agri-food industry and field practitioners).

In 2017, the ENVI Committee (Committee on Environment, Public Health and Food Safety of the EU Parliament) as defined Food Defence as *"the protection of food from intentional contamination or adulteration by biological, chemical, physical or radiological agents. It includes measures regarding prevention, protection, mitigation, response and recovery form intentional acts of food contamination".* The potential impact on human health of deliberate sabotage of agricultural crops, seed or food can be estimated by extrapolation from the many documented examples of unintentional outbreaks of foodborne disease. One of the largest outbreak of hepatitis A associated with consumption of clams in Shanghai, China, in 1991 affected nearly 300'000 people. If an unintentional outbreak from one food can affect 300'000 individuals, a concerted, deliberate attack could be devastating, especially if a more dangerous chemical, biological or radionuclear agent was used.

Current EU capabilities to detect and respond to agro-terrorism and bio-criminal acts are dispersed across different national practitioners, normally handled by regional or national bodies and are very limited in terms of coordination. Different countries have different governmental authorities for agricultural and food domains, different collaborative networks, different border controls, different inspection bodies and different regulatory references and reporting mechanisms as well as different investigative bodies in the case of suspected food crime. The EU institutions have to start to consider the agro-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 multi-sectorial approach combing different expertise with the perspective of establishing a network aimed at protecting global food security that will contribute to increase the resilience of the European food defence system.

The main challenge is to increase the resilience of European agricultural production, food processing and distribution chain in case of sudden external shocks. Agriculture and food chains will be included as an important dimension to be analysed in the context of protection of European critical entities in case of emergencies. 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.

In this context, research should address agri-food systems shocks, with focus on the increasing effects of climate change and global trade (and their interaction) on pest outbreaks and spread, food commodity shocks, due to external challenges, urban Food supply chains interruption, organised agri-food terrorism attacks, and application of cyber security to the agro-food systems

[**References to be added on involvement of SSH and societal engagement and/or social innovation – Cross-reference to FCT / INFRA**].

HORIZON-CL3-2024-DRS-01-03: From Global to Local: how to strengthen Disaster Risk Reduction cooperation among global organizations and local first and second responders

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 2.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[81]
Type of Action	Coordination and Support Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- An inclusive and motivated network bridging other networks bringing together policy makers, industry, academia, practitioners and citizens and relevant actors to support a whole society approach to DRR at different (local, national, regional, and global) levels;
- Disaster risk and resilience map categorizing and connecting existing global, European, national and local networks and centres of expertise (inspired by the cybersecurity atlas: European Cybersecurity Atlas | Cybersecurity Atlas (europa.eu);
- Improving the governance of the expanding system of networks and organizations with an impact on DRR to ensure a constructive, effective, and integrated multilevel DRR governance system that promotes co-design of policies and implementation;
- Developing different levels of interactions and a cooperation mechanism from global, national, regional and local organisations and (first and second) responders in support of the Sendai Framework implementation;
- Shared knowledge and practices on uptake, adapting and adopting existing knowledge and solutions as concrete contribution to Sendai Framework targets.

Scope: One of the guiding principles of the Sendai Framework is that effective Disaster Risk Reduction (DRR) requires coordination and full engagement across scales and sectors to promote and support the availability and application of science and technology to decision making. In this context, multistakeholder cooperation and systematic inclusion of scientific community are essential for developing and implementing DRR activities at all levels (from global to local). In this regard, the mobilization of existing networks to ensure the integration of existing knowledge into policy implementation and development processes is a critical area of priority. Research and practitioner networks, which communicate well and disseminate their findings and work contribute to avoid duplication and allow stakeholders to build on existing results. Such networks also facilitate effective communication and transfer of research outputs to policymakers and conversely, enable policymakers to formulate and address specific questions and challenges to the scientific community. There is a clear recognition in the Sendai Framework that the existing national, regional, and global platforms for DRR have been efficient mechanisms for coherence across agendas, and they have been important in mainstreaming DRR into other policies, and in monitoring and periodic reviews. As an example, the European Scientific and Technical Advisory Group (E-STAG) coordinated by the United Nations is concrete evidence of the growing role to be played by the scientific

[81] This budget is shared with topic HORIZON-CL3-2024-DRS-01-01, HORIZON-CL3-2024-DRS-01-02, HORIZON-CL3-2024-DRS-01-04, HORIZON-CL3-2024-DRS-01-05, HORIZON-CL3-2024-DRS-01-06

community for building regional resilience to disasters. However, one of the biggest challenges to implementing the Sendai Framework is the limited connections between scientific research institutions and decision makers, affecting DRR research, capacity development, and development of risk informed policies. Of particular interest are the cooperation frameworks and dialogues (if any) with policymakers at all levels, highlighting needs for enhanced communication and dissemination of information by existing networks and platforms, stronger linkages between these networks (local, national, regional, and global levels), as well as processes and mechanisms for engagement. The governance of this expanding system of networks and organizations with an impact on DRR needs to be examined to ensure a constructive, effective, and integrated multilevel DRR governance system that promotes co-design of policies and implementation. In this respect, different levels of interactions need to be studied and a cooperation mechanism from global, national, regional and local organisations and (first and second) responders be developed.

[**References to be added on international cooperation, involvement of SSH and societal engagement and/or social innovation**].

