EN

Annex V

Horizon Europe

Work Programme 2026-2027

6. Civil Security for Society

DISCLAIMER

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the Member State or entity to which it is addressed for discussions and may contain confidential and/or privileged material.

Table of contents

Introduction

Cluster 3 provides a research and innovation response to a context of rapidly changing threats and challenges to internal security, the security of citizens, critical infrastructure and the security of society as a whole. These threats are driven by geopolitical, technological and societal changes, including:

- Instability, hybrid threats and the resurgence of war on the European continent, in particular the Russian war against Ukraine, making the need for civilian protection, preparedness, and resilience.
- Continued threat from terrorism and increased threat from organised crime.
- The potential for large-scale movements of people, whether as a result of war, the instrumentalisation of migration or other drivers, require effective border management capabilities and further efforts to combat migrant smuggling, trafficking in Human Beings (THB), and possible terrorist infiltration.
- More frequent and serious climate-related extreme events as well as other disasters, whether accidental or intentional, of human or natural origin, requiring disaster risk management and response.
- Continued technological development and digitalisation create new and unforeseen vulnerabilities and new opportunities for criminals and violent extremists, as well as new challenges, needs and opportunities for security practitioners.
- Cyber threats that put infrastructures, businesses and individuals at risk.
- Negative socio-economic trends and climate adaptation that create potential for greater social polarisation and mistrust, which may escalate into conflict and/or create opportunities for extremists and malicious actors to spread hate speech and disinformation.

In addressing these and their related challenges, this Work Programme will support the implementation of the EU's upcoming Internal Security Strategy and Preparedness Union Strategy and the sectoral strategies, legislation and action plans identified in the **Destinations**:

- **Better protect the EU and its citizens against Crime and Terrorism (FCT)**

Link to the Horizon Europe strategic plan 2025-2027: Expected impact 13 "Tackling crime and terrorism more effectively and increasing the resilience of infrastructures".

- **Effective management of EU external borders (BM)**

Link to the Horizon Europe strategic plan 2025-2027: Expected impact 12 "Facilitating legitimate movement of passengers and goods into the EU, while preventing illicit acts".

- **Resilient infrastructure (INFRA)**

Link to the Horizon Europe strategic plan 2025-2027: Expected impact 13 "Tackling crime and terrorism more effectively and increasing the resilience of infrastructures".

- **Disaster-Resilient Society for Europe (DRS)**

Link to the Horizon Europe strategic plan 2025-2027: Expected impact 11. “Reducing losses from natural, accidental and human-made disasters”.

- **Strengthened Security Research and Innovation (SSRI)**

Link to the Horizon Europe strategic plan 2025-2027: Cross-cutting Destination that supports all the Expected impacts identified above.

Each Destination includes an introductory section that explains the relevant policy objectives, specifies elements to be taken into account for the topics of the Destination and identifies specific expected impacts. Proposals should set out a credible pathway to contribute to the specific expected impacts.

In addition, under this Work Programme, the Commission intends to entrust implementation of a call for proposals to the European Competence Centre for Cybersecurity (ECCC). The call topics foreseen for this indirectly managed action (see Appendix to this Work Programme part) relate to:

- **Increased Cybersecurity (CS)** *Link to the Horizon Europe strategic plan 2025-2027:* Expected impact 14 “Increasing cybersecurity and making the online environment more secure”.

Cluster 3 Work Programmes will support the implementation of the European Commission political guidelines 2024-2029 for a ‘Safer and more secure Europe’, a ‘Preparedness Union’, with ‘Stronger Common Borders’, protecting democracy and putting research and innovation at the heart of a resilient economy. Overall, research under this Cluster should continue to focus on preserving and securing **citizens’ basic right to feel safe.** Cluster 3 ‘civil security for society’ will therefore also support the Commission’s work:

- towards a new European Internal Security Strategy, fighting organized crime and ensuring that security is integrated in EU legislation and policies by-design.
- towards a European Civil Defence Mechanism, looking at all facets of crisis and disaster management, along community resilience building.
- to provide practitioners, law enforcement, first and second responders, critical infrastructure operators, with adequate and up-to-date tools for lawful access to digital information, while safeguarding fundamental rights.
- to strengthen European competitiveness and make better use of public procurement and in particular support innovation procurement.

Successful projects need to show their understanding of and contribution to a wider innovation cycle based on a needs-driven capability development approach that triggers research, steers its implementation and capitalises on its outcomes. This means that projects need to show, on the one hand, an understanding of the capability requirement and policy context that has led to the R&I need, and, on the other hand, a strategy for ensuring the uptake of the outcomes including opportunities where relevant for using EU funds for deployment.

Cross-cutting themes

Various themes run through this Work Programme, cutting across the different sectoral Destinations. A first set of themes respond to the wider challenges identified in the three key strategic orientations of the Horizon Europe strategic plan 2025-2027:

- *Strengthening resilient societies and democracy*. The central focus of Cluster 3 is supporting the prevention, preparedness and response to the wide range of threats to internal security identified above, as well as ensuring the security of all citizens, critical infrastructure and of society as a whole. Strengthening our democracies and making them more resilient – both materially and psychologically – has taken on a new urgency since the full-scale Russian invasion of Ukraine. European citizens need to be protected from hybrid threats such as disinformation campaigns or fake news while upholding the rule of law and basic freedoms, including freedom of speech. Civil security research and innovation needs to equip civil security practitioners with the ability to mitigate the consequences of armed conflict, in particular attacks on critical infrastructures. By funding research to strengthen and prepare our societies, democracies, and infrastructure against hybrid threats, Cluster 3 shows its ability to adapt to changing conditions and challenges.
- *Securing the digital transition*. The more widespread and ubiquitous digital technology is, the greater the threats of new and unforeseen vulnerabilities and new opportunities for criminals and violent extremists as well as new challenges, needs and tools for law enforcement authorities, infrastructures, businesses and individuals. Research on cybercrime and cybersecurity helps to address these matters. With the aim of creating a secure and trustworthy digital environment, Cluster 3 will invest in cybersecurity R&I to strengthen the EU's resilience, protect its infrastructures, and improve its ability to cope with cyber incidents. This will help increase the EU's open strategic autonomy in cybersecurity. Cluster 3 addresses cybercrime and the developing security threats in a digital age, such as criminal use of AI, to protect people, institutions and companies against cyber-enabled crimes. It will also continue to harness the opportunities of new technologies for law enforcement, border management and disaster risk reduction, and uphold the ability of the law enforcement to lawfully access and exploit digital evidence, without compromising or weakening privacy safeguards or cybersecurity (where relevant).
- *Supporting the green transition in civil security*. Climate change and environmental degradation are increasingly recognised as threat multipliers. Climate-related extreme events such as floods, droughts and forest fires pose increasing threats to people, nature business and infrastructure. Geological hazards such as earthquakes, volcanic eruptions, and tsunamis are also threats affecting security. As EU Member States and Associated Countries face similar challenges, *including varied and evolving transnational* disasters, Cluster 3 will develop solutions to be applied throughout the EU to keep up to date with

the developments. Cluster 3 will also address environmental crime. It will help understand how to manage borders in case of potential large-scale movements of people, including those caused by environmental stress. It will promote environmental sustainability of security solutions.

A second set of cross-cutting themes respond to challenges more specific to Cluster 3:

- *Ensuring legal and ethical outcomes that are supported by society*. Ethics, respect for the rule of law, fundamental rights, including human rights, privacy and the protection of personal data, as well as responsible research, must be at the heart of security research. Citizens and communities, including women and underrepresented groups, should be engaged, for example in assessing the societal impact of security technologies, to improve the quality of results and to build public trust. Social sciences and humanities (SSH) and social innovation need to be appropriately integrated into security research. The aim is to develop an inclusive set of civilian security solutions that are as minimally intrusive as possible while respecting freedoms, rights and values.
- *Protecting and empowering disadvantaged and vulnerable groups*. A range of groups are disproportionately exposed to violence and threats towards their security. These include, women, LGBTQI+, ethnic and racial minorities, persons with a migrant background, persons with disabilities, persons living with chronic illnesses, and elderly people and children. The vulnerability of these groups is further exacerbated by factors such as insecure supply chains for essential medicines which can be disrupted by disasters or criminal activities. The needs and rights of travellers, migrants, and refugees must be protected and promoted in border management activities. Unfortunately, these groups arealso at a higher risk of falling victim to trafficking in human beings. Research under Cluster 3 needs to consider how these groups can be better protected, including by analysing the structures that foster violence against these groups, developing measures to tackle violence, and promoting inclusive and empowering approaches that prioritise the needs and the rights of disadvantaged and vulnerable groups.
- *Improving market uptake of civil security research solutions*. Despite many success stories of tools and capabilities used by security practitioners originating from EU-funded security research projects, the uptake and deployment of successful research results remains a constant challenge. This challenge spans all destinations.
  This Work Programme:
  - continues the Cluster 3 practice of requiring projects to involve security practitioners alongside researchers and industry. Such involvement has shown its added value in ensuring that tools, technologies and capabilities are developed for the benefit of and use by end-users and practitioners;
  - strengthens this involvement by introducing in many topics a requirement that proposals should plan a mid-term deliverable where practitioners involved in the project assess the project’s mid-term outcomes;
  - innovation procurement is used under the SSRI destination, this year with the open grounds preparatory work for future Pre-Commercial Procurement (PCP) topic, to

bridge the gap between research, innovation and deployment, and thus strengthen the European market and European civil security industrial base;

- encourages synergies with other EU funding programmes and instruments to enable or facilitate the uptake of the results of research into deployable solutions. Further information about this is given below.
- the possibilities and support of security end-users like FRONTEX, EUROPOL, EU-LISA and the EU Drugs Agency, for testing and validation of security research results should be used and expanded to the fullest extent.
- supports projects which can directly or indirectly support public institutions intent on setting up their own innovation processes, which is to be encouraged.
- encourages a competitive and innovative market, accessible for small and medium-sized enterprises (SMEs).

Where relevant, Cluster 3 will make use of space technology and Earth Observation.

A third set of cross-cutting themes address the need for greater simplification and research and innovation funding in support of the EU’s competitiveness:

- *Strengthening European competitiveness*. Growing challenges, such as climate change, artificial intelligence and geopolitical tensions are changing the world we live in. It is therefore paramount that Europe is a place where growth and innovation continue to be fostered. To do so, competitiveness has been placed at the heart of the EU’s economic agenda. The Commission’s work in this area is guided by the Competitiveness Compass and the Draghi report. Cluster 3 will contribute to increasing Europe’s competitiveness through research and innovation projects which contribute to the development of key technologies, reduce dependencies and further strategic autonomy, increase resilience and security, and preserve and secure citizens’ basic right to feel safe.
- *Increased simplification.* In order to simplify applying for funding and taking part in the programme certain measures have been applied, these include topics that are more open and adequately prescriptive, and the application of lump sum funding.

International cooperation

Cluster 3 continues to require a specific approach to international cooperation to achieve the right balance between the benefits of exchange with key international partners, while ensuring the protection of the EU’s security interests and the need for strategic autonomy in critical sectors.

Under the destination ‘Disaster-Resilient Society for Europe’ (DRS), there is an established culture of comprehensive research collaboration with non-EU countries, taking account of the transnational aspect of different natural and human-made hazards and their causes (such as climate change). Therefore, under this destination, international cooperation is strongly encouraged, given the value of international cooperation, especially in developing technologies for first responders.

For the destinations relating to border management, the fight against crime and terrorism, infrastructure resilience and cybersecurity, international cooperation will be explicitly encouraged only where appropriate and specifically supportive of ongoing collaborative activities.

Synergies with other EU funding programmes and instruments

Cluster 3 will continue building and facilitating synergies with other EU funding programmes and instruments, in an approach with long-term capability development planning at its core. This is particularly important for civil security, where solutions are often demand-driven in a market that tends to be narrow, institutional, highly regulated, sensitive, and often fragmented along national lines.

From the demand side (funding for security practitioners and authorities, who are the users of security solutions), Cluster 3 will continue to operationalise the synergies with the home affairs funds: the Internal Security Fund (ISF) and the Integrated Border Management Fund (IBMF) in its two components, the Border Management and Visa Instrument (BMVI) and the Customs Control Equipment Instrument (CCEI). This will mean both facilitating the uptake of the results of Cluster 3 research by Member States and Associated Countries in their national programmes, and programming EU and specific actions with funding dedicated to taking up innovation resulting from Cluster 3 research.

In addition to the home affairs funds, Cluster 3 will continue promoting synergies with the Digital Europe Programme, the European Maritime Fisheries and Aquaculture Fund (EMFAF), the Union Civil Protection Mechanism (Knowledge for Action in Prevention and Preparedness calls for proposals, rescEU grants, early warning capabilities, and the training and exercises programme), the European Regional Development Fund (ERDF), the Cohesion Fund, the Neighbourhood, Development and International Cooperation Instrument – Global Europe instrument for the Southern and Eastern Neighbourhood and the Instrument for Pre-Accession, the Technical Support Instrument (TSI), the OLAF Union Anti-Fraud Programme (UAFP) and EU4Health.

From the supply side (funding for European innovators who develop and commercialise security solutions), the promotion of the uptake of the results of Cluster 3 research could involve the Innovation Fund and, to a lesser extent, EU actions under the ISF and the BMVI, as well as Health Emergency Preparedness and Response HERA Invest and the European Institute of Innovation and Technology (EIT).

Practical ways in which Cluster 3 will continue to improve and promote synergies include raising Member States' and Associated Countries authorities' and innovators' awareness of the opportunities for funding for uptake in other EU programmes and instruments, and tracking and studying uptake of Cluster 3 projects' results in other EU programmes and instruments; planning actions in other EU funding programmes and instruments to fund innovation in civil security that takes up the results of Cluster 3 research.

Research funded under Cluster 3 will continue to focus exclusively on civilian applications. Coordination with the European Defence Fund (EDF) and the EU Space Programme will be sought to strengthen cross-cluster complementarities also with actions foreseen in particular in Horizon Europe Clusters 2 and 4[1].

Role of the Justice and Home Affairs (JHA) agencies

EU JHA agencies and in particular Europol[2], Frontex[3] and eu-LISA[4] take on a particular role in Horizon Europe. They assist the European Commission on relevant research and innovation activities and on specific topics that identify them as desirable to be involved after grants have been awarded.

Proposals should foresee that JHA agencies could observe projects' pilots and demonstrations, with the aim of facilitating future uptake of innovations for the civil security research community.

EU JHA agencies are, however, not eligible to participate in any proposal preparation phase and should not be contacted and no documentation should be sent by applicants/consortium members before grants have been awarded.

Similarly, if the proposals concern drug-related issues, successful projects are expected to engage with the European Union Drugs Agency (EUDA) during the lifetime of the project, including validating the outcomes.

For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding.

Implementation

Proposals under certain topics in this Work Programme should plan their activities opting for the Financial Support to Third Parties (FSTP).

[1] To this end, the Commission and Member States have in place a mechanism for strategic planning and coordination of R&D related to the Copernicus Security Services (CSS), which maps current operational services and on-going and planned R&D initiatives, as well as it identifies end-user operational requirements and promotes sharing of information between projects with common interests. The mechanism drives R&D objectives listed in a Strategic Research Agenda (SRA) updated on a yearly basis. Engagement in the CSS-SRA information sharing process is therefore sought, for those projects planning to use Earth Observation and associated services for civil security applications.

[2] https://www.europol.europa.eu/operations-services-and-innovation/grants/requests-for-europol-participation-in-grants-awarded-other-entities[2]

[3] https://www.frontex.europa.eu/innovation/eu-research/news-and-events/new-eu-funded-border-security-projects-fv5jMw#:~:text=Horizon%20Europe%20is%20the%20framework,Frontex's%20role%20is%20further%20strengthened

[4] https://www.eulisa.europa.eu/

Calls

Call - Civil Security for Society

HORIZON-CL3-2026-01

Overview of this call[5]

Proposals are invited against the following Destinations and topic(s):

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)	Indicative number of projects expected to be funded
		2026		
Opening: Deadline(s):				
Overall indicative budget				

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

[5] 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 2026 and 2027

	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.

Call - Civil Security for Society

HORIZON-CL3-2027-01

Overview of this call[6]

<u>Proposals are invited against the following Destinations and topic(s):</u>

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)	Indicative number of projects expected to be funded
Overall indicative budget				

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.

[6] 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 2026 and 2027

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.

Destinations

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

As underlined in the Horizon Europe strategic plan 2026-2027, "*this Destination will support the Commission's priorities by addressing new, upcoming or unforeseen challenges and/or creative or disruptive solutions for improving the prevention, detection and deterrence of various forms of crime or terrorism/radicalisation through an enhanced understanding of the related societal issues. In doing so, research and innovation projects funded under cluster 3 will contribute to safeguarding, sustaining, and improving the Union's unique quality of life, by improving the Union's ability to prevent, detect, and deter various forms of crime and terrorism, including the different forms of hybrid threats and gender-based violence, in a proportional and human rights-compliant manner. Research under this Destination will contribute to the forthcoming Internal Security Strategy and Counter-Terrorism Agenda*".

This destination will support the implementation of the European Commission political guidelines 2024-2029 for a 'Safer and more secure Europe', a 'Preparedness Union', with 'Stronger Common Borders', protecting democracy and putting research and innovation at the heart of a resilient economy. Overall, research under this Cluster should continue to focus on preserving and securing citizens' basic right to feel safe. This destination will support the European Commission efforts towards:

- a new Counter-Terrorism Agenda to address new and emerging threats, and,
- a united approach to security, centred around a new European Critical Communication System to be used by public authorities in charge of security and safety.

To this end, 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, as well as domestic sexual violence, and gender-based violence, with a particular emphasis on protecting vulnerable populations and victims at increased risk of violence, including those affected by child sexual abuse and juvenile delinquency;
- 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 and elderly people, through a robust prevention, detection, and protection from cybercriminal activities.

More specifically, in the rapidly evolving technological and societal landscape, with climate change and environmental aspects increasingly seen as security issues, and with growing threats to vulnerable citizens, various forthcoming challenges that European society faces deserve dedicated research and innovation actions in the scope of this Destination. Some of them are:

- Challenges regarding prevention, detection and deterrence of various forms of crime and terrorism through an enhanced understanding of the related societal issues, such as
  - tackling the nexus between disinformation, hate speech and radicalisation,
  - countering gender-based violence, or
  - fighting violence-as-a-service.
- Challenges related to counterterrorism, protection of public spaces, such as
  - improving detection of remote explosives and explosives in closed spaces and urban environments, or
  - use and countering of unmanned systems, including neutralisation of commercial drone attacks.

Research and innovation funded under this Destination will contribute to policy objectives such as those of the:

- Police cooperation package[7] (information exchange[8], automated data exchange for police cooperation - "Prüm II"[9], operational cross-border police cooperation[10]);
- Counter-Terrorism Agenda for the EU[11] (incl. Regulation 2021/784/EU on addressing dissemination of terrorist content online & Directive 2017/541/EU on combating terrorism);
- EU C-UAS Strategy[12] (counter-drone policy);
- EU Strategy to Tackle Organised crime[13];
- EU Strategy on combatting Trafficking in Human Beings[14] (the modified Directive on preventing and combating trafficking in human being and protecting its victims), and the Proposal to strengthen EU legislation to prevent and fight migrant smuggling[15] (notably its aspect of reinforcing Europol's role in the fight against migrant smuggling and trafficking in human beings);

[7] COM/2021/782 final, COM/2021/784 final, ST/8720/2022/INIT.
[8] Directive (EU) 2023/977.
[9] Regulation (EU) 2024/982.
[10] Council Recommendation (EU) 2022/915.
[11] COM/2020/795 final.
[12] COM/2023/659 final.COM/2023/659 final.
[13] COM/2021/170 final.
[14] COM/2021/171 final; Directive (EU) 2024/1712; COM/2023/755 final.
[15] COM/2023/754 final.

- EU drugs measures (Strategy[16], Action Plan[17] and Roadmap to fight Drugs Trafficking and Organised Crime[18]);
- EU environmental crime measures[19] (review of the Directive 2008/99/EC on protection of the environment through criminal law);
- EU anti-corruption measures (Communication[20], proposal for a Directive[21]);
- Directive (EU) 2019/713 on non-cash means of payment;
- EU strategy on a more effective fight against child sexual abuse[22] (incl. Proposal for a regulation to prevent and combat child sexual abuse[23]);
- EU Regulation (2022/2371) on serious cross-border threats to health;
- Directive (EU) 2024/1385 on combating violence against women and domestic violence.

This Destination will also support, whenever appropriate and applicable, proposals with:

- a clear strategy on how they will adapt to the fast-evolving environment in the area of fight against crime and terrorism (evolution of related technologies, evolution of criminal modi operandi and business models related to these technologies, etc.);
- the involvement of Police Authorities in their core;
- the active role for Non-Governmental Organisations (NGOs) and Civil Society Organisations (CSOs);
- the active involvement of Small and Medium Enterprises (SMEs);
- a minimum-needed platform, i.e., tools that are modular and can be easily plugged into another platform (in order to avoid platform multiplication);
- tools that are developed and validated against practitioners’ needs and requirements;
- tools following existing or new standards for data exchange, including cybersecurity best-practices;
- a robust plan on how they will build on the relevant predecessor projects;
- education and training aspects, especially for Police Authorities and other relevant practitioners, as well as information sharing and citizen awareness raising;
- a clear strategy on the uptake and sustainability of the project results, with special attention to the access at little or no cost to created tools and methodologies by Police Authorities involved in the project;
- a well-developed plan both on how research data for training and testing will be obtained, in order to reach the requested Technology Readiness Levels (TRLs), and on how the specific TRL will be measured.

[16] 14178/20.
[17] ST/9819/2021/INIT.
[18] COM/2023/641 final.
[19] Directive (EU) 2024/1203.
[20] JOIN(2023) 12 final.
[21] COM/2023/234 final.
[22] COM/2020/607 final.
[23] COM/2022/209 final.

For Police Authorities' training-related aspects, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, in coordination with the Community for European Research and Innovation for Security (CERIS)[24].

Proposals are invited against the following topic(s):

HORIZON-CL3-2026-01-FCT-01: Impact of climate change on law enforcement

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities [25] from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).

[24] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

[25] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

Technology Readiness Level	Activities are expected to achieve TRL5-6 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- European Police Authorities are equipped with specialised skills and technologies to counter an increase in illegal activities related to the climate change and the emergence of new (opportunistic) criminal patterns;

- the functioning of European Police Authorities is adapted to the climate-changing environment;

- improved understanding by policy makers of the effects of climate change on law enforcement with a view of developing related effective European policies.

Scope: Global climate change is a megatrend expected to affect our societies over the next decade. As stated in[26], “We are already living in the climate crisis. This brings substantial security risks at global and national levels. (...) Anyone thinking about security needs to think about climate as well”. As also discussed in[27][28], e.g., climate change will affect European law enforcement in various ways, notably in the following two aspects.

Firstly, it is likely to create new opportunities and resources for organised crime, challenging current security frameworks. One of the expected outcomes of climate change will be the emergence of scarcity markets[7]. Criminal networks will aim to dominate these markets, increasing their role in the distribution of essential goods and services such as food and water. In addition, criminal networks will facilitate the movement of migrants, including women and children, escaping conflict and the effects of climate change. In this landscape, the adoption of new technologies will bolster criminal organizations of various kinds. Examples of crimes, illegal activities, threats and harms connected to climate change include: environmental crimes contributing to climate change (illegal mining and extraction, illegal deforestation, wildlife trafficking and poaching), fraud and financial crimes (greenwashing, carbon credit

[26] “Germany: National interdisciplinary climate risk assessment”: https://metis.unibw.de/assets/pdf/National_Interdisciplinary_Climate_Risk_Assessment.pdf

[27] A.Matczak, S.I. Bergh, A review of the (potential) implications of climate change for policing practice worldwide. Policing: A Journal of Policy and Practice, Vol. 17, 2023, https://doi.org/10.1093/police/paad062

[28] P. Schwartzstein (2024). Climate Change & Crime: A big, bad, largely overlooked nexus. The Council on Strategic Risks. https://councilonstrategicrisks.org/2024/10/17/climate-change-crime-a-big-bad-largely-overlooked-nexus/

fraud, misuse of climate funds), exploiting climate change-related disasters (water theft, looting after disasters, land grabbing), or social tensions (new forms of radicalisation and terrorism, violence against environmental defenders, increased displacement and migration challenging public order). While many of these criminal activities are not entirely new, their association with and amplification by climate change presents unique challenges that require thorough investigation and analysis. Recognizing these emerging trends is vital for formulating effective plans and policies, and equipping law enforcement with specialized skills, technology (including forensics) and training necessary to tackle these challenges in an increasingly volatile world.

Secondly, Police Authorities need to adapt their functioning in the climate-changing environment. It is necessary to secure their business continuity that may be jeopardized by, e.g., severe and extreme weather conditions affecting equipment and infrastructure, rise of maintenance and operational costs, or prolonged periods of services and logistics disruption. Deteriorated communication networks and rendering certain areas inaccessible or hazardous may, in consequence, turn such areas into hubs for illicit activities, requiring new capabilities, remote monitoring, specialised equipment or preparedness strategies. Police Authorities must continue their work also in case of disrupted transportation and communication. Namely, roads, power grids, and mobile networks fail during extreme weather events, slowing emergency responses, public order restoring and investigations. Alternative and easily deployable solutions to counter the impact and allow Police Authorities to respond to the challenges are needed.

In this topic, proposals are expected to address either one or both aspects. In addition to the mandatory participation of Police Authorities in the consortia, active involvement of other security practitioners, such as Border Guard or Customs Authorities, is encouraged. Technological and societal angles should be addressed in a balanced way.

Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Proposals funded under this topic are expected to provide ideas on how they would engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. For Police Authorities' training-related aspects, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

HORIZON-CL3-2026-01-FCT-02: Open topic on preventing and countering the misuse of emerging technologies for criminal purposes, including issues related to lawful access to data

Call: Civil Security for Society

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[29] from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **all** of the following expected outcomes:

- European Police Authorities are empowered with modern, accessible and validated tools, methodologies and training curricula to anticipate and cope with the misuse of new and emerging technologies for criminal purposes, with the aim to facilitate prevention,

[29] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

detection, efficient data access and investigation of criminal offences in a lawful manner and with full respect of fundamental rights;

- Reinforced interdisciplinary collaboration at the European level through the establishment of partnerships among technologists, policy makers and Police Authorities, resulting in a holistic understanding of the challenges posed by emerging technologies and in sharing of best practices;
- Clear guidelines and frameworks are created, including on procedures and rules, that ensure lawful access to data, balancing the needs of security with respect for privacy, and that foster a European approach to the related challenges for the police and the judiciary.

Scope: New and emerging technologies (e.g., new communication technologies, quantum technologies, new biometrics and identification technologies, cloud computing technologies, etc.) bring many benefits but also pose a number of new challenges for the police and the judiciary. Therefore, there is a strong need to adequately tackle challenges for Police Authorities stemming from all these new and emerging developments as well as to make sure that the lawful access to data keeps track with these evolutions, respecting applicable legislation and fundamental rights such as personal data protection and privacy.

Under the Open topic, proposals are welcome to address new and emerging technologies that are not covered by the other topics of the previous Horizon Europe Calls Fighting Crime and Terrorism, as well as of the current Call Fighting Crime and Terrorism 2026-2027. Proposals should emphasize adaptive methodologies and frameworks that can evolve in response to new threats and challenges, empowering Police Authorities to act effectively while ensuring adherence to legal standards regarding data access. Thus, research activities proposed within this topic should, in a balanced way, 1) develop modern tools, methodologies and training material for police to tackle the problem of misuse for criminal purposes of the new and emerging technologies under consideration, and 2) address issues related to lawful access to data in this context. In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content is not a mandatory requirement. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Proposals funded under this topic are expected to provide ideas on how they would engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. Similarly, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. For Police Authorities' training-related aspects, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

HORIZON-CL3-2026-01-FCT-03: Missing persons: prevention and investigation

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[30] and at least 2 Civil Society Organisations (or Non-Governmental Organisations) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table “Information about security practitioners” in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU

[30] In the context of this Destination, ‘Police Authorities’ means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

	classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved skills, tools and training curricula for European Police Authorities and Civil Society Organisations (or Non-Governmental Organisations) to work with vulnerable groups in the context of prevention of missing persons, which take into account European multicultural dimension, as well as legal and ethical rules of operation;
- enhanced investigation tools and methodologies for European Police Authorities to tackle cold cases in the context of missing persons, based on modern forensics and criminology;
- modern training curricula for Police Authorities, their improved cross-border cooperation and enhanced tools and methodologies to tackle new cases of missing persons;
- enriched European common approaches applied by Police Authorities to fight the issue of missing persons relying on the synergy of technology, the latest socio-psychological knowledge learned from cases, as well as field experience of Police Authorities and entities dealing with victims, while fully respecting fundamental rights such as privacy, protection of personal data and anonymity of victims.

Scope: The issue of missing persons is a multifaceted challenge that encompasses diverse categories and is influenced by various factors. People may go missing under a variety of circumstances, such as voluntary disappearances, abductions, cases related to mental health crises, or because of conflict, migration, geopolitical instability, natural disasters. Vulnerable groups - notably children, victims of trafficking and exploitation, and persons suffering from cognitive impairments - face an even greater risk of going missing, often under distressing and dangerous conditions. Tackling this issue requires a coordinated response from multiple stakeholders, from Police Authorities via Civil Society Organisations (CSOs) or Non-Governmental Organisations (NGOs) to the involvement of the overall society.

In an era of rapid technological advancement and societal developments, there is a pressing need to improve current European approaches to fight the issue of missing persons (prevention and/or investigation of cold and new cases) using innovative societal and technological solutions. To this end, modernised skills, training curricula and methodologies for Police Authorities, CSOs and NGOs to work with vulnerable people and children are needed, such as effective awareness raising campaigns that take into account European multicultural dimension. When it comes to investigation, Police Authorities need efficient tools that benefit from new technologies to solve cold cases while combining modern forensic science (including biometrics and digital forensics) and criminology, e.g., modern tools for using an old DNA, or accurate facial ageing, among others. Furthermore, for new cases of missing persons, apart from an improved cross-border cooperation, Police Authorities also need, on the one hand, a modernised training to face such situations more efficiently, improving the dialogues and interactions with families, and on the other hand, modern forensic tools for, for example, fast and reliable cross-matching of DNA samples between new and cold cases.

If a proposal concerns forensics, its consortium should involve forensic institutes as well. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Proposals funded under this topic are expected to provide ideas on how they would engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

HORIZON-CL3-2026-01-FCT-04: Crime prevention approaches, online and off-line, tackling the nexus between addictions and crime

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[31] and at least 2 Civil Society Organisations (or Non-Governmental Organisations) from at least 3 different EU Member States

[31] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

	or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- improved understanding of links between addictions and crime, including drivers of criminality;
- innovative and effective solutions, including training curricula, for European Police Authorities and relevant Civil Society Organisations (or Non-Governmental Organisations) to prevent addictions and related crimes, with a special attention to young people at risk;
- evidence-based support to modernising European criminal justice system's approach when dealing with addiction-related offenses;
- novel approaches of collaboration between different stakeholders, primarily European Police Authorities and Civil Society Organisations (or Non-Governmental Organisations), to increase communities' addiction resilience, security and safety.

Scope: A close and complex relationship exists between addictions, such as gambling, drug or alcohol use, and crime (e.g., criminals are often under the influence of drugs while committing crimes, gamblers or drug users commit crimes to pay for their debts or drugs). In this topic, successful proposals are expected to analyse the specific nexus between addictions and crime, with the aim of developing related modern methodologies and tools for prevention of not only addictions but also crimes related to them, both offline and online, while respecting the fundamental rights of the communities concerned and using of non-stigmatising language. Novel approaches of collaboration between different community stakeholders, from Police Authorities, civil society, national and local entities, private actors, trained psychologists, are expected to be developed as well, with the aim of increasing communities' addiction resilience, security and safety. An emphasis of the work should be on young people at risk, the criminal justice system, drivers of criminality and pathways from becoming an addict via committing a petty crime to getting involved in organised crime. Activities proposed within this topic should address the issue from various angles, combining both social research with technological development and applications in a logical manner.

Therefore, this topic requires the effective contribution of Social Sciences and Humanities (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 research activities.

Proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on if appropriate and not duplicate previous research. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact.

Furthermore, proposals funded under this topic are expected to provide ideas on how they would engage with the European Union Drugs Agency (EUDA) during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

HORIZON-CL3-2026-01-FCT-05: Countering lone-actor violence

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Actions
Eligibility	The conditions are described in General Annex B. The following

conditions	exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[32] and at least 2 Civil Society Organisations (or Non-Governmental Organisations) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- increased understanding of policy makers and relevant security practitioners of the phenomenon of lone-actor violence towards citizens in the buildings under consideration (in schools, places of worship, public administration or other buildings accessible to the public) in the European context;
- lone-actor attacks to citizens in the buildings under consideration (schools, places of worship, public administration or other buildings accessible to the public) are prevented in Europe by, e.g., detecting and tackling early signs of isolation and radicalisation, as well as the promotion of a secure and inclusive environment;
- European schools, places of worship, public administration or other buildings accessible to the public are provided with state-of-the-art means of ensuring their security;
- cooperation between European Police Authorities and relevant staff (in schools, public administration, etc.) is improved.

[32] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

Scope: Citizens in European schools, places of worship, public administration and other buildings accessible to the public increasingly face various forms of lone-actor violence. This topic aims at providing such places with solutions for ensuring civil security (of pupils, school staff, administrative workers, citizens at large) via exploring various societal and technological means of preventing such threats, with full respect of fundamental rights, such as rights to privacy and the protection of personal data. Based on a thorough analysis of the phenomenon under consideration in the European context, proposals should look into methodologies of catching and tackling early signs of isolation and radicalisation, and of addressing them by, e.g., creating appropriate programmes, including by modernising approaches for prevention of lone actor attacks. Means for raising awareness (possibly training) of the relevant staff (school staff, employees in public administration, etc., in function of the building under consideration) regarding existing risks and for keeping them up to date on security matters should be tackled as well. Ways of improving cooperation between the relevant staff and Police Authorities in this context should be analysed too. Proposed solutions should be affordable to public schools and other structures accessible to the public that are usually more limited in funding. Proposals are invited from consortia involving Police Authorities and other relevant security practitioners, Civil Society Organisations, Non-Governmental Organisations, and the appropriate balance of IT specialists, psychologists, sociologists, etc. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Activities proposed within this topic should address the issue from various angles, combining both social research with technological development and applications in a logical manner.

Therefore, 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 research activities. In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on outcomes developed by EU-funded projects, such as the ones under HORIZON-CL3-2024-FCT-01-04, and not duplicate previous research. If the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

HORIZON-CL3-2026-01-FCT-06: Prevention and mitigation of misuse of synthetic biology for bioterrorism purposes

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 4-5 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **all** of the following expected outcomes:

- increased understanding of European policy makers, research community and relevant security practitioners of the threat of bioterrorism and of synthetic biology, including a thorough analysis of what needs to be monitored in this context, what needs to be regulated and how;

- awareness raised within the community that research in synthetic biology can be used for malicious purposes.

Scope: The rising threat of bioterrorism is driven by recent scientific advancements, notably by growing accessibility of synthetic biology, genetic engineering, related commercial services and public databases, which in turn enhance their obtainability to non-state actors and individuals with malicious intentions. The proliferation of do-it-yourself biohacking and community laboratories, including gene editing and sequencing technology, dropping costs of equipment and increased simplicity of use may inadvertently facilitate knowledge and skills dissemination about biological threats and open new pathways for bioterrorism. Challenges in detection, particularly the lengthy incubation periods of biological agents, underscore the urgent need for improved identification technologies to allow for timely intervention and reduce potential mass casualties. Given that properly weaponized biological agents can be more lethal than nuclear weapons, their cross-border implications warrant focused attention. Recent incidents involving biotoxins across various European countries illustrate the feasibility of biological attacks. The increasing weaponisation of drones highlights an alarming trend that could extend to biological agents, further complicating threat landscapes. The potential economic and social consequences of biological attacks necessitate robust prevention and preparedness measures to mitigate overwhelming impacts on healthcare systems and society at large. Finally, there is a growing risk of hybrid threats from hostile states or extremist groups exploiting biotechnology for covert operations.

Proposals are expected to address the emerging threats of bioterrorism in Europe, particularly in the context of synthetic biology. Recognising bioterrorism as a low-probability but high-impact event, consortia should review current and future risks, flag areas requiring reinforced monitoring, as well as identify missing regulatory frameworks necessary for ensuring public security and safety. Furthermore, proposals should bring together diverse consortia to enhance our understanding and response to bioterrorism and create a comprehensive approach to this pressing issue.

Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content is not a mandatory requirement. Proposals funded under this topic are expected to provide ideas on how they would engage with the Europol Innovation Lab during the lifetime of the project. Similarly, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

HORIZON-CL3-2027-01-FCT-01: Open topic on online harms detection & investigation tools using a short development cycle model

Call: Civil Security for Society	
Specific conditions	
Expected EU	The Commission estimates that an EU contribution of around EUR …

contribution per project	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 … million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[33] from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

<u>Expected Outcome</u>: Project results are expected to contribute to **all** of the following expected outcomes:

- European Police Authorities benefit from a rapid deployment of targeted detection and investigation tools and related training materials, specifically tailored to counter current, foreseeable and emerging online harms at the outset of each development cycle;

[33] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

- European Police Authorities are provided with a flexible framework for adaptation via creation of a modular toolset that allows for the incorporation of new functionalities and updates based on the latest trends and threats in online harms;
- enhanced European stakeholder collaboration through facilitation of partnerships among researchers, policy makers, and Police Authorities to ensure that tools are not only effective but also user-friendly, legally and ethically sound.

Scope: As the digital landscape continues to evolve, so too do the myriads of online harms that threaten citizens' security and well-being. To address these challenges, we invite proposals for the development of detection and investigation tools that employ short development cycle models. This approach emphasizes agility and responsiveness, ensuring that tools can quickly adapt to emerging online threats, such as identity theft, disinformation, deepfakes, spoofing, digital violence, or, e.g., tools for an early detection as well as real-time monitoring and risk assessment that can identify potential fraudulent sales before they occur.