DRS03 - Improved harmonisation and/or standardisation in the area of crisis management and CBRN-E

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-DRS-01-04: Harmonised / Standard protocols for the implementation of alert and impact forecasting systems as well as transnational emergency management in the area of flash floods, volcanic and high-impact disasters

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[82]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Enhanced links between scientific community and first and second responders promoting user-targeted research and faster transfer of science results into best practices

[82] This budget is shared with topic HORIZON-CL3-2024-DRS-01-01, HORIZON-CL3-2024-DRS-01-02, HORIZON-CL3-2024-DRS-01-03, HORIZON-CL3-2024-DRS-01-05, HORIZON-CL3-2024-DRS-01-06

- Enhanced adoption of novel technologies such as advanced Earth Observation capabilities and capabilities such as those from Earth Observation space technologies into management practices and tools.
- Enhanced understanding and modelling of complex processes driven to flood events, volcanic eruptions and other high-impact disasters
- Improved methods for cross-border and cross-sectoral knowledge transfer about risk, vulnerability, exposure, and monitoring methods.
- Increased awareness and visibility of elements exposed to flood events and other high impact events.
- Identification of needs and opportunities for transferring advanced scientific results into enhancement in disaster logistics.
- Better understanding and high resolution modelling of the effects of surface runoff after short-term heavy rain events.
- Enhanced monitoring of existing structural flood protection systems
- Reduced flood risk through sustainable floodplain restoration along large rivers in Europe
- Strengthened transnational water management and flood risk prevention

Scope: Europe is confronted with increasingly intense and sometimes unexpected consequences of natural disasters such as floods and heavy rain events, as well as other geohazards such as volcanic eruptions. To respond to these emerging challenges an integrated transnational emergency management is needed, including an ongoing evaluation of applied disaster risk reduction methods, in particular alert and impact forecasting systems, identification of potential for improvement and constant innovation.

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. Emergency management plays a crucial role in this regard, taking into account the ongoing urbanization and economic growth, which put a lot of pressure on areas such as floodplains and their ability to absorb and store water.

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. Recent flash floods in Belgium, Germany and Luxembourg in July

2021 have shown that this lack of protocols hampered the efficient implementation of early warning and preparedness actions prior to the disaster event.

This topic is part of a coordination initiative between ESA and the EC on Earth System Science. Under the EC-ESA Earth System Science Initiative both institutions aim at coordinating efforts to support complementary collaborative projects, funded on the EC side through Horizon Europe and on the ESA side through the ESA FutureEO programme. Proposals should include a work package, means and resources for coordination with complementary projects funded under the Science for Society element of the ESA FutureEO programme. The projects(s) should establish a close coordination and collaboration with the relevant ESA relevant actions and projects (https://eo4society.esa.int).

[**References to be added on international cooperation, involvement of SSH and societal engagement and/or social innovation**].

DRS04 - Strengthened capacities of first and second responders

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-DRS-01-05: Increased technology solutions, institutional coordination and decision-support systems for first responders of last-kilometer emergency service delivery

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[83]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Identification and evaluation of existing technologies, highlighting their strengths and weaknesses.
- Testing and implementation of most promising user-centred technologies in real-worlds conditions.

[83] This budget is shared with topic HORIZON-CL3-2024-DRS-01-01, HORIZON-CL3-2024-DRS-01-02, HORIZON-CL3-2024-DRS-01-03, HORIZON-CL3-2024-DRS-01-04, HORIZON-CL3-2024-DRS-01-06

Scope: Supplying relief items to various demand spots in disaster-prone areas is a critical task due to last-kilometer logistics problems that hamper the process of and efficient transportation of first responders and their equipment. Blocked roads, heavy terrain and bad weather conditions are factors that are faced by first and second responders (e.g. fire brigade, emergency medical services) in the immediate response to disasters. Innovative technologies (e.g. drones, AI, sensors etc.) are considered to support emergency workers in overcoming the aforementioned challenges related to relief items delivery and can provide ability to obtain critical information remotely about the extent, perimeter, or interior of the incident as well as conduct on-scene operations remotely without endangering responders. For example, technology solutions for navigation in smoky environments in the case of wild fires can potentially increase the efficiency of search operations by fire fighters.

[**References to be added on involvement of SSH and societal engagement and/or social innovation**].

HORIZON-CL3-2024-DRS-01-06: Cost-effective sustainable technologies for CBRNE large-scale protection of population and infrastructures

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 29.00 million.[84]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved understanding of the radioactive fallout and methodology regarding robust and rapid monitoring of dose rate and nuclide specific determination with purpose of facilitating safe evacuation after a nuclear or radiological event.
- Improved tools and methods for risk assessment following a nuclear or radiological event and optimized actions after a disaster that are based on risk analysis rather than probabilities.
- Improved protection of population and infrastructures through better analysis of sensor data resulting in adequate protective actions.

[84] This budget is shared with topic HORIZON-CL3-2024-DRS-01-01, HORIZON-CL3-2024-DRS-01-02, HORIZON-CL3-2024-DRS-01-03, HORIZON-CL3-2024-DRS-01-04, HORIZON-CL3-2024-DRS-01-05

- Cost-effective protective measures based on risk analysis.
- Identification of the relevant range of different protective measures needed after a CBRNE disaster.
- Improved filtering techniques and methods for shelters for the protection of citizens following a CBRNE-incident.
- Improved air locks and detection systems providing safe entrance to critical infrastructures.
- Improved methodology regarding the safe and efficient handling of filter for shelters following a nuclear or radiological event.
- Improved understanding of contamination and decontamination of population and infrastructure following a nuclear or radiological event.
- Improved rapid procedures for decontamination of individuals after a CBRNE-incident.
- Reduction of the need for time-consuming decontamination procedures by performing contamination assessment of individuals.

Scope: A nuclear explosion in any EU member country would lead to disastrous effects for numerous EU citizens. For example, the initial effects from a nuclear explosion in a city will lead to, besides numerous dead and severely injured citizens, destroyed infrastructure. The radioactive plume containing particulate matter may damage ventilation systems and fallout will generate high dose rates. 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 CBRNE-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 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 CBRNE-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.

Protective measures in the aftermath of a CBRNE disaster may vary depending on situations. Such measures should be based on evaluated risks rather than probabilities. Starting with sensor- as well as other available data, measures could be optimized from a risk-cost point-of-view resulting in cost-effectiveness.

Based on measurement data, appropriate protective actions could be decided upon. If a risk analysis results in a low risk, a lower level of mitigating measures might be needed resulting in lower costs. Then resources can be used in other areas where they are more needed, leading to an overall optimized protection.

Protective actions should be based on risk modelling. Such modelling is based on available knowledge of different input quantities resulting in a probability distribution, from which the risk can be calculated applying a consequence function.

[**References to be added on involvement of SSH and societal engagement and/or social innovation – Cross-reference to FCT / INFRA**].

Destination - Strengthened Security Research and Innovation

Proposals for topics under this Destination should set out a credible pathway to contributing to the following impacts:

- A more effective and efficient evidence and knowledge-based development of EU civil security capabilities built on a stronger, more systematic and analysis-intensive security research and innovation cycle;
- Increased cooperation between demand and supply market actors, including with actors from other domains, fosters swift industrialisation, commercialisation, adoption and deployment of successful outcomes of security research and reinforces the competitiveness and resilience of EU security technology and industrial base and safeguards the security of supply of EU-products in critical security areas;
- R&I-enabled knowledge and value in cross-cutting matters reduces sector specific bias and breaks thematic silos that impede the proliferation of common security solutions.

The following call(s) in this work programme contribute to this destination: [...]

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-SSRI-01	12.50		23 Nov 2023
HORIZON-CL3-2024-SSRI-01		15.50	
Overall indicative budget	12.50	15.50	

Call - Support to Security Research and Innovation 2023

HORIZON-CL3-2023-SSRI-01

Conditions for the Call

Indicative budget(s)[85]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[86]	Number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-SSRI-01-01	RIA	12.50	Around 1.50	1
HORIZON-CL3-2023-SSRI-01-02	CSA		Around 1.00	2
HORIZON-CL3-2023-SSRI-01-03	IA		Around 3.00	2
HORIZON-CL3-2023-SSRI-01-04	IA		Around 3.00	1
Overall indicative budget		12.50		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.

[85] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

[86] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

SSRI 02 - Increased innovation uptake

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-SSRI-01-01: Effective pathways towards standardisation and certification schemes for security

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 1.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 12.50 million.[87]
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Better understanding of the potential value of standardised solutions and certification schemes for the demand and supply actors in the security market taking into account the specificities of the different policy areas and priorities addressed by the Cluster 3 Work Programme and in the light of the distinctive features of the EU Security market[88];

[87] This budget is shared with topic HORIZON-CL3-2023-SSRI-01-02, HORIZON-CL3-2023-SSRI-01-03, HORIZON-CL3-2023-SSRI-01-04

[88] Some of these features are described in the Action Plan for an innovative and competitive security industry, COM(2012) 417, and in the Commission staff working document on enhancing security through research and innovation COM(2021) 422

- Stronger capabilities for EU security practitioners to address security challenges[89] built on standardised solutions and certifications schemes that leverage the regulatory, policy, operational and market context of such areas.

- Plausible pathways to the development of standardised security solutions (including *de-iure* and *de-facto* approaches) that contemplate the different profiles and roles of actors, notably of EU Agencies, that must intervene in the process as well as the different instruments available, such as the EU standardisation system, public procurement or security research, among others;

- More efficient, harmonised and EU-wide endorsed processes for the development and adoption of standardised security solutions and/or certification schemes by security technology developers and users in high priority security areas;

- Better understanding of the obstacles that impede the development and adoption of standards in the different areas of security as well as of the necessary measures to overcome these;

Scope: In a complex, multidimensional and multinational environment, the impact of the actions taken to ensure the security of citizens are heavily conditioned by the availability and adequacy of the measures (including technology-based ones) deployed to prevent, prepare, react and recover from the occurrence of security threats. The quality, harmonisation, interoperability, innovation and trust brought by standardised solutions is therefore desirable in the field of civil security insofar as: i) It would increase the chances that the market is ready to offer security solutions when and where these are required; ii) It would increase the level of confidence in the quality and performance of such solutions.

Likewise, certification, understood as the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements[90], can be a useful tool to add credibility to the security equipment acquired by practitioners by demonstrating that it meets the quality and performance expectations. It also has a positive effect on the creation of a clearer European identity for these technologies[91] that should contribute to enhancing the global competitiveness of the EU companies with regards to third country competitors.

However, the definition and implementation of EU security standards and certification schemes has proven to be challenging. The obstacles found so far have their roots not only in the particular features of the security market and the EU standardisation system[92], but also in diverging national interests, in how Member State authorities have traditionally built

89 Actions shall not focus on one concrete area of security, but cover the full landscape of security areas addressed under the destinations FCT, BM, INFRA and DRS. When touching upon Disaster Risk Management, actions funded under this topic shall avoid overlapping and build on the results, as needed, of actions funded under the DRS destination in this and previous Work Programmes.

90 https://www.iso.org/conformity-assessment.html

91 An "EU brand", as referred to in the Action Plan for an innovative and competitive security industry, COM(2012) 417

92 COM(2018) 764

operational capacity or in highly competitive industrial dynamics. However, the underlying reasons for the lack of EU standards or common certification schemes for security technology are not easily identifiable. In order to fill this gap in our understanding of the phenomenon and to be in a position to propose measures to address this challenge, a thorough and holistic analysis is required.

Applicants are invited to submit proposals to explore how the development and adoption of EU standardised security solutions and certification schemes would impact the effectiveness and efficiency of the measures put in place by the EU and the Member States to face current and future threats. In relation to common certification schemes, research should also address the possibility of defining and implementing common methods for the verification and validation of security technologies (including technical performance, operational effectiveness and trustworthiness) developed under the frame of EU-funded security research projects and with the aim of ensuring the wide acceptance of their outcomes by the end-user community. To that end, emphasis should be made on the potential use and implementation of sandbox environments (technical and regulatory), in alignment with the resources being deployed by the innovation labs of EU agencies (i.e. Europol, Frontex and eu-Lisa).