This topic welcomes innovative ideas focused on creating efficient detection and investigation tools to combat varying forms of online harms, which should be selected at the beginning of every new development cycle, in agreement with all stakeholders involved in the consortia, especially including concrete needs of Police Authorities. The emphasis on short development cycles allows proposals to remain dynamic, responsive to the fast-paced nature of online threats, and capable of addressing both established issues and new challenges as they arise. Proposals should focus on the iterative process of tool development, integrating feedback from Police Authorities to ensure continuous improvement and relevance in combating online harms. Ultimately, the goal is to foster a proactive and effective response to safeguarding online spaces for all users, regardless of their gender identity or expression.

Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Proposals funded under this topic are expected to provide ideas on how they would engage with the Europol Innovation Lab during the lifetime of the project. Furthermore, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

HORIZON-CL3-2027-01-FCT-02: Community policing in diverse societies in Europe

Call: Civil Security for Society

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[34] and at least 2 Civil Society Organisations (or Non-Governmental Organisations) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **all** of the following expected outcomes:

- new tools, skills and methodologies for Police Authorities to deal efficiently with diverse communities as well as with diversity among police personnel are identified, developed

[34] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

and disseminated throughout Europe, leading to, among others, an increased trust to Police Authorities in general;

- modern and effective training curricula for European Police Authorities are developed on community policing in diverse societies, including post-conflict zones, and addressing the needs of individuals from various ethnic and religious backgrounds, as well as marginalized groups such as migrants, LGBTQ+ individuals, or returnees from war.

Scope: This topic addresses challenges of community policing in increasingly diverse and sometimes also fragile societies, including the integration of returnees from conflict zones, migrants, as well as marginalized communities such as LGBTQ+ individuals and various ethnic and religious groups.

Encompassing a post-conflict dimension too, particularly in the context of Ukraine, this topic aims to foster inclusive community policing practices that can adapt to the complexities of diverse societal dynamics. Proposals should explore innovative and inclusive approaches in police education, training and management that go beyond traditional models, resulting in an effective engagement with a diversifying society. Proposals should also seek to identify and develop effective practices and training programs that encourage a deeper understanding of diversity among police personnel. In addition, proposals should assess how effective cooperation with Civil Society Organizations (or Non-Governmental Organisations) - representing various communities - can enhance reporting mechanisms, reduce hate crimes, and strengthen trust and cooperation between the police and the population. By improving police-citizen relations across diverse European contexts, the proposals should aim to contribute to enhanced security and social stability in Europe. Proposals' findings should generate valuable insights applicable to varied policing environments, ultimately informing police forces across Europe about non-violent conflict resolution and constructive engagement strategies. Through collaborative research and training, proposals should equip Police Authorities with the tools, skills and methodologies necessary to effectively serve and engage with diverse communities, foster social cohesion, and build trust throughout Europe.

Activities proposed within this topic should address the issue from various angles, combining social sciences with technological development and applications in a logical manner.

Therefore, 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 research activities.

Proposals should outline the plans to develop possible future uptake and upscaling at national and EU level for possible next steps once the project is finalised. Proposals should also consider, build on if appropriate and not duplicate previous research. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Furthermore, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

HORIZON-CL3-2027-01-FCT-03: Open topic on enhanced prevention, detection and deterrence of societal issues related to various forms of crime

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[35] and at least 2 Civil Society Organisations, CSOs (or Non-Governmental Organisations, NGOs) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).

[35] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

Technology Readiness Level	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Beneficiaries must provide financial support to third parties in the form of grants. The maximum amount to be granted to each third party is EUR 60 000 to support effective collaboration and/or coordination with additional relevant national Police Authorities and/or CSOs/NGOs from EU Member States or Associated Countries.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- improved, modern, uniform and validated tools, skills or methodologies as well as innovative training curricula for security practitioners (European Police Authorities, Non-Governmental Organisations, Civil Society Organisations) to prevent, detect and deter criminal or terrorist offences under consideration, taking into account all applicable legislation and fundamental rights;
- enhanced understanding of the cultural and societal aspects of crime or terrorism/radicalisation offences under consideration as well as on the key challenges related to combating them;
- evidence-based support to policymakers on shaping and tuning of regulation related to crime or terrorism/radicalisation offences under consideration;
- enhanced perception by citizens that Europe is an area of freedom, justice, security and respect of privacy and human rights, thanks to, e.g., innovative awareness-raising campaigns explaining to citizens the key and evolving mechanisms of crime or terrorism/radicalisation offences under consideration, and how to protect against them.

Scope: Under the Open Topic, proposals are welcome to address both existing and upcoming challenges in fighting crimes that are deeply rooted in cultural and/or societal factors that are not covered by the other topics of Horizon Europe Calls Fighting Crime and Terrorism 2021-2022, Fighting Crime and Terrorism 2023-2024 and Fighting Crime and Terrorism 2025 and Fighting Crime and Terrorism 2026-2027.

Adapted to the nature, scope and type of proposed activities, proposals should convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. Proposals should also delineate the plans to develop possible future uptake and upscaling at national and EU level for possible next steps after the research project completion. If applicable, research proposals should consider building on previous research, including but not limited to, research stemming from Horizon Framework Programmes.

The proposals funded under this topic that concern issues which are within the mandate of Europol[36] are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. Similarly, if the proposals concern drug-related issues, they are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from applying for funding. If the funded proposal concerns radicalisation, the consortium is encouraged to liaise with the EU Knowledge Hub on prevention of radicalisation with the aim of facilitating the streamlining of their priorities and the dissemination of their results.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Proposals should plan their activities opting for the Financial Support to Third Parties in order to provide financial support to practitioners (Police Authorities and/or Non-Governmental Organisations/Civil Society Organisations) for expanding the proposed work in terms of additional user groups, complementary assessments, technology- or methodology-testing activities. From 5% up to 20% of the EU funding requested by the proposal may be allocated to the purpose of financial support to third parties. Proposals must clearly describe the objectives and the expected results to be obtained, including the elements listed in the application template. Proposals are also expected to describe the methods and processes relevant to comply with the general eligibility conditions for financial support to third parties set out in General Annex B and to demonstrate effectiveness (impact).

To ensure the active involvement of and timely feedback from relevant security practitioners, i.e., Police Authorities and Non-Governmental Organisations / Civil Society Organisations, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Activities proposed within this topic should address, in a balanced way, both technological and societal dimensions of the issue under consideration. 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.

[36] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0794 (Annex I)

HORIZON-CL3-2027-01-FCT-04: Open topic on increasing security of citizens against terrorism, including in public spaces

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities[37] from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

[37] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- enhanced ability of European Police Authorities and other relevant security practitioners to identify and prevent emergent challenges in the terrorism-related issue under consideration;
- harmonised and modern tools as well as procedures for European Police Authorities and other relevant security practitioners to counter the terrorism-related problem under consideration, in full compliance with applicable legislation on protection of personal data and protection of fundamental rights;
- improved cooperation between European Police Authorities and other relevant security practitioners, as well as with international actors, in tackling the problem in question;
- training curricula for European Police Authorities and other relevant security practitioners are developed for an improved countering of the terrorism-related problem under consideration.

Scope: Under the Open Topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for increasing security of European citizens against terrorism, including in public spaces, that are not covered by the other topics of Horizon Europe Calls Fighting Crime and Terrorism 2021-2022, Fighting Crime and Terrorism 2023-2024, Fighting Crime and Terrorism 2025 and Fighting Crime and Terrorism 2026-2027.

Adapted to the nature, scope and type of proposed projects, proposals should convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Proposals should also delineate the plans to develop possible future uptake and upscaling at national and EU level for possible next steps after the research project. Research proposals should consider, build on if appropriate and not duplicate previous research, including but not limited to research by other Framework Programmes' projects. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. The proposals funded under this topic that concern issues which are within the mandate of Europol[38] are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. For aspects of training of Police Authorities, cooperation of successful proposals with CEPOL is expected, provided that the Agency opts out from

[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0794 (Annex I)

applying for funding. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

HORIZON-CL3-2027-01-FCT-05: Effective and evidence-based responses to the increased availability and use of synthetic drugs and stimulants in Europe

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[39] and at least 2 Civil Society Organisations (or Non-Governmental Organisations) from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology	Activities are expected to achieve TRL 6-7 by the end of the project – see

[39] In the context of this Destination, 'Police Authorities' means public authorities explicitly designated by national law, or other entities legally mandated by the competent national authority, for the prevention, detection and/or investigation of terrorist offences or other criminal offences, specifically excluding police academies, forensic institutes, training facilities as well as border and customs authorities.

Readiness Level	General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **all** of the following expected outcomes:

- evidence base is improved for effective prevention, treatment and harm reduction of synthetic drugs and stimulants in Europe;

- relevant European security practitioners, notably Police Authorities, Civil Society Organisations and Non-Governmental Organisations, are equipped with skills, tools and technology aimed at reducing the violence and offending associated with use and marketing of these substances, as well as at combatting drug trafficking from its origin to destination (i.e., through the entire supply chain);

- increased understanding of relevant European security practitioners and policy makers regarding the influence of external drivers of change of societal, technological, legal, economic and ethical nature to the availability and use of different types of synthetic drugs and drug markets~~.~~

Scope: This topic asks for proposals that seek to develop effective and evidence-based responses to the growing prevalence of synthetic drugs and stimulants, such as cocaine and crack cocaine, within the EU. As these substances increasingly influence the drug landscape, the urgent need for enhanced understanding and strategies in their prevention, treatment, and harm reduction has never been clearer. Key focus areas include:

- Evidence-based approaches, strengthening the evidence base to inform effective prevention strategies, treatment modalities, and harm reduction practices targeted at synthetic drugs and stimulants. This includes identifying best practices in current interventions and evaluating their efficacy.
- Reducing violence and offending, exploring strategies to mitigate the violence and criminal behaviour associated with the use and marketing of synthetic drugs. This involves understanding the socio-economic and cultural factors that contribute to these phenomena and proposing targeted interventions.
- Improving technologies and tools to combat drug trafficking from its origin to destination (i.e., through the entire supply chain).
- External drivers of change, analysing the impact of geopolitical situations, legal frameworks, and societal factors on the availability and consumption of various drugs, and addressing how international crises affect organised crime and drug markets in the EU. This includes investigating the repercussions of global developments on local drug dynamics and identifying adaptive response strategies.

In light of the underdeveloped evidence base surrounding synthetic drugs, proposals should aim to foster collaboration among researchers, policymakers, and security practitioners to create a comprehensive and effective response to this pressing issue in Europe. previous research, including but not limited to research by other Framework Programmes' projects. Coordination among the successful proposals from this topic should be envisaged to avoid duplication and to exploit complementarities as well as opportunities for increased impact. To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project. Activities proposed within this topic should address, in a balanced way, both technological and societal dimensions of the issue under consideration. The proposals funded under this topic are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community. Similarly, the proposals funded under this topic are expected to engage with the EU Drugs Agency during the lifetime of the project, including validating the outcomes. Finally, proposals are expected to address all applicable considerations expressed in the Introduction of the Fighting Crime and Terrorism Destination.

Destination - Effective management of EU external borders

Proposals submitted under this Destination should contribute to the expected impact of the Horizon Europe strategic plan 2025-2027: “facilitating legitimate movement of passengers and goods into the EU, while preventing illicit acts”.

This Destination will support the implementation of the European Commission Political Guidelines 2024-2029, with research and innovation for future border management contributing to resilience and competitiveness. This includes investing in the update and development of future European digital and integrated border management that respects and promotes EU values. This will contribute to equip European border, coast guards and customs authorities with the future European state-of-the-art solutions, as well as to the preparedness and capabilities to manage future challenges across the EU external borders, including potential instrumentalisation of migration, hybrid attacks, migrant smuggling, and trafficking linked to transnational terrorism and/or organised crime.

Research and innovation under this Destination will focus on preserving and securing the basic right to feel secure and on protecting and promoting fundamental rights as a priority for both European citizens and third country nationals. It will do so by funding projects which will study, develop and test possible future solutions that both strengthen, and make safer, European borders.

Projects funded under this Destination will promote technological and social research and innovation and further explore and develop solutions that enhance the technological sovereignty of European authorities, in the areas of border management, customs and supply chain security, and civilian aviation and maritime security.

Research and innovation funded under this Destination will contribute to policy objectives such as:

- the Multiannual Strategic Policy for European Integrated Border Management[40];
- the implementation of the Capability Roadmap of the European Border and Coast Guard[41] and its updates;
- the proposals to strengthen EU legislation to prevent and fight against migrant smuggling[42];
- the proposals on digitalisation of travel documents and facilitation of travel[43];
- the new European Internal Security Strategy;

[40] COM (2023) 146 final.
[41] FRONTEX MB Decision 16/2024.
[42] COM/2023/754 final; COM/2023/755 final.
[43] COM (2021) 277 final; COM (2024) 670 final.

- the new Counter-Terrorism Agenda;
- the forthcoming EU Preparedness Strategy;
- the EU Port Strategy;
- the civil security aspects of the updated EU Maritime Security Strategy[44] and of the Ocean Pact;
- the EU Cable Security Action Plan[45];
- the new European action plans against drug trafficking and against weapons trafficking;
- the proposals for EU Customs reform[46], including the proposed EU Customs Authority and Data Hub;
- the security aspects of the Comprehensive EU toolbox for safe and sustainable e-commerce[47]
- the security aspects of the Competitiveness Compass for the EU[48].

Research and innovation will contribute to sustain and improve capabilities to cope with potential future critical situations or emerging challenges regarding both the flow of people and the flow of goods across external EU borders. These capabilities may include but not limit to:

- monitoring, preparedness and reaction in border management tasks, managing irregular or illegal activities involving people or goods across external borders of the EU;
- safeguarding and promoting fundamental rights and EU values, and ensuring legal compliance, in efficient border management;
- efficiency, performance, environmental impact and reaction in border management tasks in all geographical and meteorological conditions;
- integrated and continuous border surveillance, situational awareness and analysis support;
- safety, user experience and performance of practitioners' staff in border management;
- security, privacy and usability of identity and (travel) documents and credentials;

[44] JOIN/2023/8 final.

[45] ` JOIN(2025) 9 final

[46] COM (2023) 257 final; COM (2023) 258 final – 2023/0156(COD); COM (2023) 259 final – 2023/0157(NLE); COM (2023) 262 final – 2023/0158(CNS).

[47] COM(2025) 37 final

[48] COM(2025) 30 final

- facilitating travel of bona fide passengers across external borders of the EU;
- prevention, detection and disruption of trafficking of dangerous, illicit and illegal goods and materials through external borders of the EU and the supply chain.

Furthermore, research and innovation under this Destination will contribute to:

- safeguard the technological sovereignty of the EU in critical security areas by contributing to a more competitive and resilient EU security technology and industrial base;
- lower the environmental impact and footprint of border, customs and supply chain security tasks, through innovative solutions and methods;
- integrate and improve safety and cybersecurity of EU information systems, of innovative equipment, and of information and data in these areas, especially during their exchange at operational or tactical levels;
- improve interoperability both among proposed solutions and also with future technological developments in the areas of border management, customs and supply chain security, and civilian maritime and aviation security.

Research projects funded under this Destination should engage with all stakeholders involved, including travellers, migrants, and operators, as relevant.

Projects should align and contribute primarily to the realisation of the Capability Roadmap of the European Border and Coast Guard (EBCG) published by the EBCG Agency (Frontex), especially the Roadmap’s mid- and long-term perspectives. The Roadmap provides strategic vision for investments into the development of capabilities and is the result of integrated planning between the Member States and the European Border and Coast Guard Agency. Proposals submitted under this Destination should explain the alignment primarily with the Capability Roadmap and the plans for further uptake of the research outcomes, especially by involved practitioners in line with their national Capability Development Plans.

Frontex will be closely associated with and will assist Member States and the European Commission in drawing up and implementing relevant research and innovation activities. The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) may also assist the European Commission on relevant research and innovation activities and specific topics.

At the proposal preparation stage, Frontex and/or eu-LISA will not provide guidance on or otherwise be involved in the preparation of project proposals. However, proposals should consider and anticipate that Frontex and/or eu-LISA may observe pilots and demonstrations during project implementation to facilitate the future uptake of innovations within the border and coast guard community.

To accomplish the objectives of this Destination, additional eligibility conditions have been defined regarding the active involvement of relevant security practitioners or end-users in the research projects' consortia.

Cross-community and cross-authority synergies within civil security can be an asset, for example in relation to combat crime and terrorism (across external borders); Disaster-Resilient Society (regarding natural hazards and disasters); Resilient Infrastructure (regarding threats to infrastructures, coming from across borders).

Proposals submitted under this Destination should demonstrate how they plan to build on relevant predecessor projects; to consider the citizens' and societal perspectives; to include education, training and awareness raising for practitioners and citizens; to measure the achieved TRL.

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. Knowledge and technologies developed by research funded under this Destination may be taken up with co-funding of instruments such as the Integrated Border Management Fund, in its components of the Border Management and Visa Instrument (BMVI) and Customs Control Equipment Instrument (CCEI), and/or their subsequent funding instruments. Member States authorities participating in research projects can plan to use those instruments for uptake (piloting, testing, validation, scale-up, transfer, acquire, deploy, etc) of innovative solutions developed from research, as early as TRL 7.

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

Successful proposals under this Destination are invited to cooperate with other EU-led or EU-funded initiatives in the relevant domains, such as the Knowledge Networks for Security Research & Innovation funded under Horizon Europe Cluster 3, or other security research and innovation working groups set-up by the Commission or EU Agencies.

Funded projects are encouraged to liaise with the European Commission's Joint Research Centre (JRC), for example with regards to a possibility of testing the relevant research outputs at the JRC Border Security Lab.

Where possible and relevant, synergy-building and clustering initiatives with projects in the same area should be considered, in coordination with the Community for European Research and Innovation (CERIS)[49].

Cluster 3 will further incentivise the use of European Space Programmes' services for border management innovation where relevant and their services and capabilities, including demonstration and validation of new technologies in operational environments.

[49] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

Proposals are invited against the following topic(s):

HORIZON-CL3-2026-01-BM-01: Advanced border surveillance and situational awareness

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Border or Coast Guard Authorities from at least 2 different EU Member States or Associated countries. For these participants, applicants must fill in the table “Eligibility information about practitioners” in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved border situational awareness, especially in the context of large-scale movements of people across borders, including from potential instrumentalisation of irregular migration, conflicts, social, economic, environmental and climate stress;
- Improved detection, localization, characterization and, when applicable, neutralisation, of unmanned vehicles alone or in swarms, involved in trafficking or smuggling activities across external borders, while complying with legal and ethical guidelines;
- Better safeguard and promotion of fundamental rights thanks to enhanced situational awareness;
- Reliable, redundant detection and reaction capacities without putting staff and society at risk.

Scope: Capabilities for situational awareness and surveillance of land and sea borders need improvement, in consideration of potential future challenges that may require updated capabilities. These may include potential future large-scale movements of people across external borders, resulting from future attempts to instrumentalisation of irregular migration, but also from conflicts, social, economic, environmental and climate stress in the European neighbourhood; as well as increasing availability and capability of unmanned aerial, surface, and underwater vehicles with increased payload capacity and range that make it easier to transport goods and, possibly, persons, including in connection will illicit or illegal activities such as trafficking of goods and smuggling of people across external EU borders. These challenges will be particularly relevant in the Eastern European neighborhood and Eastern external borders.