In addition, research should show how standardised security solutions and certification schemes can be utilised to give continuity to the results of EU-funded research onto other funding instruments oriented to the commercialisation (e.g. EIC Accelerator) and/or the acquisition and deployment (e.g. ISF, IBMF) of innovative technologies.

The proposed research will need to take into consideration the EU security policy priorities addressed by the Cluster 3 Work Programme (including in the area of Infrastructure Protection, Disaster Resilience, Fight Against Crime and Terrorism and Border Management), the particular features of the EU security market, the relevant legal framework in place and the roles of the different stakeholders that could potentially steer and contribute to the development and adoption of EU standardised security solutions and certification schemes (e.g. policy makers, security authorities, end-users, public buyers, industry –including SMEs- and other organisations of interest –including European Standards Organisations-). Especial emphasis should be made on the role of EU Agencies[93] and of the EU Innovation hub for internal security.

Research should not only shed light on the value of standards and certification, but also on the obstacles that impede their development and adoption, the challenges and opportunities to address those obstacles and practical pathways to follow in cases where their potential value justifies the action. The alternatives proposed should not only focus on formal *de-iure* standards issued by European Standardisation Organisations (CEN, CENELEC, ETSI) and National Standardisation Bodies, but also, and notably, on *de-facto* approaches that can rely on multilateral voluntary agreements, joint cross-border public procurement or research, among other instruments. Comparing the adequacy of each approach in different scenarios derived

[93] For example, the European Border and Coast Guard Regulation (REGULATION (EU) 2019/1896), in its Article 10, states that the tasks to be performed by the European Border and Coast Guard Agency include, among others, the development of technical standards for information exchange and the support to the development of technical standards for equipment in the area of border control and return, and the development of common minimum standards for external border surveillance.

from the context mentioned above shall be the basis for the applicants to deliver concrete policy recommendations for the development and adoption of EU standardised solutions.

Proposals shall envisage a close collaboration and interaction with the EC-chaired or funded initiatives that hold the widest body of knowledge in the area of security research, such as the Networks of Practitioners funded under H2020 Secure Societies work programme, the European Networks for Security Research & Innovation funded under Horizon Europe Cluster 3 work programme, the Community of European Research and Innovation for Security (CERIS), the innovation labs of EU Agencies and the EU innovation hub for internal security. The proposals shall also exploit the knowledge and build on the results of previous or current EU-funded security research projects with activities in the field of pre-normative research and standardisation, as well as on the achievements of ongoing policy-led initiatives for the development of mandatory or voluntary standardisation and certification schemes.

The project shall have a maximum estimated duration of 2 years.

International cooperation is encouraged.

Also in this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content is a mandatory requirement.

HORIZON-CL3-2023-SSRI-01-02: Open grounds for pre-commercial procurement of innovative security technologies

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 1.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 12.50 million.[94]
Type of Action	Coordination and Support Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Consolidated demand for innovative security technologies built on the aggregation of public buyers with a common need expressed in functional and/or operational terms without prescribing technical solutions;

[94] This budget is shared with topic HORIZON-CL3-2023-SSRI-01-01, HORIZON-CL3-2023-SSRI-01-03, HORIZON-CL3-2023-SSRI-01-04

- Better informed decision-making related to investment in innovative security technologies based on a better understanding of the potential EU-based supply of technical alternatives that could address common needs of EU public buyers;

- Better informed decision-making related to investment in innovative security technologies based on an improved visibility of the potential demand in the EU market for common security technologies;

- Increased capacity of EU public procurers to align requirements with industry and future products and to attract innovation and innovators from security and other sectors through common validation strategies, rapid innovation, experimentation and pre-commercial procurement.

Increased innovation capacity of EU public procurers through the availability of innovative tendering guidance, commonly agreed validation strategies and evidence-based prospects of further joint procurement of common security solutions.

Scope: End-users and public procurers from several countries are invited to submit proposals for a preparatory action that should build the grounds for a future Pre-Commercial Procurement action. Both this preparatory action and the future PCP action are open to proposals oriented to the acquisition of R&D services for the development of innovative technologies, systems, tools or techniques to enhance border security, to fight against crime and terrorism, to protect infrastructure and public spaces, and/or to make societies more resilient against natural or man-made disasters.

Projects funded under this topic should also consider submitting a proposal to an open call for a follow-up PCP action that the Commission may include in the Cluster 3 Work Programme 2025-2027 (subject to budget availability and priorities of the Work Programme 2025-2027). In preparing the grounds for a possible future PCP action, the outputs of this CSA should take into consideration:

- The policy priorities described in this Work Programme Part for the security areas mentioned above;

- The EU Directive for public procurement and in particular with the provisions related to PCP;

- The specific provisions and funding rates of PCP actions and the specific requirements for innovation procurement (PCP/PPI) supported by Horizon Europe grants, as stated in the General Annex H of the Horizon Europe Work Programme;

- The guidance for attracting innovators and innovation, as explained in the European Commission Guidance on Innovation Procurement C(2021) 4320, in particular those measures oriented to reduce the barriers to high-tech start-ups and innovative SMEs.

During the course of the project, the applicants are expected to deliver clear evidence on a number of aspects in order to justify and de-risk a possible follow-up PCP action, including:

- That the challenge is pertinent and that indeed a PCP action is required to complete the maturation cycle of certain technologies and to compare different alternatives;
- That there is a consolidated group of potential buyers with common needs and requirements which are committed to carry out a PCP action in order to be able to take an informed decision on a future joint-procurement of innovative solutions;
- That there is a quantifiable and identifiable community of potential buyers (including and beyond those proposed as beneficiaries in the proposal) who would share to a wide extent the common needs and requirements defined and who could be interested in exploring further joint-uptake of solutions similar to those developed under the PCP, should these prove to be technologically mature and operationally relevant by the end of the project;
- That the state of the art and the market (including research) has been explored and mapped, and that there are different technical alternatives to address the proposed challenge;
- That a future PCP tendering process is clear, that a draft planning has been proposed and that the supporting documentation and administrative procedures will be ready on due time in order to launch the call for the acquisition of R&D services according to the PCP rules.
- That the technology developments to be conducted in the future PCP can be done in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data.
- That in developing technology solutions, societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) can be taken into account in a comprehensive and thorough manner.

If the applicants intend to submit a proposal for a follow-up PCP in a future Horizon Europe Cluster 3 Work Programme, they should ensure that the above evidence is consolidated in the project deliverables of this CSA before the submission of the PCP proposal.

The project should have a maximum estimated duration of 1 year.

HORIZON-CL3-2023-SSRI-01-03: Accelerating uptake through open proposals for advanced SME innovation

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Indicative budget	The total indicative budget for the topic is EUR 12.50 million.[95]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Facilitated access to civil security market for small innovators;
- New business models to bring innovation closer to the public security buyers;
- 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 big and small EU security industry and technology actors to ensure the sustainability of the EU innovation capacity in the civil security domain and increase technological sovereignty of the EU in critical security areas.

Scope: Europe's 25 million small and medium enterprises (SMEs) are the backbone of the EU economy. SMEs can bring innovation to societal challenges, including the security of EU citizens. Innovative SMEs and high-tech start-ups can transform and modernise EU security capabilities.

However, despite the innovation capacity of EU SMEs, these often experience difficulties in finding their way to the public markets. These include red-tape in public contracts, access to new customers, access to finance, industrial competition and IP valorisation. These difficulties are exacerbated in markets that show restrictions of different kind, as it is the case of security.

Knowing that SMEs require additional support to reach the security buyers and that the collaboration opportunities offered by the projects of the Pillar II of Horizon Europe can be a catalyst for uptake, this topic aims to offer a collaborative environment for small innovators to tailor their innovations to the specific needs of civil security end-users.

Applicants are invited to submit proposals for technology development along with the following principles:

- Focus on mature technological solutions addressing EU security policy priorities in the areas addressed by the Cluster 3 work programme.
- Not overlapping with the scope of the topics included in the other destinations of this work programme
- Fostering collaboration between SMEs from different MS

[95] This budget is shared with topic HORIZON-CL3-2023-SSRI-01-01, HORIZON-CL3-2023-SSRI-01-02, HORIZON-CL3-2023-SSRI-01-04

- With high involvement of security end-users in the role of validator and potential first-adopter of the proposed innovations

- Fostering collaboration schemes between small companies and research and technology organisations and/or big industrial players aimed at fostering innovative technology transfer or creating innovative business models that facilitate access to market and strengthen the innovation capacity of EU SMEs and start-ups in the domain of civil security.

The involvement of big industries in the projects should not focus on technology development but on supporting the SMEs in bringing their innovations to the market. Examples of activities include but are not limited to, acting as first buyer/integrator of the developed technologies, assimilating market requirements, facilitating access to additional funding, approaching potential public buyers, assess competitive landscape, supporting in innovation management (methodological and process innovation, business model innovation, market innovation), assist in IP management and exploitation, provide guidance for expansion to future markets, etc. In the same fashion, the participation of research and technology organisations should not focus on technology development but on supporting the small industrial players in accelerating the technology transfer of innovative security solutions for their further development and production.

It is encouraged that one SME takes the coordinator role[96]. Exceptions to this requirement should be duly justified.

The projects shall have a maximum estimated duration of 2 years.

In this call, projects should address the areas of FCT and DRS. Some examples of domains that could be addressed under the FCT area are: […]. Some examples of domains that could be addressed under the DRS area are: […].

Only one project addressing FCT and one project addressing DRS will be funded.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content is not a mandatory requirement.

SSRI 03 – Cross-cutting knowledge and value for common security solutions

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-SSRI-01-04: Improved safety and security of security practitioners operating in hazardous environments

Specific conditions

[96] If a MIDCAP is included in the proposal, it could also take the role of coordinator.

Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 12.50 million.[97]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved safety, security, performance and user experience (including personal safety and security) for EU security practitioners operating in hazardous environments;
- Better situational awareness supporting decision-making systems of European security authorities, civil protection and medical emergency services including better communication, preparedness and preparation.

Scope: The safety, security, performance and user experience of security practitioners is an increasingly demanding capability, where the use of next generation technologies can be decisive.

EU security practitioners operate in hazardous environments with a wide variety of threats to their integrity. These can range from the increased brutality of criminals, making use of automatic weapons, to the exposure to blasts and CBRN incidents (both intentional and accidental), the operation in rough environmental conditions (e.g. at high seas) or pandemics outbreaks. Increasing the personal protection, comfort and tactical situation awareness of police officers, border guards, customs officers and first responders (including civil protection and medical emergency services) can not only save lives, but also contribute to a more effective and dynamic response to security threats.

Therefore, the equipment of EU security practitioners needs to be updated to the latest technological advancements. This could include new lightweight materials, smart wearable IoT devices with advanced human interfaces. It could also include advanced sensors, not only to increase their tactical situational awareness but also to facilitate the monitoring of their vital functions and the tracking of their position and movements. All these systems need to be integrated into an architecture that is modular and that ensures communication and interoperability with Command and Control centres, with other officers and with tactical equipment deployed on the field of operations such as detection equipment, communications, autonomous systems and remotely operated platforms.