This may be particularly relevant for unsupervised and difficult-to-control land and sea borders of the Union and the Schengen area.

Research funded under this topic should develop solutions that, through better awareness, improve efficiency and reaction time of detection, search, rescue, and recovery operations near land and sea borders, in diverse geographical and meteorological conditions. Research funded under this topic can also promote cross-border cooperation at European regional level around innovative border management solutions demonstration testbeds.

Projects funded under this topic should develop solutions that go beyond state-of-the-art in clearly demonstrable ways, including measurable improvements in detection range, accuracy, response time, automation, and system resilience.

Improved border surveillance and situational awareness must better safeguard and promote fundamental rights and EU values, with a particular regard to human rights. Solutions should also provide reliable and redundant capacities, while ensuring the safety of staff, users, and persons who may be victim of illicit activities across external borders.

The EBCG Capability Roadmap recognises that future capabilities that help detect cross-border irregularities and cases requiring Search and Rescue activities are essential. Solutions should be modular and scalable to cater to the regional and challenges specificities.

Compatibility and integration with the European Border Surveillance System (EUROSUR) is essential, and compatibility and/or exploitation of other European information-sharing environments, like the Common Information Sharing Environment (CISE), would be an additional asset.

Proposals should demonstrate that the proposed equipment and technologies contribute to cost reduction and energy efficiency of border surveillance and situational awareness operations.

Proposals submitted under this topic are expected to address the priorities of the European Border and Coast Guard (ECBG) and of its Agency (Frontex). This should start from the definition of requirements and the design phase, including alignment with the EBCG Capability Roadmap and on the engagement with the Agency during the project implementation. At the proposal preparation stage, Frontex will not provide guidance on or otherwise be involved in the preparation of project proposals. However, proposals should consider and anticipate that Frontex may observe pilots and demonstrations during project implementation to facilitate the future uptake of innovations within the border and coast guard community.

To ensure active involvement and timely feedback from relevant security practitioners, proposals should include a mid-term deliverable consisting of an assessment of the project's mid-term outcomes, conducted by the practitioners involved in the project.

In this topic, the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the research objectives.

HORIZON-CL3-2026-01-BM-02: Accessible and available travel facilitation

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Action

Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Customs Authorities from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved trusted, secure, and easier automated seamless facilitation for travel, border crossing through border crossing points (BCPs), and/or visa procedures with an integrated approach, minimized risk for bias, and accessible for all travellers minimising digital divides;
- Facilitated solutions with same approach adaptable by all European staff, in all conditions and border control points (BCPs);
- Reduce workload and improve safety, user experience and performance of practitioners' staff involved in border management.

Scope: Facilitation of travel and border crossings at border crossing points (BCPs) across the external EU borders went, and is further going, through developments thanks to updated procedures and regulatory frameworks and to innovative European technologies. From automated border control (ABC) gates to "no-gate" solutions and "seamless travel", and with systems like the Entry-Exit System (EES) and the Electronic Travel and Information Authorisation System (ETIAS), Europe has one of the most advanced, secure and facilitated border check systems in the world.

Travel facilitation schemes are still not as fair, inclusive and accessible as they should be. There are several technical exceptions that for example make difficult for families, people with reduced mobility, or relatively lower digital skills, to smoothly use travel and border crossing facilitation solutions.

On the other hand, both technical systems and procedures may have differences depending on the context or the BCP of application. This may be a limit for the performance and user experience of European integrated border management, especially in a perspective of a larger help to national members of the European Border and Coast Guard (EBCG) from the Standing Corps of the EBCGA.

According to the European Border and Coast Guard (EBCG) Capability Roadmap, legal border crossings should be as swift and simple as possible, preferably fully automated. Border Crossing Points should also have the ability to detect any unauthorised crossings of persons or goods.

Innovation funded under this topic will develop and test solutions for advanced seamless travel and border crossing and/or visa procedures, protecting and promoting fundamental rights, minimising the risk for bias and being accessible for all travellers, with no or minimised limitations depending on age, groups, physical or digital abilities. Solutions should minimise potential for discrimination or physical or digital divide regarding travel facilitation schemes.

Furthermore, solutions should be tested for use with the same approach by all European staff in all conditions and BCPs.

The proposed solutions should include automated decision support systems suggesting to the end-users (border checks operators) which procedure, technology or database can be used without infringing rights of travellers. Solutions should also integrate and, if appropriate, further develop, privacy-preserving biometric matching in encrypted domains, that minimises data shared (for example limiting to matching scores) to improve data protection.

Proposals submitted under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) and of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). This should start from the definition of requirements and the design phase of their work, including basing on the EBCG Capability Roadmap; and on the engagement with the Agencies during the implementation of the project. At the stage of proposal preparation, Frontex and eu-LISA will not provide any guidance on, or otherwise be involved in the preparation of, project proposals. Proposals should consider and foresee that Frontex and eu-LISA may observe pilots and demonstrations when the project will be implemented, with the aim of facilitating future uptake of innovations for the border and coast guard community.

To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project.

HORIZON-CL3-2026-01-BM-03: Reliability of age assessment methods in the context of security and border management

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Coordination and Support Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved protection of minors, including by more reliable age assessments and by minimising the use of intrusive age assessment methods;
- Improved adaptation, preparedness and cooperation of authorities in the fight against human trafficking;

- Expanded European-based knowledge on reliability, accuracy and efficiency of age assessment methods.

Scope: Many unaccompanied children and young persons arriving at the external EU borders and seeking asylum, lack official documents showing their identity and age. Age assessment methods are important as they contribute to the determination of, for example, where an individual will be initially housed and what services, supports, and legal processes they will receive to ensure protection and, of applicable, child protection.

In other cases, minors are victim of trafficking of human beings (THB) criminal activities, either across the EU external borders, or within the EU borders. In other cases again, age assessment methods are necessary for law enforcement investigations on protecting children, forensic investigation, and/or the identification of victims.

No age assessment method can offer a 100% reliability. Different approaches have different sensitivity and specificity, and different sample sizes and representativeness, and some approaches are based on a non-European knowledge base. Furthermore, there is considerable variation in methods of age assessment. Methods may use approaches as diverse as interviews, psychological assessments and other holistic approaches; medical approaches such as X-rays, CT scans, DNA methylation, dental observation, or other analyses; other approaches such as image analysis; and they may use or not artificial intelligence (AI) for data analysis.

EU regulations, and guidelines by EUAA[50], 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. Further studies, reports or documents have also been elaborated by the European Migration Network[51], European networks of security practitioners for innovation, as well as at national level. The project funded by this topic should also consider these, as well as previous research, including but not limited to research by other relevant EU Framework Programmes projects.

This Cooperation and Support Action will not develop methods or technologies of age assessment. Rather, it will analyse and research, including literature review and research with practitioners, the current and potential methods for age assessment. It should assess and compare scientific reliability, sensitivity and specificity of different methods, as well as their potential risks for fundamental rights and how to minimize them.

While the research results would not imply any legislative or policy decision on age assessment methods, the research will develop evidence-based results on options for more (compared to the state-of-the-art) appropriate models of age assessment methods that protect fundamental rights. The results of research funded by this topic will contribute to capabilities

[50] EASO. Age assessment practices in EU+ countries: updated findings (europa.eu) https://euaa.europa.eu/sites/default/files/EASO_Age_assessment_practices_updated.pdf

[51] https://ec.europa.eu/home-affairs/networks/european-migration-network-emn_en

for better identification of children and minors in the migratory, security, border management and other contexts, following the principles of the EU Strategy on the rights of the child[52]. They will also contribute to the exchange of practices among European authorities.

Synergies with other Horizon Europe Cluster 3 Destinations, such as "Better protect the EU and its citizens against Crime and Terrorism" and "Disaster-Resilient Society for Europe", as well as with Destinations of Horizon Europe Cluster 2 "Inclusive Society".

HORIZON-CL3-2027-01-BM-01: Open topic on research and innovation for effective management of EU external borders that promotes fundamental rights and EU values

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Border, Coast Guard or Customs Authorities from at least 2 different EU Member States or Associated countries. For these participants, applicants must fill in the table "Eligibility information about practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology	Activities are expected to achieve TRL … by the end of the project – see

[52] COM(2021) 142 final

Readiness Level	General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved border management solutions that protect and promote fundamental rights of both EU citizens and Third Country Nationals.

Scope: Under this Open topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions within this Destination that are not covered by the other topics, in either Call Border Management 2026 and Call Border Management 2027.

In particular, this topic will fund research projects that explore, develop and test knowledge and technology solutions in the areas of the areas of border surveillance, border checks, customs and supply chain security, and civilian maritime and aviation security border management that protect and promote fundamental rights of both EU citizens and Third Country Nationals, and EU values.

Adapted to the nature, scope, type and target TRL (if applicable) of proposed projects, proposals should convincingly explain how they will plan and/or carry out demonstration, testing and validation of developed tools and solutions. Proposals should be convincing in explaining the methods they intend to use for demonstrating, testing and validating the proposed tools and solutions. Proposals should also delineate the plans to develop possible future follow-up research and development and/or uptake, upscaling and/or application and use at national and EU level as possible next steps after the research project.

Research proposals should consider, build on if appropriate and not duplicate previous research, including but is not limited to research by other Framework Programmes' projects.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

HORIZON-CL3-2027-01-BM-02 Trusted, secure, quality future digital travel credentials

Call: Civil Security for Society

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	…
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

<u>Expected Outcome</u>: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Development, testing and integration of issuance, validation and sharing capabilities for possible future types of Digital Travel Credentials (DTC);
- Integration of innovative, on-the-move, biometrics and biometric acquisition modalities into DTCs;
- Improved secure connectivity and interoperability for DTCs;
- Improved capability of issuance of emergency travel documents and/or emergency DTCs;
- Improved capability to assess quality of biometrics samples included in DTCs

<u>Scope</u>: Issuance, verification and management of digital travel credentials (DTCs) is relevant for border management, immigration and visa management. Furthermore, it could also be

relevant to combat illicit activities such as terrorism, crime or frauds. This topic aims at supporting research and innovation that explore, develop and test enhanced capabilities for securely issuing, verify and manage (including sharing) possible future types of digital travel credentials (DTCs) for travel across the external borders of the EU.

The proposed solutions must be compatible with current, planned or foreseeable EU DTCs formats, and with applicable ICAO schemes, but they should also push forward to possible further types of DTCs ("Type 2" and "Type 3").

Additionally, the funded project should also work on the integration of current and new biometrics, and/or new biometric acquisition modality, in DTCs. This includes but does not limit to biometrics such as fingermark, palmprint, palmmark, rolled fingerprint, contactless fingerphotos, and biometric acquisition modalities such as on-the-move, including those modalities developed by previous projects funded by this Destination of Horizon Europe Cluster 3. The project should develop and/or contribute to reference biometric sample quality assessments standards for these biometric modalities included in the DTCs.

The funded research project(s) can also address the use case of verification, issuance or re-issuance of (emergency) DTCs in cases of emergencies (including evacuations of EU citizens).

Funded research can additionally address the security of breeder documents, which risk to be "weak links" when they are used to obtain genuine, secure travel credentials.

The proposed solutions should include automated decision support systems suggesting to the end-users (border checks operators) which procedure, technology or database can be used without infringing rights of travellers. Solutions should also integrate and, if appropriate, further develop, privacy-preserving biometric matching in encrypted domains, that minimises data shared (for example limiting to matching scores) to improve data protection.

Proposals submitted under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex) and of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). This should start from the definition of requirements and the design phase of their work, including basing on the EBCG Capability Roadmap; and on the engagement with the Agencies during the implementation of the project. At the stage of proposal preparation, Frontex and eu-LISA will not provide any guidance on, or otherwise be involved in the preparation of, project proposals. Proposals should consider and foresee that Frontex and eu-LISA may observe pilots and demonstrations when the project will be implemented, with the aim of facilitating future uptake of innovations for the border and coast guard community.

To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project's mid-term outcomes, performed by the practitioners involved in the project.

HORIZON-CL3-2027-01-BM-03 Detection and characterisation of threats or illegal, illicit goods in cargo

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and innovation action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 Customs Authorities from at least 2 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Legal and financial set-up of the Grant Agreements	Beneficiaries must provide financial support to third parties in the form of grants. The maximum amount to be granted to each third party is EUR 100 000 to support the expected outcomes of the topic and effective collaboration and/or coordination with additional relevant national Customs Authorities, including testing and validation activities within the projects.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Increased security of air, maritime, land, or postal transport, cargo and supply chain;
- Address accidental or intentional explosions, fires, noxious chemicals, material degradation, or autonomous threats in cargo;
- Enhanced capabilities to detect, characterise, track and trace, and seize dangerous, regulated, illicit devices, goods or material;
- Increased mobility of the customs authorities' resources and equipment and improved agility for a faster and more coordinated response;
- Interoperability of customs control equipment and interconnectivity with other systems.

Scope: Today's global economy and high-volume trade flows require much and fast transport to deliver products worldwide. Traders and consumers expect quick and easy transactions, while customs administrations face the challenge of controlling the goods without disrupting their flow. This is exploited by organised crime and terrorist organisations, which take advantage of the large amount of goods to conceal threats or illegal and/or illicit materials in legal commercial cargo, with the aim of causing damage, disruption, or of it illegally crossing borders unnoticed.

Customs authorities must ensure a high level of compliance with both security and revenue objectives: trafficked materials may represent a threat of cross-border terrorist nature; organised crime traffic illegal goods across external borders, often combining physical goods with illicit digital transactions; smuggled materials entering the EU pose safety and security risks for consumers; and undetected smuggled licit materials entering the EU deprives the Member States of the revenue due if the material had been legally traded.

The importance and reliability of air cargo is expected to further increase. Air cargo can represent continuity assurances to cope, at least in the short term and for critical lines, with supply chain and/or distribution crises. Air carriers flying cargo and mail to the EU must ensure it is screened, or that it comes from a secure supply chain, validated according to EU regulations. Nevertheless, the risk for well-concealed materials not being detected during screening, or the risk of concealment during the supply chain is still relevant. In addition, maritime cargo is the most common transport mode in global trade – trade flow disruptions to cargo shipments can have a significant impact on the global economy. The air and maritime cargo context present security challenges as well as high potential consequences of threats, primarily but not limited to explosives and incendiary devices.

Innovation funded under this topic will develop and test solutions for cargo security, relevant to one or more transport modes (maritime, air, postal, road, or rail); and usable at one (or more) crucial point(s) of the supply chain. Innovation can also develop enhanced capabilities for customs to detect illicit, regulated and or/ dangerous goods and transactions, and to be able to effectively characterise them in a timely manner. Improved tracking and tracing capabilities will facilitate the seizing of the materials while contributing to collecting evidence to further support investigations and prosecutions.

Logistical hubs also need to strengthen their capabilities to adapt to changes, like increased trade flows, and customs authorities need to mobilise their available resources among the different BCPs to ensure efficient and fast controls. Faster and more efficient cargo security and detection capabilities are hence needed to effectively protect cargo from loading to delivery, while still ensuring the flow of commerce. The need for better mobility and improved agility for customs is accompanied by the need to deploy scalable solutions, that are interoperable with other systems to facilitate co-sharing of equipment between BCPs and between Member States.

Detection capabilities could target one or more type(s) of dangerous, illicit and/or illegal goods or materials, including: explosive or incendiary devices; illicit drugs and their precursors; illegally traded species, including covered by the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) and considering the European Deforestation Free Products Regulation; contraband; trafficked weapons; chemical, biological, radiological, nuclear and explosive (CBRN-E) material or precursors; F-gases; and/or various modi operandi related to cross-border trafficking, including involving cargo.

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, tracking and tracing systems, distributed ledger technologies, non-intrusive inspection.

Equipment and technologies enabling increased security of 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. 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.

Proposals received under this topic should demonstrate how the project would integrate the perspective for the whole supply chain, from load to delivery. Proposed solutions should be interoperable with the different relevant equipment and systems deployed by the customs authorities, and proposals should demonstrate how their solutions would align with existing interoperability standards (if any). Proposals submitted under this topic are expected to align with the customs reform (if adopted) and the priorities of the EU Customs Authority (if operational) and its Data Hub.

To ensure the active involvement of and timely feedback from relevant security practitioners, proposals should plan a mid-term deliverable consisting in the assessment of the project’s mid-term outcomes, performed by the practitioners involved in the project.

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

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

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

Destination - Resilient Infrastructure

Following the Commission political guidelines 2024-2029 this Destination will support the implementation of the directives on the Resilience of Critical Entities (CER)[53] and on Network and Information Security (NIS2)[54]. Actions will focus on upgrading physical and digital security and resilience of critical entities and their supply chains, including the European strategic autonomy aspect.

Research and innovation investments will continue addressing emerging and existing challenges for critical entities, including hybrid threats. Cross-destination and cross-cluster cooperation will be fostered to better understand the risks, including both the technological, organizational and underpinning societal issues, and to deliver innovative, scalable, long-lasting and effective tools to prevent, detect, and investigate them. These actions will contribute to realising the objectives of the EU Security Union Strategy[55] and Counter-Terrorism Agenda[56] and forthcoming the EU Preparedness Strategy.

Furthermore, this Destination will continue to develop measures to improve the resilience, safety and security of urban and peri-urban areas against deliberate or accidental human actions, preserving citizens’ right to feel safe and have access to essential services, while meeting climate resilience objectives of the EU Adaptation Strategy[57].

Projects funded under this Destination will promote technological and social innovations enhancing the sovereignty of European critical entities, authorities and operators including their respective supply chains. Moreover, submitted proposals should consider current policy developments and meet expectations of the following EU legislation and policy documents, whichever would be relevant to the challenges addressed by the proposal:

- EU Cybersecurity Strategy[58];
- EU Maritime Security Strategy[59];
- EU Aviation Security Strategy[60];
- Europe-wide Climate Risk assessment (EUCRA) and Commission Communication on Managing Climate Risks;
- Joint Framework on Countering Hybrid Threats[61] and the Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats[62];

[53] Directive (EU) 2022/2557.
[54] Directive (EU) 2022/2555.
[55] COM (2020) 605 final.
[56] COM (2020) 795 final.
[57] COM (2021) 82 final.
[58] JOIN (2020) 18 final.
[59] Council of the EU 11205/14 JOIN(2023) 8 final.
[60] REGULATION (EC) No 300/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002
[61] JOIN (2016) 18 final.
[62] JOIN (2018) 16 final.

- EU C-UAS Strategy[63];
- EU Space Strategy for Security and Defence[64];
- EU Disaster Resilience Goals[65];
- EU Action Plan on Cable Security[66].

To this end, these proposals should contribute to the achievement of one or more of the following generic impacts:

- both physical and digital aspects of critical entities security are addressed,
- new and upgraded systems support the interoperability enabling rapid response and recovery from complex security incidents without significant human involvement, and situational awareness and information sharing functionalities are available, especially where emergency responders intervention is required;
- security-by-design and preparedness-by-design are default features of both newly created and upgraded infrastructures;
- urban, peri urban areas are better protected with technological, organisational, and social innovations, and deepened public involvement;
- public awareness of risks and threats to critical infrastructure is considerably raised;

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

It will be important also to take into account how research results can be advanced to deployable solutions after the projects lifetime, utilising validation and capacity-building programmes like the Internal Security Fund, Digital Europe Programme and other.