Significant progress made in the defence domain, where the enhancement of force protection in the domains of C-IED and CBRNe capabilities and Personnel Recovery techniques was

[97] This budget is shared with topic HORIZON-CL3-2023-SSRI-01-01, HORIZON-CL3-2023-SSRI-01-02, HORIZON-CL3-2023-SSRI-01-03

identified as a priority in the 2018 CDP revision[98]. This has led to research developments in this area, such as the projects funded following the 2017 call of PADR, where the topic PADR-FPSS-01-2017, subtopic b) addressed tailor-made blast, ballistic and CBRN protection of military personnel.

Bearing in mind the specificities of the operational environment of police forces, border guards, customs officers and civil protection practitioners, the developments carried out for defence applications cannot be directly used for civil applications. However, technology developments in the defence domain can serve as a reference for the development of future protective equipment for civil security stakeholders.

Applicants are invited to propose solutions for cutting-edge personal protection equipment for security practitioners in the lines described above. Research should build, to the extent possible, on the results of previous EU funded security research projects such as the FP7 projects IF REACT[99] and SMARTPRO[100]. Research should not unnecessarily duplicate or overlap with previous research in the defence domain, such as the VESTLIFE project[101] funded under the PADR and other research projects funded under the Joint Investment Programme on CBRN protection established by the EDA[102]. However, research should build on their results to the extent possible.

Proposals should consider a strong involvement of end-users in the design, testing and validation of the proposed solutions. In particular, the priorities of the EU-agencies in this domain should be addressed. Proposals should also take into account requirement for green and sustainable equipment, as well as legal and ethical, including data protection, requirements.

Solutions developed under this topic should be validated in high-fidelity scenarios with close to real operational conditions. These scenarios shall contemplate different hazardous situations for police authorities, border guards, customs authorities and civil protection practitioners. Extensive validation should therefore be conducted, where the user experience can be used not only to evaluate the operational relevance of the solutions proposed but also to refine the system design for an optimal configuration.

Also in this topic the integration of the gender dimension in research and innovation content is a mandatory requirement.

Call - Support to Security Research and Innovation 2024

HORIZON-CL3-2024-SSRI-01

98 "The EU Capability Development Priorities: 2018 CDP revision", European Defence Agency, 2018
99 https://cordis.europa.eu/project/id/285034
100 https://cordis.europa.eu/project/id/607295
101 https://ec.europa.eu/defence-industry-space/vestlife_en
102 https://eda.europa.eu/what-we-do/all-activities/activities-search/captech-cbrn-and-hf

Conditions for the Call

Indicative budget(s)[103]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[104]	Number of projects expected to be funded
		2024		
Opening: na				
HORIZON-CL3-2024-SSRI-01-01	PCP	15.50	Around 6.00	1
HORIZON-CL3-2024-SSRI-01-02	IA		Around 3.00	2
HORIZON-CL3-2024-SSRI-01-03	IA		Around 3.50	1
Overall indicative budget		15.50		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.

103 The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

104 Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

SSRI 02 – Increased innovation uptake

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-SSRI-01-01: Demand-led innovation through public procurement

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 15.50 million.[105]
Type of Action	Pre-commercial Procurement

Expected Outcome: 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).

Scope: End-users and public procurers from several countries are invited to send proposals for launching a Pre-Commercial Procurement action for the acquisition of R&D services for the development of innovative civil security technology solutions.

The proposals should build on the outcomes of CSA projects funded under previous work programmes aimed at creating *Stronger grounds for pre-commercial procurement of innovative security technologies*[106]. The successful proposals could therefore give continuity to the works initiated by those CSA projects.

[105] This budget is shared with topic HORIZON-CL3-2024-SSRI-01-02, HORIZON-CL3-2024-SSRI-01-03

[106] *For example, topic HORIZON-CL3-2022-SSRI-01-03: Stronger grounds for pre-commercial procurement of innovative security technologies.*

The proposals are expected to provide clear evidence on a number of aspects in order to justify and de-risk the PCP action, including:

- That the challenge is pertinent and that indeed a PCP action is required to complete the maturation cycle of certain technologies and to compare different alternatives;
- That there is a consolidated group of end-users and procurers with common needs and requirements which are committed to carry out a PCP action in order to be able to take an informed decision on a future joint-procurement of innovative solutions;
- That there is a quantifiable and identifiable community of potential buyers (including and beyond those proposed as beneficiaries in the proposal) who would share to a wide extent the common needs and requirements defined and who could be interested in exploring further joint-uptake of solutions similar to those developed under the PCP, should these prove to be technologically mature and operationally relevant by the end of the project;
- That the state of the art and the market (including research) has been explored and mapped to the needs, and that there are different technical alternatives to address the proposed challenge;
- That the PCP tendering process is clear, that a draft planning has been proposed and that the supporting documentation and administrative procedures will be ready in due time in order to launch the call for R&D services according to the PCP rules.
- That there is a commitment to pursue the exploitation of results beyond the end of the project through engagement with stakeholders and implementation of exploitation strategies towards future uptake.

The open market consultations required prior to launching the PCP call for tenders must have taken place in at least three EU Member States. Market consultations conducted during the previous CSA projects can be used if this requirement is fulfilled, and if it is justified that: i) their purpose was enough to guarantee the viability of the procurement and; ii) that the state-of-the-art has not changed since they were conducted.

In relation with the PCP tendering process, the applicants should clarify how they intend to guarantee that:

- The principles of the EU Directive for public procurement and in particular with the provisions related to PCP will be duly respected;
- Conflict of interests will be avoided, including through the ineligibility of bids from technology providers who are also beneficiaries of the project or who have been beneficiaries of the previous CSA projects;
- The confidentiality of the intellectual property of potential bidders will be protected;

- The technology developments to be conducted in the PCP will be done in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data;

- In developing technology solutions, societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) will be taken into account in a comprehensive and thorough manner;

- All participating public buyers commit to comply with EU data protection legislation in the development of innovative, advanced systems to support security and in particular the principles of data protection by design and by default;

- The guidance for attracting innovators and innovation, as explained in the European Commission Guidance on Innovation Procurement C(2021) 4320, will be duly taken into account, in particular those measures oriented to reduce the barriers to high-tech start-ups and innovative SMEs.

Applicants should propose an implementation of the project that includes:

- A minimal preparation stage dedicated to finalise the tendering documents package for a PCP call for tenders based on the technical input resulting from the previous CSA projects, and to define clear verification and validation procedures, methods and tools for the evaluation of the prototypes to be developed throughout the PCP phases.

- Launching the call for tenders for research and development services. The call for tenders should envisage a competitive development composed of different phases that would lead to at least 2 prototypes from 2 different providers to be validated in real operational environment at the end of the PCP cycle;

- Conducting the competitive development of the prototypes following the PCP principles including a design phase, an integration and technical verification phase and a validation in real operational environment phase. In evaluating the proposals and the results of the PCP phases, the applicants should consider technical merit, feasibility and commercial potential of proposed research efforts.

- Consolidating the results of the evaluation of the developed prototypes, extracting conclusions and recommendations from the validation process, and defining a strategy for a potential uptake of solutions inspired in the PCP outcomes, including a complete technical specification of the envisaged solutions and standardisation needs and/or proposals. This strategy should consider joint-cross border procurement schemes and exploit synergies with other EU and national non-research funds.

The applicants are expected to maximise the visibility of the project outcomes to the wide community of potential EU public buyers. Liaison with other civil security communities beyond those addressed by the project is encouraged in order to assess the possible reuse and extensibility of the identified solutions to different domains.

HORIZON-CL3-2024-SSRI-01-02: Accelerating uptake through open proposals for advanced SME innovation

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 15.50 million.[107]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Facilitated access to civil security market for small innovators;
- New business models to bring innovation closer to the public security buyers;
- 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 big and small 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.

Scope: Europe's 25 million small and medium enterprises (SMEs) are the backbone of the EU economy. SMEs can bring innovation to societal challenges, including the security of EU citizens. Innovative SMEs and high-tech start-ups can transform and modernise EU security capabilities.

However, despite the innovation capacity of EU SMEs, these often experience difficulties in finding their way to the public markets. These include red-tape in public contracts, access to new customers, access to finance, industrial competition and IP valorisation. These difficulties are exacerbated in markets that show restrictions of different kind, as it is the case of security.

Knowing that SMEs require additional support to reach the security buyers and that the collaboration opportunities offered by the projects of the Pillar II of Horizon Europe can be a catalyst for uptake, this topic aims to offer a collaborative environment for small innovators to tailor their innovations to the specific needs of civil security end-users.

Applicants are invited to submit proposals for technology development along with the following principles:

[107] This budget is shared with topic HORIZON-CL3-2024-SSRI-01-01, HORIZON-CL3-2024-SSRI-01-03

- Mature technological solutions addressing EU security policy priorities in the areas addressed by the Cluster 3 work programme.
- Not overlapping with the scope of the topics included in the other destinations of this work programme
- Fostering collaboration between SMEs from different MS
- With high involvement of security end-users in the role of potential first-adopter of the proposed innovations
- Fostering collaboration schemes between small companies and research and technology organisations and/or big industrial players aimed at fostering innovative technology transfer or creating innovative business models that facilitate access to market and strengthen the innovation capacity of EU SMEs and start-ups in the domain of civil security.

The involvement of big industries in the projects should not focus on technology development but on supporting the SMEs in bringing their innovations to the market. Examples of activities include but are not limited to, acting as first buyer/integrator of the developed technologies, assimilating market requirements, facilitating access to additional funding, approaching potential public buyers, assess competitive landscape, supporting in innovation management (methodological and process innovation, business model innovation, market innovation), assist in IP management and exploitation, provide guidance for expansion to future markets, etc. In the same fashion, the participation of research organisations should not focus on technology development but on supporting the small industrial players in accelerating the technology transfer of innovative security solutions for their further development and production.

It is encouraged that one SME takes the coordinator role[108]. Exceptions to this requirement should be duly justified.

The projects shall have a maximum estimated duration of 2 years.

In this call, projects should address the areas of BM and INFRA. Some examples of domains that could be addressed under the BM area are: […]. Some examples of domains that could be addressed under the INFRA area are: […].

Only one project per area will be funded.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content is not a mandatory requirement.

SSRI 03 – Cross-cutting knowledge and value for common security solutions

Proposals are invited against the following topic(s):

[108] If a MIDCAP is included in the proposal, it could also take the role of coordinator.

HORIZON-CL3-2024-SSRI-01-03: Data repository for security research and innovation

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 15.50 million.[109]
Type of Action	Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Accurately gathered, stored, managed and preserved research training and testing data, which is verified and selected in order to be realistic, up-to-date and sufficient, makes research more trustworthy and reproducible.
- Researchers and projects can further increase the impact and visibility of their work by not just archiving research materials, but also opening them up for reuse and citation by other relevant actors and stakeholders.
- Properly shared and re-used relevant research data can save lives, help develop solutions and maximise the knowledge.

Enhanced collaboration among relevant research community, improved trust between researchers and practitioners/end-users, facilitated co-operation between different research projects and reduced burden of wasted research or lost results.

Scope:

- Avoiding that security research projects develop important data and at the end of their life cycle, this data is simply lost instead of being stored and handed over to the following project, which unnecessarily needs to start gathering this perhaps already existing research material again from scratch.
- In security domain, due to its specificities, the special categories of data involved or/and unique limitations, which may call for additional requirements, a consolidated, common research database is particularly desired. It is of utmost importance that security practitioners are provided with an increased interoperability and improved (cross-border) exchange of data thanks to harmonised data file formats across Europe, which would easily take into account technological evolutions, i.e. be adaptable in time. Such a lack of realistic, up-to-date and sufficient training and testing data for research purposes and consequently the need for a database, data repository or any other effective and useful

[109] This budget is shared with topic HORIZON-CL3-2024-SSRI-01-01, HORIZON-CL3-2024-SSRI-01-02

tool(s) to gather, manage and store varying security research data, have been regularly raised by the projects working in the area of security.