Where possible and meaningful, synergy-building and clustering initiatives with successful actions in the same, or other relevant areas. should be considered, including the organisation of international events in coordination with the Community for European Research and Innovation for Security (CERIS) [67].

[63] COM (2023) 659 final.
[64] JOIN (2023) 9 final.
[65] (2023/C 56/01); COM (2023) 61 final.
[66] JOIN(2025) 9 final
[67] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

Proposals are invited against the following topic(s):

HORIZON-CL3-2026-01-INFRA-01: Tools to support stress tests of critical infrastructure

Call: HORIZON-CL3-2026-01 Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following additional eligibility conditions apply: This topic requires involvement as beneficiaries of at least 3 relevant practitioners from EU Member States or Associated Countries. Depending on the specific proposal submitted, these practitioners should represent one or several of the following portfolios: • critical infrastructure operator, • national or regional authority responsible for critical infrastructure resilience, • civil protection authority, • law enforcement or private companies providing security for critical infrastructure. For these participants, applicants must fill in the table “Information about security practitioners” in the application form with all requested information. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Critical infrastructure operators and authorities have access to efficient, adaptable, and reliable tools enabling or improving virtual and physical stress tests of their respective assets;
- Critical entities have broader and deeper understanding of their technical and operational vulnerabilities, improving the scenario building and stress tests exercises;
- Systems allowing notification and collaboration under stress conditions are available for relevant stakeholders.
- Critical entities are better equipped for post-incident investigations, including data collection;
- Improved operational procedures including incidents management and training curricula are developed.

Scope: The resilience of critical infrastructure is of paramount importance as disruptions to these systems usually have significant consequences for the economy, public health, or safety. These systems, responsible for providing essential services for modern society, are increasingly complex and interconnected, making them vulnerable to a range of threats, including cyber-attacks, physical attacks, malfunctions, human errors or natural disasters.

Their stress testing is a crucial step in identifying vulnerabilities and improving resilience. The aim of this topic is to support that process with tools and methodologies for stress testing critical infrastructure, in order to find technical and operational vulnerabilities, mark most effective solutions to resolve such problems, gather and analyse data for improved resilience, and while building on the conclusions of previous exercises, deliver more reliable and comprehensive stress testing protocols.

The proposed solutions may among others support simulation and modelling, scenario building, data analytics, including geospatial information, assessment of risks, as well as impact of human factors engineering. Solutions should allow flexible configuration taking into account the evolving nature of threats and hazards. If feasible they should also be adaptable to different sectors and types of critical infrastructure. Moreover, they need to recognise the relevant regulatory frameworks and allow application of the developed tools under the current regime.

Coordination among the successful proposals from this topic and projects funded under HORIZON-CL3-2025-01-INFRA-01: *Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures* and HORIZON-CL3-2025-01-INFRA-02: *Open topic for role of the human factor for resilience of European critical entities*, should be envisaged in order to avoid duplication, share resources and exploit complementarities and opportunities for increased impact.

HORIZON-CL3-2026-01-INFRA-02: Security challenges of the green transition in urban und peri urban areas

Call: HORIZON-CL3-2026-01 Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following additional eligibility conditions apply: This topic requires involvement as beneficiaries of at least 3 relevant practitioners from EU Member States or Associated Countries representing regional or municipal critical infrastructure operator or authority. For these participants, applicants must fill in the table “Information about security practitioners” in the application form with all requested information. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Identification and analysis of potential new hazards related to innovative technologies being deployed in the urban and peri-urban environments;
- Verification of measures countering potential safety and security risks, hazards and challenges arising in areas hosting green technologies;
- Contribution to building awareness and societal acceptance for safe and secure green transition.
- Impacts of incidents involving new and emerging technologies are examined, including environmental risks and their supply chains;
- Authorities and critical infrastructure operators are equipped with efficient strategies and methodologies for safe and secure integration of new and emerging technologies into urban and peri-urban areas.

Scope: Climate change and environmental degradation are an existential threat to the world, and the green transition is a critical component of the EU's strategy to reduce and mitigate their impacts. This approach is also part of the effort to transform Europe into a modern, resource-efficient and competitive economy. However, rapid deployment of new and emerging technologies, such as, but not limited to: green roofs and walls, solar power installations, electric vehicle charging stations, energy storages, smart sensors and surveillance systems, green transportation systems, nature-based construction materials, or specific infrastructure solutions may create new interdependencies including legacy infrastructure, may affect the surroundings just by the accumulation of deployed solutions, or otherwise create new potential risks and hazards of unknown scale and origin.

Any proposal submitted under this topic should investigate the integration of so-called *green technologies* into urban and peri-urban areas to identify and explore any existing or hypothetical physical and cyber risks and vulnerabilities resulting from this phenomenon, including, but not limited to: battery fires, toxic leaks, electric shocks, structural integrity, toxic waste, data privacy, land management disruptions or social and community tensions. The proposed inquiry should also consider the threat of malicious access and misuse of managing systems potentially leading to harm to health, loss of life or economic damage, regardless of whether the intention is criminal, vandalism or a hybrid attack. Conclusions of these activities should inform first responders and authorities and improve their preparedness. Early threat recognition should improve prevention of any major incidents, and in the event of such an accident occurring, should provide strategy, managerial advice or methodologies for addressing them.

Proactive elimination of major safety and security risks stemming from the green transition should allow future proofing for this group of new technologies, as well as building credibility and their common acceptance by the general public, backed by checked facts and evidence-based safety and security policies.

HORIZON-CL3-2027-01-INFRA-01: Enhancing physical protection of critical infrastructures

Call: HORIZON-CL3-2027-01 Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following additional eligibility conditions apply: This topic requires involvement as beneficiaries of at least 3 relevant practitioners from EU Member States or Associated Countries. Depending on the specific proposal submitted, these practitioners should represent one or several of the following portfolios: • critical infrastructure operator, • national or regional authority responsible for critical infrastructure resilience, • civil protection authority, • law enforcement or private companies providing security for critical infrastructure. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all requested information. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 6-7 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Critical infrastructure operators and authorities have improved physical risks and hazards assessment capabilities;
- Perimeter security, access control, surveillance systems and other systems used by or relevant to critical infrastructure operators are capable of coping with threats from misuse of new and emerging technologies;
- Improved operational procedures, including incidents management and training curricula, are developed.
- Innovative solutions for critical infrastructure resilience are being developed, utilising recent advancements in spatial planning, security-by-design, preparedness-by-design and nature based elements;

Scope: Physical protection of critical infrastructure should keep up its advancement to match risks and hazards stemming from malicious use of new and emerging technologies, and evolving operational environment, as well as improve its safety and security measures against traditional threats. Following this approach entities providing essential services should reduce their vulnerability, among others, to threats from improvised explosive devices, ramming attacks, sabotage, uncooperative and hostile unmanned platforms including swarm robotics, penetration of access points by unauthorised individuals and vehicles, unauthorised access to hazardous material storage, removal of critical components, or deterioration of critical infrastructure due to age, inadequate design or changed operational conditions, including climate.

Proposals submitted under this topic should identify and analyse possible new challenges for the physical security of the critical entities and develop adequate tools, recommendations, manuals and training programmes for relevant operators and authorities.

Coordination among the successful proposals from this topic and projects funded under HORIZON-CL3-2025-01-INFRA-01: *Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures* and HORIZON-CL3-2025-01-INFRA-02: *Open topic for role of the human factor for resilience of European critical entities*, should be envisaged in order to avoid duplication, share resources and exploit complementarities and opportunities for increased impact.

HORIZON-CL3-2027-01-INFRA-02: Impact of malicious use of Open-Source Intelligence on critical infrastructure business continuity

Call: HORIZON-CL3-2027-01 Civil Security for Society	
Specific conditions	
Expected EU contribution per	The Commission estimates that an EU contribution of around EUR … million would allow these outcomes to be addressed appropriately.

project	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 … million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following additional eligibility conditions apply: This topic requires involvement as beneficiaries of at least 3 relevant practitioners from EU Member States or Associated Countries. Depending on the specific proposal submitted, these practitioners should represent one or several of the following portfolios: • critical infrastructure operator, • national or regional authority responsible for critical infrastructure resilience, • law enforcement or private companies providing security for critical infrastructure. For these participants, applicants must fill in the table “Information about security practitioners” in the application form with all requested information.
Technology Readiness Level	Activities are expected to achieve TRL 8 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Critical infrastructure operators and authorities have improved awareness of Open-Source Intelligence (OSINT) and their potential impact on security of their operations.
- Toolbox for OSINT mapping, including enhanced analysis and risk flagging is developed and available to relevant stakeholders.
- Critical infrastructure operators and authorities have improved incident response, emergency plans and business continuity models.
- Potentially harmful OSINT is being effectively removed from the public domain, hampering preparations and attempts of attacks against CI, including the lone wolf and hybrid attack scenarios.

- Awareness campaigns and training curricula for critical entities' employees are developed.

Scope:

The malicious use of Open-Source Intelligence (OSINT) is a known concern and technique used by offenders to retrieve personal and professional information about entities and their employees either to immediately plot illegal actions or use it to access more sensitive data with social engineering techniques like tailored data phishing. Although singular information may seem harmless, their critical mass coupled with reasoning and automated processing of large data blocks, could reveal critical vulnerabilities and possible attack vectors. This modus operandi is of special concern for critical infrastructure operators and authorities, as it can be used to aggregate sensitive information, identify potential protection gaps, discover the security measures, such as camera and sensor locations or target individuals with special access privileges in order to orchestrate more sophisticated and harmful attacks. OSINT can also be used to impede critical infrastructure operations indirectly, gathering information and affecting their supply chains.

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

Proposals should build upon outcomes and tools of other relevant projects, adapting, optimising and integrating them when necessary to achieve the highest possible technology readiness level of the project results. The proposals funded under this topic are expected to engage with the Europol Innovation Lab during the lifetime of the project, including validating the outcomes, with the aim of facilitating future uptake of innovations for the law enforcement community.

Destination - Increased Cybersecurity

The Horizon Europe Work Programme for Cybersecurity 2026-2027 aims to enhance the resilience of the European digital ecosystem by addressing emerging threats, securing critical digital infrastructure, and strengthening privacy-preserving mechanisms. The proposed topics seek to advance research and innovation in cybersecurity, fostering technological sovereignty and trust in digital technologies.

Destination - Disaster-Resilient Society for Europe

Given the increasing frequency and ever greater impacts of disasters resulting from climate extremes, natural, geohazards and human-made hazards, the EU needs to invest more in improving disaster risk management, tools for first responders and societal resilience. In this respect, along the orientations given in the Horizon Europe strategic plan 2025-2027, the main objectives of this destination supporting the reduction of losses from natural, accidental and human-made disasters will be pursued in continuity with the strategic plan 2021-2024.

This destination will support the implementation of the European Commission political guidelines 2024-2029 for a ‘Safer and more secure Europe’, a ‘Preparedness Union’, with ‘Stronger Common Borders’, protecting democracy and putting research and innovation at the heart of a resilient economy. Overall, research under this Cluster should continue to focus on preserving and securing citizens’ basic right to feel safe. This destination will support the European Commission efforts towards:

- enhancing efforts to prevent and prepare for new threats, especially those linked to chemical, biological, radiological and nuclear (CBRN) security.
- continuing to address risks to security from climate change impact / step up work on climate resilience and preparedness.
- supporting medical countermeasures against public health threats.

Moreover, this destination will support the implementation of UN Disaster Risk Reduction policies, the EU Disaster Resilience Goals[68] involving closer coordination with the Union Civil Protection Knowledge Network, the rescEU initiative and Member States’ civil protection authorities, as well as an enhanced dialogue at international level with the United Nations Office for Disaster Risk Reduction (UNDRR) on recommendations for the Sendai Framework[69] and United Nations Sustainable Development Goals (SDGs). Such closer coordination with other programmes will make it possible to further streamline future research programming. For example, Cluster 3 should focus on its core added value, which is a strong operational character for preparedness, response and learning, while maintaining complementarities with broader prevention issues such as climate-related risks, covered by Cluster 5, and the Mission on Climate Change Adaptation. There are similar examples in closer coordination with Cluster 6 and the One Health approach, regarding, for instance, water and food security threats (as a result of intentional degradation or terrorist acts).

From a technological perspective, the Destination will ensure greater involvement of practitioners in close cooperation with the Member States and EU agencies, not only in research development and implementation, but also the identification of gaps and needs and future research topics. Actions to develop tools and technologies to meet operational

[68] 2023/C 56/01); COM (2023) 61 final.

[69] UNDRR, Sendai Framework for Disaster Risk Reduction 2015-2030.

capability needs should be aimed at higher technological readiness levels (TRLs). Finally, it will be important to take into account how research results, both those still to come and those already developed in past projects under the DRS destination, can be turned into deployable solutions by being combined with capacity-building programmes (in particular the Internal Security Fund, funding under the Union Civil Protection Mechanism[70] the European Regional Development Fund, and the Cohesion Fund) and social innovation to support the entry into the market of developed technologies. Actions will also aim to ensure that there is a link between R&I and possible procurement (e.g., in the area of medical countermeasures).

Proposals for topics under this Destination should have the overarching objective of improving resilience. Actions will continue to explore initiatives and experiments involving the development of technological or methodological solutions for crisis management and support for emergency responders, getting the general public more involved in this area and improving interactions between regional and/or local authorities, public practitioners, private operators and civil society. Actions could also take into consideration regions vulnerable to extreme weather events in coastal areas, sea level rise and other climate change impacts, which may prone to disaster risks (e.g. the Arctic). New tools or solutions should build on what has been developed in past projects and be capable of being integrated into existing (legacy) systems. Actions will also focus on multi-service capability developments, in particular tools and technologies to support direct operational needs in case of a disaster. This will be done in a scalable way, covering areas from small rural towns to economically developed ones with a high population density, and opening research initiatives to international cooperation. Capabilities need to be upgraded to match the new resilience stakes and expectations of practitioners and of society as a whole. We should learn from past disaster events by identifying gaps in capabilities that the response to such events showed were lacking. For example, one of such gaps are the availability of medical countermeasures used to effectively respond to deliberate or accidental releases of CBRN substances.

The destination will continue to follow a multi-hazard approach, addressing disasters and threats of all kinds, including their cascading issues, climate-related or natural and geological hazards, industrial accidents, pandemics, intentional hostile acts including terrorism and armed conflict. Particular attention will be paid to floods and wildfires, as well as to chemical, biological, radiological, nuclear and explosive (CBRN-E) threats. To this end, proposals should contribute to the achievement of one or more of the following impacts:

- Enhanced citizen and regional and/or local authorities' involvement in research actions, and in operational measures that may result from research, with focus on risk awareness and enhanced disaster prevention and preparedness, including youth awareness raising and education;

[70] See the UCPM scientific needs assessment on disaster risk management: https://civil-protection-knowledge-network.europa.eu/media/outcome-report-scientific-research-needs-exercise.

- Improved disaster risk governance (from prevention, preparedness to mitigation, response, deployment of countermeasures and recovery, using updated risk assessment methods and decision criteria, and including knowledge transfer and awareness of innovative solutions) from international to regional and/or local levels;

- Strengthened capacities of first responders in all operational phases related to any kind of (natural and human-made, including hybrid threats) disasters in support of field operations with validation of tools and technologies used in disaster responses including emergencies, and demonstration of their interoperability.

More precisely, in the context of exacerbated impacts of various disaster threats on vulnerable societies, research and innovation actions are highly needed to face the many challenges faced by European Society. Some of them are:

- Challenges related to inclusion of the general public, regional and/or local communities and voluntary organisations as active partners in order to:
    - empower citizens to act and help them to improve their disaster risk awareness and own resilience to crises, including accountability for regional and/or local administrative decisions on residual risks, youth awareness raising and education;
    - provide means for regional and/or local decision-makers and operational responders, i.e., first and second responders. A “second responder” is a worker who supports "first responders" such as police, fire, and emergency medical personnel. They are involved in preparing, managing, returning services, and cleaning up sites during and after an event requiring first responders, including crime scenes and areas damaged by fire, storm, wind, floods, earthquakes, or other natural disasters. These types of services may include utility services (shutdown or reinstatement of electrical, gas, sewage, and/or water services), wireless or wireline communication services, specialty construction (i.e. shelter construction), hazardous waste clean-up, road clearing, crowd control, emergency services (i.e. Red Cross[71]), first aid, food services, security services, social services (i.e., trauma counsellors), and sanitation, infrastructure owners, regional and/or local authorities (including public services, transport and utilities) to coordinate prevention and preparedness actions, bearing in mind the socio-economic and cultural context, and for operational responders to influence regional and/or local planning decisions that affect exposures and vulnerability to risks in short and long term;
    - address citizens’ perception of, and involvement in, civil defence in the event of very large-scale disasters including armed conflict.

- Challenges regarding the reinforcement of disaster risk governance and the consideration of knowledge and innovative solutions in order to:

[71] https://redcross.eu

  - Improve operational management of crises at different levels (prevention, preparedness, response, recovery) and scales (international to regional and/or local),
  - Reinforce the uptake and transfer of knowledge to risk managers, first and second responders and decision-makers;
  - Strengthen resilience and enhancing protection strategies for emergency services and healthcare workers in case of disasters;
  - Reinforce civil defence capability, looking at all facets of crisis and disaster management, alongside community resilience building;
  - Enhance preparedness for optimised detection, prevention, response and control measures in case of bioterrorism or emerging diseases.
- Challenges related to the validation and usability of tools and technologies, including the demonstration of their interoperability, in the context of strengthened first responder’s capacities as to:
  - Enhance risk awareness, preparedness and communication about foreseeable impacts of disasters;
  - Deploy innovative solutions in emergency situations including trusted communication channels, medical care, medical countermeasures, support equipment (e.g. detectors), triage of victims as well as protection of first responders;
  - Enhance validation of tools, technologies and processes for cross-border prevention, decision-support and responses to climate-related and geological disasters and emergency crises by different practitioner sectors (firefighters, medical emergency services, civil protection, police, NGOs);
  - Enhance interoperability of tools and technologies used in international emergency (real-case) situations related to natural hazards, CBRN-E threats and hybrid threats via inputs such as standard operating procedures for foresight, risk analysis or guidance with the aim to improve market uptake.

This Destination will also support, whenever appropriate and applicable, the proposals with some or all of the following goals:

- A clear strategy from international to regional and/or local on how the overall society will adapt to the evolving disaster risks based on the subsidiarity principle (from the citizen level to international decision-making);
- The involvement of different responders (firefighters, civil protection, medical emergency, police) and regional and/or local authorities in research, development and validation of methods and tools;

- the active role for Non-Governmental Organisations (NGOs) and Civil Society Organisations (CSOs);
- the active involvement of Small and Medium Enterprises (SMEs);
- a robust plan on how they will build on the relevant predecessor projects, and clustering with existing research (EU and national) actions to maximise complementarities and synergies and avoid duplication of efforts;
- education and training aspects for first and second responders for different types of threats (climate-related, geohazards, accidental, intentional), as well as information sharing and awareness raising of the citizens;
- a clear strategy on the uptake of the outcomes, defined in consultation with the involved stakeholders;
- a well-developed plan both on how research data for training and testing will be obtained, in order to reach the requested Technology Readiness Levels (TRLs), and on how the specific TRL will be measured.

Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, including the organisation of international conferences in close coordination with the Community for European Research and Innovation for Security (CERIS)[72] activities and/or other international events.

Proposals are invited against the following topic(s):

HORIZON-CL3-2026-01-DRS-01: Designing new ways of risk awareness and enhanced disaster preparedness

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Action
Eligibility	The conditions are described in General Annex B. The following

[72] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

conditions	exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Development of innovative tools and methodologies to monitor and improve risk awareness across society, integrating diverse community perspectives and leveraging advanced technologies;
- Creation of comprehensive, inclusive preparedness plans that involve all societal sectors and governance levels, ensuring coordinated and effective responses to disasters;
- Establishment of a resilient, adaptive response framework that enhances collaboration between public authorities, communities, and private sectors, improving overall disaster resilience.

Scope: Building on the whole-of-society and whole-of-government approach, this topic should contribute to enhancing risk awareness and disaster preparedness through the development of innovative tools, methodologies, and frameworks. A key focus should be on integrating diverse societal perspectives and vulnerable groups, ensuring inclusive participation in risk communication strategies, and leveraging advanced technologies to improve public understanding of hazards and vulnerabilities. Efforts should aim at designing and validating novel approaches to risk perception, communication, including digital platforms, immersive technologies, and participatory tools that foster citizen engagement and behavioural change. Special attention should be given to marginalized or vulnerable groups to ensure equitable access to risk information and preparedness resources.

Furthermore, proposals should work towards the creation of comprehensive, multi-stakeholder preparedness plans that involve all levels of governance, civil society, the private sector, and local communities. These plans should establish mechanisms for cross-sectoral coordination, efficient resource allocation, and effective decision-making in crisis situations. Research should also explore innovative governance models that enhance interoperability and cooperation between different entities. To strengthen disaster resilience, proposals should develop and test adaptive response frameworks that enhance collaboration between public authorities, communities, and businesses. These frameworks should incorporate near real-time risk assessment tools, digital simulations, and scenario-based exercises to improve the capacity to anticipate, respond to, and recover from disasters. The integration of AI-driven decision-support systems, digital twin technologies, and predictive analytics could further contribute to a more effective, evidence-based crisis response.

Projects are expected to contribute to the overall enhancement of societal resilience by fostering a culture of preparedness, strengthening community-driven disaster risk reduction initiatives, and ensuring that all actors within society have the necessary tools and knowledge to respond effectively to future crises.

International cooperation in this topic is strongly recommended. Proposals should also take into account lessons learned from past disasters and align with existing EU policies, frameworks, and international commitments in the field of disaster risk reduction and crisis management.

HORIZON-CL3-2026-01-DRS-02: Multi-hazard approach and cumulative / cascading impacts

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).

Technology Readiness Level	Activities are expected to achieve from TRL 6 to 7 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Integrate single-hazard systems into multi-hazard next generation predictive models to assess cascading effects (e.g., heatwave, floods, droughts, landslides, heavy rain) and interactions across meteorological, geophysical, and technological hazards;
- Enhance hazard forecasting and response through research on model integration and platform interoperability;
- Collect reliable data (same granularity and format) and ways to share and analyse it. The interoperability of all kinds of systems and information sharing is crucial;
- Improve knowledge/experience-sharing from past emergencies to cope with future emergencies, also strengthening trans-national knowledge and data exchange among EU countries;
- Improve disaster risk management due to single/multiple threats through a holistic, systemic and cross-cutting approach, also considering changing climate, environmental and socio-economic conditions.;
- Development of holistic Risk and Resilience Metrics to support multi-hazard prevention strategies, encompassing main physical, economic and social effects.

Scope: Advancing multi-hazard risk assessment and disaster resilience is a necessity. The advancement will be achieved by integrating single-hazard models into next-generation predictive systems capable of analysing cascading and cumulative effects. A key focus should be on improving the understanding of interactions between meteorological, geophysical, and technological hazards, including their compounding impacts on societies, economies, and critical infrastructure.

Proposals should aim to develop and validate integrated forecasting models that enhance the prediction and management of multi-hazard scenarios, incorporating real-time data, AI-driven analytics, and remote sensing technologies. These models should facilitate improved hazard forecasting by addressing challenges in platform interoperability and data exchange, ensuring that diverse hazard monitoring systems at local, national, and global levels can effectively communicate and operate in synergy.

Efforts should also explore the interoperability of regional and national hazard warning systems, enhancing global forecasting capabilities for hazards such as landslides triggered by extreme weather events, or cumulative damage modelling for earthquakes and their aftershocks. Research should address gaps in loss estimation models by considering the cascading and long-term impacts of disasters on infrastructure, supply chains, and communities. Furthermore, proposals should contribute to the development of advanced tools and methodologies to assess the combined effects of multiple hazards on critical infrastructure, ensuring that disaster risk management strategies account for interdependencies across sectors. This should include scenario-based stress testing, digital twins for risk modelling, and AI-powered decision-support systems to enhance resilience planning for lifeline services such as energy, water, transport, and telecommunications.

A holistic, systemic, and cross-cutting approach should be applied to disaster risk management, taking into consideration climate change trends, environmental degradation, and socio-economic vulnerabilities. The topic should lead to the creation of comprehensive Risk and Resilience Metrics, integrating physical, economic, and social dimensions to support decision-makers in designing effective prevention and adaptation strategies.

Projects should contribute to strengthening risk governance at multiple levels by fostering collaboration between scientific communities, policymakers, emergency responders, and infrastructure operators. Alignment with EU policies, international risk reduction frameworks, and best practices in resilience planning should be ensured, maximizing the applicability and impact of the developed solutions.

HORIZON-CL3-2026-01-DRS-03: Development of innovative tools, equipment and technologies for responses to disasters and emergencies for search and rescue in hazardous conditions

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply:

	This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Creation of cutting-edge tools, equipment, and technologies to enhance disaster and emergency response capabilities for various practitioners;
- Taking into consideration existing technologies, development of autonomous drones and robotics specifically designed for search and rescue operations in hazardous conditions such as wildfires and earthquakes;
- Improvement of response efficiency and safety for survivors and emergency practitioners through the adoption of advanced, technology-driven solutions in disaster scenarios.

Scope: The scope of this topic is the development of innovative tools, equipment, and technologies to enhance the capabilities of emergency responders operating in complex and hazardous disaster environments. By leveraging advancements smart protective equipment, in robotics, autonomous systems, and human sensor technologies, the aim is to improve the efficiency, safety, and effectiveness of search and rescue operations, particularly in high-risk scenarios such as wildfires, earthquakes.

Proposals should explore the design, testing, and validation of innovative solutions capable of performing critical tasks in disaster-stricken areas. These technologies should be tailored to operate in extreme conditions, including high temperatures, unstable terrains, and low-visibility environments. Research should address challenges related to autonomous navigation, AI-driven decision-making, real-time situational awareness, and seamless integration with existing command-and-control systems used by first responders. Collaboration of different practitioners should be supported.

Efforts should be made to enhance interoperability and data-sharing capabilities between various platforms, emergency response teams, and crisis management systems. A key aspect of this research should be the practical deployment and validation of these technologies through field exercises and simulations in real-world disaster scenarios. User-driven design approaches should ensure that developed solutions align with the operational needs of responders in disasters.

Furthermore, proposals should consider ethical, legal, and social implications associated with the deployment of autonomous technologies in emergency response. Issues such as data privacy, cybersecurity, public acceptance, and compliance with regulatory frameworks should be addressed to facilitate the responsible and effective use of these innovations.

Projects should contribute to strengthening Europe’s disaster response capacity by equipping practitioners with state-of-the-art technological solutions that enhance their ability to operate safely and efficiently in life-threatening environments. Alignment with EU policies and international best practices should be ensured to maximize the scalability and real-world applicability of the developed solutions.

HORIZON-CL3-2026-01-DRS-04: Open topic on driving innovation uptake of disaster risk solutions

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 8 by the end of the project – see General Annex B.
Security Sensitive	Some activities resulting from this topic may involve using classified

Topics	background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Accelerated the adoption of high-TRL (Technology Readiness Level) disaster risk solutions across diverse sectors;
- Facilitated integration of innovative technologies into existing disaster preparedness, response, and recovery frameworks;
- Promoted collaboration among stakeholders to scale proven solutions and enhance resilience;
- Addressed barriers to deployment, ensuring accessibility and usability of advanced DRS technologies.
- Strengthened evidence-based decision-making through demonstration and validation of high-TRL solutions in real-world scenarios;

Scope: This topic aims to foster the widespread adoption and integration of high-TRL (Technology Readiness Level) disaster risk solutions (DRS) across multiple sectors, enhancing societal resilience to various hazards. The focus is on overcoming barriers to deployment, ensuring accessibility, and strengthening collaboration among stakeholders to drive innovation uptake. Projects should promote the adoption of high-TRL solutions by public and private sector organizations involved in disaster risk management, developing strategies for scaling and commercializing innovative DRS technologies to ensure they reach end-users efficiently. They should also demonstrate how these technologies can complement or replace existing disaster preparedness, response, and recovery frameworks by developing interoperability standards and guidelines for integrating new solutions into national and European civil protection systems.

Addressing deployment barriers is crucial, including identifying and mitigating technical, regulatory, financial, and social obstacles hindering the uptake of advanced solutions, while ensuring accessibility and usability for diverse stakeholders such as first responders, local authorities, and vulnerable communities. Projects should also demonstrate the real-world effectiveness of high-TRL solutions through large-scale pilot projects and demonstrations, generating robust evidence to support data-driven decision-making and optimize disaster risk reduction strategies. Initiatives should align with EU disaster resilience objectives and build on existing programs, ensuring synergies with relevant policies, funding mechanisms, and technological ecosystems. Proposals are encouraged to incorporate digital tools, AI-driven analytics, IoT applications, and other emerging technologies to enhance disaster preparedness and response.

HORIZON-CL3-2027-01-DRS-01: Open Topic on advanced protective gear optimized for CBRN-E (Chemical, Biological, Radiological, Nuclear, Explosives) environments and new generation of smart protective equipment for disaster responders

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 7-8 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Development of advanced protective gear specifically designed for optimal performance in Chemical or Biological or Radiological, and Nuclear or Explosives (CBRN-E) environments;
- Taking into accounts of past research outputs, creation of innovative smart protective equipment for disaster responders, incorporating advanced technologies to enhance safety and operational efficiency.

- Improvement of protective solutions to ensure the safety and effectiveness of disaster responders operating in hazardous and high-risk environments.

Scope: This topic aims to advance the development of protective gear specifically designed for optimal performance in specificities of the Chemical, Biological, Radiological, Nuclear, and Explosives (CBRN-E) environments, along with the creation of a new generation of smart protective equipment for disaster responders. Projects should focus on the use of innovative materials, technologies, and design features that enhance the protective capabilities of gear used in high-risk, hazardous environments, ensuring the safety and well-being of disaster responders. The integration of advanced technologies will be crucial to enhancing the operational efficiency and effectiveness of the equipment.

Projects should build upon existing research outputs, specifically under other Horizon Europe Cluster 4, and technologies to create smart, adaptive protective solutions that respond dynamically to evolving threats in CBRN-E scenarios. This includes the incorporation of features similar to automated hazard detection, environmental monitoring, and advanced communication systems to provide real-time situational awareness. The new gear should meet rigorous safety standards while improving the comfort, mobility, and usability of responders, enabling better performance and faster decision-making in demanding environments.

Proposals should focus on providing comprehensive solutions that combine robust protection, operational support, and data-driven insights, ensuring a holistic approach to safety. Collaboration between research institutions, manufacturers, and end-users will be essential to ensure that the resulting products meet the practical requirements of practitioners in the field.

HORIZON-CL3-2027-01-DRS-02: Societal resilience, engagement of the younger Generations and digital innovation for disaster resilience

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least …

	If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Developed tailored education programs for younger generations, incorporating digital tools and gamification to enhance disaster awareness and engagement;
- Strengthened societal resilience by actively involving younger generations, citizens, and local authorities in disaster preparedness and response initiatives;
- Promoted collaborative research that integrates youth perspectives and community involvement, fostering a more resilient society in the face of disasters and crises.
- Impact and the behaviour of children, young people, and other vulnerable groups before, during, and after climate-related disasters and health emergencies.
- Training and education tools to engage young people and other vulnerable populations in preparedness and crisis management.

Scope: This topic focuses on enhancing societal resilience by actively engaging younger generations in disaster preparedness, response, and recovery through digital innovation, education, and community involvement. Projects should develop tailored innovative solutions that integrate digital tools, gamification, and interactive learning methods to improve disaster awareness, risk perception, and response capabilities among younger generations. These initiatives should empower younger generations[73], to become active contributors to resilience-building efforts, equipping them with the knowledge, leadership skills, and

[73] In the context of the European Union, **youth** is typically defined as individuals between the ages of **13 and 30**. This definition aligns with the EU's Youth Strategy, which focuses on supporting young people’s personal and professional development. However, some EU programs may adjust the age range slightly depending on the specific context (e.g., education, employment, or participation), but the 13-30 age bracket is recognized in EU policies related to youth.

Particular attention should be given to the behaviour of children, young people, and other vulnerable groups before, during, and after climate-related disasters and health emergencies. Participatory approaches, including youth-led initiatives, citizen science, and digital engagement platforms, should be prioritized to enhance community-based resilience and ensure young people's perspectives are integrated into decision-making processes.

Projects should also focus on leveraging emerging technologies - such as artificial intelligence, virtual and augmented reality, social media analytics, and serious games - to engage young people in disaster preparedness and crisis response. Additionally, innovative communication strategies should be explored to enhance youth participation, particularly through digital technologies and social media. Practical examples, including pilots and real-world case studies, should be developed to test and refine these approaches.

Proposals should explore methods to interconnect young people's data with crisis management teams, practitioners, and authorities, ensuring that their contributions are effectively integrated into emergency response frameworks. Training and education tools should be designed to engage young people and other vulnerable populations in preparedness and crisis management, promoting long-term resilience.

By fostering collaborative research and youth-driven initiatives, projects should contribute to innovative and inclusive resilience strategies that align with EU policies on disaster risk reduction, education, digital transformation, and civil protection. Proposals should ensure synergies with existing initiatives and frameworks, such as the Sendai Disaster Risk Reduction Framework.

HORIZON-CL3-2027-01-DRS-03: Enhancing Decision Support System for Disaster Crises: Leveraging Emerging Technologies for Improved Civil Preparedness and Crisis Management

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply:

	This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Development of a decision support system for disaster crises, utilizing near real-time data from the ground to enhance situational awareness and response;
- Creation of systems designed to bolster civil preparedness, ensuring timely and effective management of various disaster scenarios;
- Integration of advanced data analysis and decision-making tools to support authorities and first responders in disaster situations.

Scope: This topic focuses on enhancing existing decision support systems for disaster crises by integrating emerging technologies to improve civil preparedness and crisis management. The objective is to advance the capabilities of existing systems, making them more reliable, adaptable, and efficient through the incorporation of trustworthy AI technologies that ensure transparency, accountability, and ethical decision-making processes. Projects should aim to enable quicker and more informed responses during disaster scenarios.

Proposals should focus on creating advanced systems designed to strengthen civil preparedness, helping authorities and responders manage various disaster situations in a timely and effective manner. These systems should leverage cutting-edge AI-driven tools to process large volumes of data, providing actionable insights that improve decision-making during critical moments. Emphasis should be placed on integrating advanced data analysis and predictive modelling to anticipate disaster developments and guide interventions, while ensuring that the systems are transparent, explainable, and built on principles of trustworthiness and ethical AI use.

The expected outcome is to create systems that not only enhance operational efficiency and response times but also foster better collaboration among stakeholders, including local authorities, emergency services, and other relevant actors. Projects should also contribute to improving the usability and accessibilit of decision support systems for diverse users, ensuring they are easily integrated into disaster management frameworks and can be used effectively in different crisis situations. The solutions should align with EU guidelines on AI ethics[74] and resilience-building, ensuring they complement existing civil protection and crisis management initiatives while driving innovation in disaster risk reduction.

HORIZON-CL3-2027-01-DRS-04: Enhancing Preparedness for large-Scale cross-border disasters

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

[74] AI Act

- Utilization of virtual and augmented reality training to simulate large-scale and transboundary disasters, improving first responders' readiness and response capabilities;
- Development of diverse crisis scenarios using VR/AR technology, providing immersive, practical training experiences for emergency personnel, responders and decision makers;
- Strengthening the ability of responders and decision makers to manage large-scale, cross-border disaster scenarios through advanced, technology-driven training programs;
- Improve knowledge/experience-sharing from past emergencies to cope with future emergencies, also strengthening trans-national knowledge and data exchange among EU countries.

Scope: The scope of this topic is on enhancing preparedness for large-scale, cross-border disasters by leveraging advanced training methodologies, including virtual reality (VR) and augmented reality (AR) simulations and Digital Twins. The objective is to improve the readiness and response capabilities of disaster responders and emergency management personnel by providing immersive, technology-driven training experiences that replicate complex disaster scenarios.

Proposals should develop and validate innovative VR/AR-based crisis simulation models that can accurately depict diverse large-scale disaster situations, including transboundary hazards such as wildfires, floods, earthquakes, and industrial accidents. These simulations should incorporate near real-time data, AI-driven scenario adaptation, and multi-user interaction capabilities to ensure realistic, high-impact training exercises. Special attention should be given to the interoperability of these training platforms, allowing emergency services from different regions and countries to collaborate in joint preparedness exercises.

Research should also explore how digital training environments can enhance situational awareness, decision-making, and coordination among first responders and relevant authorities. The integration of gamification techniques, AI-driven coaching systems, and real-time performance assessment should be considered to maximize learning outcomes and adaptation to evolving crisis scenarios linking to previous themes (e.g. biometrics and long lasting disturbance, or whole of the society security, multi-hazard theme etc).

Furthermore, proposals should focus on strengthening knowledge and experience-sharing mechanisms across EU member states by developing transnational training frameworks and crisis management protocols. This should include the establishment of digital platforms and collaborative networks to facilitate the exchange of lessons learned from past emergencies, fostering continuous improvement in disaster response strategies.

Ethical, legal, and social aspects related to the use of immersive training technologies should also be addressed, ensuring compliance with data protection regulations and maximizing public trust in the adoption of these tools. Projects should align with existing EU disaster risk reduction policies and international best practices to ensure the practical applicability and scalability of the developed solutions.

Destination - Strengthened Security Research and Innovation

Since the Preparatory Action for Security Research[75] the EU-funded security research and innovation programme has contributed substantially to knowledge and value creation in the field of internal security. The programme has been fundamental to the consolidation of a European security ecosystem, which is better equipped to capitalise on research and innovation outcomes to support the EU security priorities. This Destination aims to contribute to reducing thematic fragmentation, bringing closer together the actors from different security domains, and expanding the market beyond traditional thematic silos. It also creates knowledge and value through research in matters (including technology, but also social sciences and humanities) that are not exclusive of only one security area, but cross-cutting to the whole Cluster.

As underlined in the Horizon Europe strategic plan 2025-2027, proposals for the topics under this Destination ‘should support with cross-cutting actions the expected impacts outlined above [in the Cluster 3 Destinations]. The destination will increase the impact of the work carried out in the EU security Research and Innovation (R&I) ecosystem and contribute to its core values, namely:

- a focus on the potential and practical final use of the outcomes of security R&I;
- forward-looking planning of EU security capabilities;
- the development of security technologies that are socially acceptable, developed in quadruple helix[76] and that have added value for industrialisation, joint procurement, commercialisation, and the acquisition and deployment of successful R&I outcomes;
- safeguarding the EU’s open strategic autonomy and technological sovereignty in critical security areas by contributing to a more competitive and resilient EU civil security technology and industrial base;
- experimenting with research and innovation programming; and
- helping to make the European R&I ecosystem more consistent’.

Many of the programme outcomes have materialised in relevant scientific findings, maturation of promising technology areas, operational validation of innovative concepts or support to policy implementation. However, a key challenge remains in improving innovation uptake and thus contributing to the development of security capabilities[77], support of Start-ups

[75] COM(2004) 72.

[76] Through the interaction of public authorities, academia, industry and the public.

[77] For the purpose of the work programme, the terms “Capability” should be understood as "the ability to pursue a particular policy priority or achieve a desired operational effect”. The term “capability” is often interchanged with the term “capacity”, but this should be avoided. “Capacity” could refer to an amount or volume of which one organisation could have enough or not. On the other hand, “capability” refers to an ability, an aptitude or a process that can be developed or improved in consonance with the ultimate objective of the organisation.

and Small-Medium Enterprises (SMEs) and deployment of innovation by security practitioners.

The extent to which innovative technologies developed thanks to EU R&I investment are industrialised and commercialised by EU industry, and acquired and deployed by end-users, could reflect the impact achieved with the programme. As explained in the Commission staff working document on Enhancing security through research and innovation[78] there are factors inherent to the EU security ecosystem (often attributed to the market) that hinder the full achievement of this impact, such as market fragmentation, cultural barriers, analytical weaknesses, programming weaknesses, ethical, legal and societal considerations or lack of synergies between funding instruments, among others. To that aim, there is a need to create a favourable environment that is designed with the main purpose of increasing the impact of security R&I, which provides the right tools that serve to tackle the factors that hinder innovation uptake.

Therefore, security research and innovation should foster and enhance the development of innovative tools, technologies and capabilities for the benefit of practitioners that can use in their day-to-day work. To this end proposals 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 Destination will trigger actions that will help bringing these and other developments closer to the market, thus contributing to the measures facilitating the uptake of innovation. Those actions will help developers (including industry, research organisations and academia) to accelerate product development and improve the valorisation of their research investment. They will also support buyers and users in materialising the uptake of innovation and further develop their security capabilities. The aim is to increase the capacity of EU public procurers to align their requirements with the EU security industrial capacity and to attract innovation and innovators from security and other sectors through common validation strategies, rapid innovation, experimentation and pre-commercial procurement.

[78] https://home-affairs.ec.europa.eu/document/download/ff888398-0b0a-4511-9717-ad41beb22314_en?filename=SWD-2021-422_en.PDF

Finally, the Destination will contribute to the development of the tailored analytical capacity required for the adoption of capability-driven approaches aimed at fostering a forward-looking capability-driven approach in security.

Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, including the organisation of international conferences in close coordination with the Community for European Research and Innovation for Security (CERIS)[79] activities and/or other international events.

Proposals are invited against the following topic(s):

HORIZON-CL3-2026-01-SSRI-01: Open topic on supporting disruptive technological innovations for civil security

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Research and Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 4-5 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU

[79] https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

	classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Improved preparedness, evidence-based approaches and response capabilities, along with a strengthened ability to mitigate risks from diverse threats, by integrating validated disruptive technologies into real-world operations;
- Accelerated adoption of innovative solutions by reducing barriers through rigorous testing and validation, fostering collaboration among public authorities, industry, and researchers to align technologies with real-world needs.

Scope: This topic aims to support the integration of disruptive technological innovations into civil security by strengthening research and innovation activities that enhance preparedness, response capabilities, and risk mitigation. A key focus is bridging the gap between early-stage, low Technology Readiness Level (TRL) research and applied security solutions, ensuring that emerging technologies are effectively transitioned into operational use.

Projects should prioritize disruptive solutions that address diverse security threats while improving the efficiency and effectiveness of civil security operations. Emphasis should be placed on ensuring that these technologies are robust, reliable, scalable, and aligned with the needs of security practitioners. This includes fostering a structured pathway for transitioning low TRL innovations into practical applications, ensuring rigorous validation processes for safety, performance, and interoperability.

To achieve this, proposals should promote strong collaboration between researchers, public authorities, industry partners, and end-users. Such partnerships will help align technological advancements with real-world security needs, facilitating the co-development of solutions that are both innovative and operationally relevant. Ensuring that emerging technologies are ethically sound, transparent, and accessible will also be crucial to their successful adoption.

The expected outcomes of this topic include improved preparedness through the adoption of cutting-edge technologies tailored to emerging security challenges, enhanced risk mitigation capabilities, and the accelerated integration of disruptive innovations into civil security frameworks. By fostering a collaborative ecosystem, projects should ensure that promising research transitions effectively into practical security applications, contributing to a more resilient and adaptive civil security landscape across Europe.

HORIZON-CL3-2026-01-SSRI-02: Demand-led innovation in security

Call: Civil Security for Society	
Specific conditions	
Expected EU	The Commission estimates that an EU contribution of around EUR …

contribution per project	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 … million.
Type of Action	PCP
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected 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: As past experience shows that pre-commercial procurement opens up the procurement market for startups and enables the public sector to address societal challenges more effectively, public procurers should make more strategic use of PCP. Applicants are invited to submit proposals for PCP action to acquire Research and Development (R&D) services and innovative civil security technology solutions.

Proposals should demonstrate interest from a broader community of potential buyers, beyond the direct beneficiaries, who share similar needs and are open to jointly adopting the solutions developed, provided they are proven mature and operationally viable. The proposals must include an analysis of the state of the art and market landscape, aligning research activities with identified needs and presenting a range of technical alternatives to address the challenge. Furthermore, to stimulate dialogue with the supply side, public procurers are required to organise proposals should demonstrate sustainability of the action beyond the life of the project.

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*. The proposals should provide clear evidence to justify and de-risk the PCP action, demonstrating that the identified challenge is significant and necessitates a PCP action to mature certain technologies and compare alternatives. It must be shown that a consolidated group of practitioners and procurers with shared needs and requirements is committed to the PCP process, enabling informed decisions on future joint procurement of innovative solutions. Activities covered should include cooperation with policy makers to reinforce the national policy frameworks and mobilise substantial additional national budgets for PCP and innovation procurement in general beyond the scope of the project. The tendering process must be well-defined, supported by a draft plan, and include readiness of documentation and administrative procedures to ensure a compliant launch of the call for R&D services under PCP rules.

Proposals must demonstrate commitment to exploiting project results beyond its conclusion, ensuring engagement with stakeholders and implementation of strategies for future uptake. Applicants should also clarify measures to ensure compliance with the principles of the EU Directive on public procurement, particularly those related to PCP. The required open market consultations should be completed in at least three EU Member States. Prior consultations conducted under previous CSA projects may be used, provided they ensured procurement viability and remain relevant to the current state of the art.

Involvement of procurement decision makers is needed to ensure that end solution(s) are adopted by public buyers, increasing the societal impact of the related research activities. Therefore, procurers should declare in the proposal their interest to pursue deployment of solutions resulting from the PCP in case the PCP delivers successful solutions and indicate whether they will:

- Procure successful solution(s) as part of the PCP.
- Launch a separate follow-up procurement after the PCP to buy such type of solutions.
- Adopt successful solutions without the need to procure them (e.g. in case of open-source solutions).
- Foresee financial or regulatory incentives for others to adopt successful solutions (e.g. in case the final end-users of the solutions are not the procurers but for example citizens).

- In these four cases, the procurers can implement the project as a fast-track PCP[80]. In the first case, the procurers must foresee the budget in the proposal to purchase at least one solution during the PCP. In the second case, the procurers should include in the proposal a deliverable that prepares the follow-up procurement to purchase such type of solution(s) after the PCP. In the first and third case, the procurers must foresee sufficient time during the project to deploy and validate that the solutions function well after installation. In the fourth case, the procurers can use financial support to third parties to provide financial incentives to final end-users to adopt the solutions, with a maximum budget of EUR 100.000.

Applicants should propose an implementation of the project that includes:

- A minimal preparation stage dedicated to finalising the tendering documents package for a PCP call for tenders based on the technical input, and to define clear verification and validation procedures, methods and tools for the evaluation of the prototypes to be developed throughout the PCP phases.
- Moreover, to ensure the sustainability and uptake of the developed solutions, proposals should outline clear plans for post-PCP activities. As outlined in the general annexes of the Horizon Europe Work Programme, the topic allows public buyers to use the fast-track PCP option (e.g. 2 instead of 3 phases) when they commit to buying or deploying the resulting solutions after the PCP. However, if such a commitment is not yet in place at the proposal stage, the call requires proposers to include a deliverable outlining concrete activities to prepare the ground for follow-up deployment or procurement after the PCP.
- 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.

[80] see General Annex H of the Horizon Europe Work Programme.

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.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

HORIZON-CL3-2026-01-SSRI-03: Public Procurement of Innovation for security

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	PPI
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Last mile support to previous PCP actions;

- Development and deployment of innovative security solutions to address emerging threats, improving the effectiveness and efficiency of public security services;
- Implementation of pilot projects and real-world testing, ensuring scalability and contributing to innovative security technologies.

Scope: This Public Procurement of Innovative Solutions (PPI) initiative aims to advance the adoption of innovative civil security solutions. The focus is on solutions that have been partially demonstrated on a small scale and are nearly or already available in small quantities but have not yet been widely adopted or produced at scale. These solutions should demonstrate a clear market potential and be new to the procurers, their market segment, or the internal EU market, and must be relevant to procurers across EU Member States and/or Associated Countries.

This PPI will specifically target innovative solutions that can address critical challenges in civil security and that are aligned with market readiness criteria. The solutions must meet requirements for sustainability, interoperability, adaptability, and be commercially viable while still holding residual market risks, such as not yet being produced in large quantities or at market-ready quality and pricing.

This initiative will focus on solutions that have already demonstrated partially successful results but require scaling, refinement, or deployment in new environments to meet mass-market price/quality standards. This is in line with Horizon Europe's objective of fostering the early adoption of innovations that are critical to improving civil security across Europe[81].

In compliance with the requirements of the Horizon Europe Work Programme – Annex H, this action will engage in open market consultations with potential tenderers and end-users to identify gaps between perceived procurement needs and current industry developments. Feedback from these consultations will inform the PPI tender specifications, ensuring that the PPI emphasizes the early adoption of innovative solutions rather than the procurement of fully mature or mass-market technologies. The market readiness of the solutions can be verified through conformity testing, certification, or quality labelling. The work will also involve establishing evaluation criteria based on best-value-for-money rather than solely on the lowest price, ensuring that innovations are assessed for both their technical performance and their potential to deliver long-term value.

The PPI contract notices will be published EU-wide, with offers evaluated on objective criteria, ensuring transparency and fairness in the selection process. Functional/performance-based specifications will be used to define the challenges and problems to be solved, rather than prescriptive solutions, and procurement will avoid any conflicts of interest. The distribution of Intellectual Property Rights (IPR) will be clearly outlined in the PPI call for tenders, in line with the objective of promoting fair and wide exploitation of the results.

[81] For more information see the General Annex H – Specific Conditions for Actions with PCP/PPI of Horizon Europe Work Programme.

Unless the PPI is undertaken as a follow-up to an FP7, Horizon 2020 or Horizon Europe PCP, or unless the situation is a low-value PPI below national procurement thresholds, the following obligations apply:

- To prepare the call for tenders, an open market consultation with potential tenderers and end-users must be held to inform the market well in advance of the upcoming PPI and broach the views of the market on the PPI's intended scope. Information retrieved from this consultation about the gap between perceived procurement needs and on-going industry developments must be taken into account in the PPI tender specifications, so that the PPI duly focuses on 'early adoption' of 'innovative' solutions.
- The market must be informed well in advance of the target date for publishing the PPI call for tenders. Market readiness prior to deployment can be verified through the organisation of e.g. conformity testing, certification or quality labelling of solutions.
- The PPI contract notices must be published EU-wide in at least English, offers must be accepted and communication with stakeholders must be enabled at all stages in at least English. All offers must be evaluated according to the same objective criteria, regardless of the geographical location, size of organisation or governance structure of the tenderers.
- The prior information notices for the open market consultation, early announcements of the expected publication date of the PPI call for tender, and the PPI contract notice must be promoted and advertised widely, using Horizon Europe internet sites and national contact points in particular. The Commission must be informed at least 5 days before the expected date of publication of the PIN for the open market consultation and 30 days before the expected date of publication of the PPI contract notice. The PPI call for tenders must remain open for at least 60 days.

By fostering the early adoption of innovative technologies, this PPI initiative will enable the European civil security sector to address emerging threats, while contributing to the EU's broader goals of technological sovereignty and market innovation. This will allow public authorities to remain at the forefront of addressing evolving risks and threats. The action will also catalyze innovation, drive competition, and significantly reduce the time needed to move from the initial concept to market.

HORIZON-CL3-2026-01-SSRI-04: Development of Ecosystem and Next-Generation Capabilities for European Critical Secured Communication Systems in Civil Security

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Creation of an integrated ecosystem for secure and resilient communication systems to support civil security operations across Europe;
- Advancement of next-generation capabilities, ensuring robust, scalable, and interoperable communication systems for critical civil security functions relevant for the future EUCCS.

Scope: The European Union Critical Communication System (EUCCS) is a flagship initiative aiming at gradual development of a unified, secure, and interoperable communication infrastructure to support critical public safety and civil security operations across Europe. Aims to provide law enforcement, first responders, emergency services, and other critical sectors with reliable, real-time communication capabilities, even in challenging or high-risk environments. This topic aims to streamline the creation of an integrated ecosystem for secure and resilient communication systems that support civil security operations across Europe. It aims to advance next-generation capabilities, ensuring robust, scalable, and interoperable communication systems tailored to the critical civil security functions that will be required for the future European Union Critical Communication System (EUCCS).

The project will develop secure communication devices and applications that meet the unique needs of practitioners across various disciplines. These solutions will go beyond current broadband technologies, enabling specialized, ruggedized devices that support hands-free capabilities, including wearable sensors, haptics, and augmented reality to enhance situational awareness. Devices will be designed to ensure communication in environments lacking cellular infrastructure and will be built with high standards of security and trustworthiness.

The solutions should be mission-critical, offering high availability, resilience, and secure data exchange, even in areas with limited or no commercial network coverage. They must be fully compatible with EUCCS, leveraging 3GPP Mission Critical Services (MCX) and open APIs to create a versatile and interoperable ecosystem. By working closely with first responders and utilizing open platforms, the project will ensure that the developed solutions address the specific operational needs of responders, facilitating effective cross-agency and pan-European collaboration.

HORIZON-CL3-2027-01-SSRI-01: Accelerating uptake through open proposals for advanced SME innovation

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	Innovation Action
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and

	SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Facilitate increased and sustained collaboration between SMEs, public research partners, and academia, leading to improved knowledge transfer within the European innovative SME ecosystem;
- Mitigate difficulties in access to finance and new international markets, thereby enhancing the growth and expansion of European innovative SMEs.

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 and medium innovators to tailor their innovations to the specific needs of civil security end-users, taking into account the urge to address the diverse needs of all citizens, regardless of gender.

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;
- Fostering collaboration between SMEs from different Member States and Associated Countries;
- Involving 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.

Examples of activities to plan in the proposed projects include, but are not limited to: 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.

The participation of research and technology organisations should not focus on own 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[82]. Exceptions to this requirement should be duly justified.

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

This topic contributes to the Strategic Technologies for Europe Platform (STEP[83]) and addresses civil security technologies falling under the sectors of “Digital technologies and deep-tech innovation[84]]”. This topic contributes to the objectives stated in the STEP Regulation, e.g., to support the European industry and boost investment in critical technologies in Europe, and, to contribute to reducing or preventing the strategic dependencies of the Union. Proposals under this topic that are eligible and exceed the evaluation thresholds will be awarded a STEP Seal.

HORIZON-CL3-2027-01-SSRI-02: Open grounds for future pre-commercial procurement of innovative security technologies

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	CSA
Eligibility	The conditions are described in General Annex B. The following

[82] If a MIDCAP is included in the proposal, it could also take the role of coordinator.
[83] OJ L, 2024/795, 29.2.2024, ELI: http://data.europa.eu/eli/reg/2024/795/oj
[84] https://strategic-technologies.europa.eu/index_en

conditions	exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected outcomes:

- Establish a consolidated group of potential buyers with shared needs and requirements, committed to carrying out a PCP action for future joint procurement of innovative solutions;
- Evidence for Future PCP Action: Provide clear evidence justifying the necessity of a PCP action to complete the maturation cycle of certain technologies and compare different alternatives.

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 (PCP) action. Both this preparatory action and the future PCP action are open to proposals oriented to the acquisition of Research and Development (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 human-made disasters.

In preparing the grounds for a possible future PCP action, the outputs of this Coordination and Support Action (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 and gender 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.
In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

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

HORIZON-CL3-2027-01-SSRI-03 Demand-led innovation in security

Call: Civil Security for Society	
Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR … 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 … million.
Type of Action	PCP
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least … If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL … by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Project results are expected to contribute to **some or all** of the following expected 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: As past experience shows that pre-commercial procurement opens up the procurement market for startups and enables the public sector to address societal challenges more effectively, public procurers should make more strategic use of PCP. Applicants are invited to submit proposals for PCP action to acquire Research and Development (R&D) services and innovative civil security technology solutions.

Proposals should demonstrate interest from a broader community of potential buyers, beyond the direct beneficiaries, who share similar needs and are open to jointly adopting the solutions developed, provided they are proven mature and operationally viable. The proposals must include an analysis of the state of the art and market landscape, aligning research activities with identified needs and presenting a range of technical alternatives to address the challenge. Furthermore, to stimulate dialogue with the supply side, public procurers are required to organise proposals should demonstrate sustainability of the action beyond the life of the project.

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*. The proposals should provide clear evidence to justify and de-risk the PCP action, demonstrating that the identified challenge is significant and necessitates a PCP action to mature certain technologies and compare alternatives. It must be shown that a consolidated group of practitioners and procurers with shared needs and requirements is committed to the PCP process, enabling informed decisions on future joint procurement of innovative solutions. Activities covered should include cooperation with policy makers to reinforce the national policy frameworks and mobilise substantial additional national budgets for PCP and innovation procurement in general beyond the scope of the project. The tendering process must be well-defined, supported by a draft plan, and include readiness of documentation and administrative procedures to ensure a compliant launch of the call for R&D services under PCP rules.

Proposals must demonstrate commitment to exploiting project results beyond its conclusion, ensuring engagement with stakeholders and implementation of strategies for future uptake. Applicants should also clarify measures to ensure compliance with the principles of the EU Directive on public procurement, particularly those related to PCP. The required open market consultations should be completed in at least three EU Member States. Prior consultations conducted under previous CSA projects may be used, provided they ensured procurement viability and remain relevant to the current state of the art.