- As a follow up of the outcomes and results of the running/finished project coming from the 2021 data topic: HORIZON-CL3-2021-FCT-01-04: Improved access to fighting crime and terrorism research data, the successful proposal, should subsequently focus on creation and deployment of a fully functional and operational common research data repository, which will extend to cover other security research areas.

- The 2021 data topic project: HORIZON-CL3-2021-FCT-01-04: Improved access to fighting crime and terrorism research data will develop the skeleton of how such a repository of R&I data should be created, by providing a detailed roadmap consisting of a clear set of rules, conditions and characteristics that such a consolidated database should have. This roadmap will provide technical, legal and ethical requirements for a training and testing research data mostly in the area of fighting crime and terrorism but the same project will already take into account possible applications of identified solutions in different security research domains, such as infrastructure resilience, border management or disaster resilience. The roadmap will also assess if the repository should be centralised or distributed, how to deal with "aging" data, how efficiently projects should exchange data among them taking into account security R&I specificities.

- The newly developed data repository will enable security community (researchers, practitioners, industry, policy makers) access the scientifically satisfactory amount of up-to-date high quality and realistic data which is or was used to develop reliable (mostly digital and based on AI but also non-digital and not linked with big data) tools, technologies and solutions in support of security research and innovation. This data repository could also be very useful for verification and validation of new innovative security solutions developed under various calls in the most recent Work Programme.

- Taking into account the complexity of the future repository, a multi-faceted approach will be needed and the proposal, with the help of the roadmap's findings developed by the previous 2021 project, should look into, among other issue, the following aspects:

    - What exact data should be stored in the repository

    - Interoperability with existing operational systems

    - Interoperability/compatibility with European open science cloud (EOSC), with the developments carried out under the Digital Programme and with the developments carried out under the ISF 2021 data call.

    - How to search for data

    - Data models for security research - Harmonising of data formats

    - Concept of operations for the use of the repository by/during EU-funded security R&I projects, modalities of use, user profiles/schemes, etc.

  - Legal issues, avoidance of any bias, accessibility levels related to the sensitivity of various data sets, solutions for annotation as well as for the aging of the data, etc.

- The proposal should carry out extensive testing and evaluation (verification and validation), in close cooperation with ongoing projects, which would access the repository, populate it and use data intensively during the project implementation.

- The proposal should develop an exploitation and sustainability plan, including funding instruments to be used for the operationalisation of the prototype developed under the project as well as finding possibilities to maintain the repository after the lifetime of the project so that it not only continues to well function but is able to be extended with new data. The data repository will need to grow so it will have to be treated as an ongoing system. Co-ordination with already existing platforms or communities already using another reliable domain-specific data repository/ies for archiving and sharing research data is strongly recommended in order to verify if it would be possible to adhere in the future to a larger system or infrastructure of repositories such as European Open Science Cloud (EOSC) for example.

- Adopting sound security practices, such as developing comprehensive access rules to allow only authorized users with a legitimate need to access, modify, or transmit data, are crucial. Combined with a digital signature approach or multi-factor authentication, access rules go a long way in keeping sensitive data stored in a data repository secure. These and other security measures will enable the research community to fully leverage large volumes of data without introducing unnecessary security risks.

- The repository developed by the proposal should preserve the research data in different security research domains, such as infrastructure resilience, border management or disaster resilience across time and help security research community easily find, access and re-use the necessary data. The development and the functioning of the repository will be based on the outcomes of the roadmap from the 2021 FCT call project within the remits of Horizon Europe regulation (including ethics). Data sharing will be based on open science principle of ‘as open as possible, as closed as necessary’. To make data Findable, Accessible, Interoperable, and Reusable (FAIR), the basics of good Research Data Management will have to be applied.

- All necessary system features as well as the functioning of the repository should comply with privacy and data protection requirements when handling data, in order to facilitate data management ensuring full access to the data actually needed (in line with the necessity and proportionality principle and in full respect of fundamental rights and applicable legislation.

Budget[110]

	Budget line(s)	2023 Budget (EUR million)	2024 Budget (EUR million)
Calls			
HORIZON-CL3-2023-FCT-01		43.00	
	from 01.020230	*43.00*	
HORIZON-CL3-2024-FCT-01			37.00
	from 01.020230		*37.00*
HORIZON-CL3-2023-BM-01		28.82	
	from 01.020230	*28.82*	
HORIZON-CL3-2024-BM-01			29.00
	from 01.020230		*29.00*
HORIZON-CL3-2023-INFRA-01		See footnote[111]	
HORIZON-CL3-2024-INFRA-01			15.00
	from 01.020230		*15.00*
HORIZON-CL3-2023-CS-01		See footnote[112]	
HORIZON-CL3-2024-CS-01			
HORIZON-CL3-2023-DRS-01		28.82	
	from 01.020230	*28.82*	
HORIZON-CL3-2024-DRS-01			29.00
	from 01.020230		*29.00*
		12.50	

110 The budget figures given in this table are rounded to two decimal places.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

111 To which EUR 15.04 million from the 'na' budget will be added making a total of EUR 15.04 million for this call.

112 To which EUR 70.25 million from the 'na' budget will be added making a total of EUR 70.25 million for this call.

HORIZON-CL3-2023-SSRI-01	*from 01.020230*	*12.50*	
HORIZON-CL3-2024-SSRI-01			15.50
	from 01.020230		*15.50*
Other actions			
Estimated total budget		113.15	125.50