Involvement of procurement decision makers is needed to ensure that end solution(s) are adopted by public buyers, increasing the societal impact of the related research activities. Therefore, procurers should declare in the proposal their interest to pursue deployment of solutions resulting from the PCP in case the PCP delivers successful solutions and indicate whether they will:

- Procure successful solution(s) as part of the PCP.
- Launch a separate follow-up procurement after the PCP to buy such type of solutions.

- Adopt successful solutions without the need to procure them (e.g. in case of open-source solutions).
- Foresee financial or regulatory incentives for others to adopt successful solutions (e.g. in case the final end-users of the solutions are not the procurers but for example citizens).

In these four cases, the procurers can implement the project as a fast-track PCP[85]. In the first case, the procurers must foresee the budget in the proposal to purchase at least one solution during the PCP. In the second case, the procurers should include in the proposal a deliverable that prepares the follow-up procurement to purchase such type of solution(s) after the PCP. In the first and third case, the procurers must foresee sufficient time during the project to deploy and validate that the solutions function well after installation. In the fourth case, the procurers can use financial support to third parties to provide financial incentives to final end-users to adopt the solutions, with a maximum budget of EUR 100.000.

Applicants should propose an implementation of the project that includes:

- A minimal preparation stage dedicated to finalising the tendering documents package for a PCP call for tenders based on the technical input, and to define clear verification and validation procedures, methods and tools for the evaluation of the prototypes to be developed throughout the PCP phases.
- Moreover, to ensure the sustainability and uptake of the developed solutions, proposals should outline clear plans for post-PCP activities. As outlined in the general annexes of the Horizon Europe Work Programme, the topic allows public buyers to use the fast-track PCP option (e.g. 2 instead of 3 phases) when they commit to buying or deploying the resulting solutions after the PCP. However, if such a commitment is not yet in place at the proposal stage, the call requires proposers to include a deliverable outlining concrete activities to prepare the ground for follow-up deployment or procurement after the PCP.
- 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

[85] see General Annex H of the Horizon Europe Work Programme.

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.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Other actions not subject to calls for proposals

1. External expertise for reviews of projects (2026-2027)

This action will support the use of appointed independent experts for the monitoring of actions (grant agreement, grant decision, public procurement actions, financial instruments) funded under Horizon Europe and previous Framework Programmes for Research and Innovation, and where appropriate include ethics checks, as well as compliance checks regarding the Gender Equality Plan eligibility criterion.

Form of Funding: Other budget implementation instruments

Type of Action: Expert contract action

2. Workshops, conferences, experts, communication activities, studies and innovation uptake promotion (2026-2027)

- Support to workshops, expert groups, communications activities, or studies. Workshops are planned to be organised on various topics to involve end-users (e.g. the Community for European Research and Innovation for Security); preparation of information and communication materials, etc.
- Organisation of cybersecurity conferences and support to other cybersecurity events; socio-economic studies, impact analysis studies and studies to support the monitoring, evaluation and strategy definition for cybersecurity and digital privacy policy.
- Support to promotion of innovation uptake, including through supporting developing certification testing methodologies for innovative technologies.
- Needs analysis and options for enabling the sharing of security research projects outputs (tools).

Form of Funding: Procurement

Type of Action: Public procurement

3. Indirectly Managed Action by the ECCC (2026)

The Commission intends to conclude a contribution agreement with the European Cybersecurity Competence Centre (ECCC) for the implementation of Horizon Europe cybersecurity actions not co-funded by Member States, in accordance with Article 5(5) of Regulation (EU) 2021/8878. Further to the contribution agreement, the ECCC will launch a call for proposals in accordance with the specifications in the Appendix set out below. These include topics where participation will be limited in accordance with Article 22(5) of the Horizon Europe Regulation to legal entities established in Member States and Horizon Europe Associated Countries (eligible countries). In addition, for such topics, in order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, will not be eligible to participate.

The Commission intends to conclude a contribution agreement with the ECCC, in accordance with Article 5(5) of Regulation (EU) 2021/8878. In particular, the contribution agreement will entrust the ECCC with the implementation of a call for proposals according to the specifications in the Appendix set out below.

Legal entities: European Cybersecurity Competence Centre (ECCC), Polytechnic University of Bucharest, Strada Splaiul Independentei Nr.313, Sector 6, Bucharest 060042, Romania

Form of Funding: Indirectly managed actions

Type of Action: Indirectly managed action

Indicative budget: EUR … million from the 2026 budget

APPENDIX – Indirectly managed action by the ECCC

Specifications of the ‘Increased Cybersecurity’ call to be launched by ECCC

Call - Increased Cybersecurity

HORIZON-CL3-2026-02-CS-ECCC

Conditions of the call[86]

Proposals are invited against the following topic(s):

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[87]	Indicative number of projects expected to be funded
		2026		
Opening: April 2026 (tentative) Deadline(s): September 2026 (tentative)				

[86] The Executive Director-of the ECCC may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Executive Director of the ECCC 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 2025.

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

Approaches and tools for security in software and hardware development and assessment (including open source)	RIA			
Enhancing the Security and Robustness of AI Models and Systems (SecureAI)	IA			
Post-quantum cryptography	RIA			
Emerging challenges: Human aspects of Cybersecurity	RIA			

Approaches and tools for security in software and hardware development and assessment (including open source)

Specific Conditions	
Expected EU Contribution per Project:	The Commission estimates that an EU contribution of between EUR XXX and XXX 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 XX million.
Type of Action:	Research and Innovation Actions (RIA)
Security Sensitive Topics:	Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Enhanced security frameworks for both hardware and software supply chains.
- Secure and trusted chip architectures for next-generation computing systems.
- Integrated security-by-design approaches in software development.
- Security testing methodologies, including AI-driven security testing methodologies.
- Standardized methodologies for hardware security assessment.

Scope: The increasing complexity and globalization of software and hardware supply chains introduce new vulnerabilities that cyber adversaries can exploit. Ensuring the security of both software and hardware components across the lifecycle of digital systems is paramount. innovative tools, methods, and processes to secure the entire ecosystem of software and hardware development.

a. Secured hardware systems over trusted Chips

The security of modern computing infrastructures relies heavily on the robustness of hardware components. This subtopic aims to develop robust security solutions for hardware platforms, focusing on secured microprocessors, secure boot mechanisms, and cryptographic acceleration. Proposals are also expected to address the risks of hardware-based vulnerabilities and backdoors, ensuring the security of devices from edge to cloud. Synergies with existing EU initiatives on trusted hardware (e.g., CHIPS JU, EuroHPC) are encouraged. The topic is expected to:

- Develop new architectures for tamper-resistant chips and processors. Exploring novel designs for secure microprocessors, leveraging hardware-level security enhancements, and integrating cryptographic co-processors for enhanced protection against tampering and side-channel attacks.
- Enhance supply chain transparency for chip production and integration. Exploring innovative ways to improve traceability and accountability in chip manufacturing processes, including methods such as secure hardware roots of trust, blockchain for tracking components, or certification mechanisms.
- Establish security-by-design methodologies for hardware security assessment. Advancing methodologies for systematic security testing of hardware components, including automated vulnerability analysis, verification frameworks, and integration of security assessment into chip design and lifecycle management.
- Develop self-healing firmware able to recover from cyber-attacks. Develop firmware able to leverage advanced anomaly detection, AI-driven threat mitigation and secure rollback mechanisms to automatically identify cyber-attacks, isolate compromised components restore the system to a trusted state while maintaining operational continuity.

b. Software Supply Chain security

The integrity of software supply chains is critical to mitigating cybersecurity threats such as supply chain attacks, dependency vulnerabilities, and compromised software components. This subtopic focuses on mitigating security risks in software supply chains, including secure code provenance, automated vulnerability detection, and secure software development lifecycle (SDLC) methodologies. Proposals should integrate AI-assisted security testing and formal verification approaches, leveraging standards like ISO/IEC 27036 for supply chain security. The topic is expected to:

- Develop innovative tools for real-time software vulnerability detection and automatic patching. Advancing the state of automated detection techniques, incorporating dynamic analysis, AI-driven pattern recognition, predictive analytics to proactively identify security weaknesses before exploitation and self-healing mechanisms.
- Enhance secure software frameworks. Exploring new methodologies for integrating security-by-design principles across development workflows, incorporating approaches

such as automated security policy enforcement, modular security components, and improved dependency management.

- Improve resilience against supply chain cyber threats. Investigating novel mitigation strategies, including provenance tracking for software components, secure update distribution mechanisms, enhanced anomaly detection, and multi-layer defense approaches to ensure integrity and trustworthiness.

Enhancing the Security and Robustness of AI Models and Systems (SecureAI)

Specific Conditions	
Expected EU Contribution per Project:	The Commission estimates that an EU contribution of between EUR XXX and XXX 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 XX million.
Type of Action:	Innovation Actions (IA)
Security Sensitive Topics:	Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Development of robust AI models capable of resisting adversarial manipulation.
- Improved methodologies for detecting and mitigating data poisoning and backdoor attacks.

Scope: The increasing reliance on AI in cybersecurity, critical infrastructure, and decision-making processes raises concerns about the security and robustness of AI systems. As AI models become more prevalent, they are increasingly targeted by adversarial attacks that manipulate inputs, compromise training data, or introduce hidden vulnerabilities. This topic aims to strengthen the resilience of AI systems and algorithms against various threats and attacks, such as enhancing their resilience against adversarial attacks, backdoor injections, and data poisoning. Proposals should develop real-time anomaly detection, and robust federated learning techniques, in synergies with leading efforts on AI transparency, and in compliance with the AI Act. The topic is expected to:

- Develop robust AI models resistant to adversarial attacks. Exploring techniques to harden AI models against adversarial perturbations, such as adversarial training, robust optimization, and defense mechanisms that enhance the trustworthiness of AI predictions.
- Improve detection of manipulated or poisoned training data. Advancing methodologies to identify and mitigate compromised datasets, leveraging techniques such as anomaly detection, provenance tracking, and automated data validation mechanisms.

Post-quantum cryptography

Specific Conditions	
Expected EU Contribution per Project:	The Commission estimates that an EU contribution of between EUR XXX and XXX 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 XX million.
Type of Action:	Research and Innovation Actions (RIA)
Security Sensitive Topics:	Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Development of quantum-resistant cryptographic primitives for enhanced security and privacy.
- Strengthened cryptanalysis and mathematical security validation methods.
- High-assurance post-quantum cryptography (PQC) implementations suitable for diverse applications.
- Integration of PQC into security architectures and protocols across multiple sectors.

Scope: As quantum computing advances, traditional cryptographic methods are at risk of becoming obsolete. The transition to quantum-resistant cryptographic systems is necessary to ensure long-term security and privacy in digital communications, identity management, and secure infrastructures. This topic aims to design, develop, and implement post-quantum cryptographic (PQC) solutions that address evolving security challenges while maintaining efficiency and interoperability. This topic focuses on transitioning to quantum-resistant cryptographic systems, supporting the emergence of advanced cryptographic primitives, from design to concrete implementations, such as:

- PQC for Enhanced Security and Privacy and Compliance in Digital Identity Systems. Investigating novel cryptographic schemes that ensure secure authentication, identity verification, and privacy preservation in alignment with regulatory frameworks.
- New Key Encapsulation Mechanisms and more compact and efficient signatures. Exploring new cryptographic primitives that balance security, performance, and usability in practical applications.
- PQC for Resilient Security and Privacy in Connected Collaborative Computing (3C) Networks. Developing quantum-resistant security measures for distributed computing environments, cloud-based services, and federated systems.
- Machine-checking of Security proofs, correctness of codes, absence of classes of side-channels + High-Assurance PQC + Audit and Maintenance of Critical Open-Source Security Software. Enhancing verification methods, automated proof-checking, and software assurance techniques to minimize implementation risks.
- Strengthening mathematical security validation and secure implementations Cryptanalysis. Advancing cryptanalysis research to validate and refine PQC schemes, ensuring robust protection against emerging threats.
- High-performance PQC (also includes PQC for resource-constrained devices). Investigating optimized cryptographic protocols for integration into constrained environments such as IoT, embedded systems, and mobile platforms.
- Integration into higher-level protocols. Research activities on how PQC solutions can be effectively embedded into widely used security standards, networking protocols, and digital transaction frameworks.
- Redefining Privacy in the new digital era. Examining the implications of PQC on data privacy, secure multiparty computation, and regulatory compliance in an evolving cryptographic landscape.

Emerging Challenges and Cyber Threats

Specific Conditions	
Expected EU Contribution per Project:	The Commission estimates that an EU contribution of between EUR XXX and XXX 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 XX million.
Type of Action:	Research and Innovation Actions (RIA)
Security Sensitive Topics:	Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Development of novel cyber threat analysis frameworks.
- Advanced detection mechanisms for AI-generated cyberattacks.
- Technologies and solutions to counter cyber and hybrid cyber-kinetic threats, particularly those targeting industrial IoT and automation systems.

Scope: The increasing sophistication of cyber threats, including AI-generated attacks and hybrid cyber-kinetic operations, presents significant risks to critical infrastructures, businesses, and individuals. This topic aims to develop innovative methods for detecting, analyzing, and mitigating emerging cyber threats, ensuring a more resilient and adaptive cybersecurity landscape. The topic focuses on novel cyber threats such as AI-generated cyberattacks and hybrid cyber-kinetic threats and on the development of advanced mechanisms to detect and respond to sophisticated attacks, including novel paradigms to develop resilient systems and infrastructures. The topic is expected to:

- Develop novel cyber threat analysis frameworks. Research on adaptive threat intelligence frameworks that leverage AI, big data analytics, and behavioral modeling to detect, predict, and respond to evolving cyber threats.

- Enhance detection mechanisms for AI-generated cyber-attacks. Investigating techniques to identify adversarial AI behaviors, synthetic attack vectors, and AI-driven misinformation campaigns that manipulate digital ecosystems.

- Develop technologies and solutions to counter cyber and hybrid cyber-kinetic threats, e.g. threats against industrial IoT and automation systems. Exploring multidisciplinary approaches to securing industrial IoT, automation systems, and cyber-physical infrastructures against coordinated cyber-kinetic attacks, leveraging techniques such as digital twins, anomaly detection, and self-healing security architectures.

6. Indirectly Managed Action by the ECCC (2027)

The Commission intends to conclude a contribution agreement with the European Cybersecurity Competence Centre (ECCC) for the implementation of Horizon Europe cybersecurity actions not co-funded by Member States, in accordance with Article 5(5) of Regulation (EU) 2021/8878. Further to the contribution agreement, the ECCC will launch a call for proposals in accordance with the specifications in the Appendix set out below. These include topics where participation will be limited in accordance with Article 22(5) of the Horizon Europe Regulation to legal entities established in Member States and Horizon Europe Associated Countries (eligible countries). In addition, for such topics, in order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, will not be eligible to participate.

The Commission intends to conclude a contribution agreement with the ECCC, in accordance with Article 5(5) of Regulation (EU) 2021/8878. In particular, the contribution agreement will entrust the ECCC with the implementation of a call for proposals according to the specifications in the Appendix set out below.

Legal entities: European Cybersecurity Competence Centre (ECCC), Polytechnic University of Bucharest, Strada Splaiul Independentei Nr.313, Sector 6, Bucharest 060042, Romania

Form of Funding: Indirectly managed actions

Type of Action: Indirectly managed action

Indicative budget: EUR … million from the 2027 budget

APPENDIX – Indirectly managed action by the ECCC

Specifications of the 'Increased Cybersecurity' call to be launched by ECCC

Call - Increased Cybersecurity

HORIZON-CL3-2027-02-CS-ECCC

Conditions of the call[88]

Proposals are invited against the following topic(s):

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[89]	Indicative number of projects expected to be funded
		2027		
Opening: April 2027 (tentative) Deadline(s): September 2027 (tentative)				
AI for Cybersecurity applications	RIA			

[88] The Executive Director-of the ECCC may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Executive Director of the ECCC 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 2025.

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

Privacy Enhancing Technologies	IA			
Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)	IA			
Emerging challenges: Human aspects of Cybersecurity	RIA			
Post-quantum cryptography	TBC			

AI for Cybersecurity applications

Specific Conditions	
Expected EU Contribution per Project:	The Commission estimates that an EU contribution of between EUR XXX and XXX 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 XX million.
Type of Action:	Research and Innovation Actions (RIA)
Security Sensitive Topics:	Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Development of AI-driven solutions for real-time cyber threat detection.
- Advancement of adaptive AI systems that evolve with dynamic cybersecurity challenges.
- Support for Security Operation Centres (SOCs) and Cyber Hubs with AI-enhanced capabilities.

Scope: Artificial Intelligence (AI) is increasingly utilized in cybersecurity for threat detection, incident response, and adaptive defense mechanisms. However, AI-driven systems themselves are susceptible to adversarial manipulation and bias. This topic aims to advance AI-based cybersecurity applications while ensuring that AI-driven solutions remain resilient, transparent, and compliant with regulatory frameworks such as the AI Act. In this context the topic explores the role of all flavours of AI, including generative AI, in cybersecurity applications, including automated threat detection, adaptive cyber defense, and AI-driven cyber threat intelligence. Proposals should develop solutions for trustworthy AI in cybersecurity contexts including addressing adversarial AI risks, in compliance with the provisions of the AI Act. The topic is expected to:

- Develop AI-driven solutions and tools for real-time cyber threat detection. Investigating novel machine learning techniques to detect anomalies, malicious activity, and AI-powered cyber threats in real time, improving situational awareness and response times.
- Develop adaptive AI systems capable of evolving with dynamic cybersecurity challenges. Exploring AI techniques that continuously learn from new cyber threats, adapting to emerging attack patterns while maintaining robustness and explainability.
- Support the future enhancements of Security Operation Centres/Cyber Hubs. Developing AI-enhanced SOC frameworks that integrate predictive analytics, automation, and threat intelligence to strengthen proactive defense measures.

Privacy Enhancing Technologies

Specific Conditions	
Expected EU Contribution per Project:	The Commission estimates that an EU contribution of between EUR XXX and XXX 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 XX million.
Type of Action:	Innovation Actions (IA)
Security Sensitive Topics:	Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Development of scalable and efficient privacy-enhancing technologies (PETs) that comply with data protection regulations.
- Strengthened user control over personal data through Privacy by Design and Privacy by Default approaches.
- Enhanced interoperability of security and privacy mechanisms across computing environments to support secure data-sharing frameworks.

Scope: Privacy-enhancing technologies (PETs) are crucial to ensuring data security and confidentiality while enabling responsible data sharing and processing. This topic aims to advance the state-of-the-art in privacy-enhancing technologies (PETs) by developing innovative solutions that protect individual privacy while enabling secure and responsible data usage. PETs such as secure multi-party computation (MPC), differential privacy, federated learning, and homomorphic encryption play a pivotal role in fostering trust in data-driven systems. Proposals should focus on delivering practical, scalable, and efficient mechanisms that uphold the highest standards of data protection, ensuring full alignment with the General Data Protection Regulation (GDPR) and related data protection frameworks. The topic is expected to:

- Develop scalable and efficient PETs that at the same time ensure compliance and alignment with relevant data protection frameworks. Exploring novel cryptographic techniques, privacy-preserving machine learning models, and federated data architectures that facilitate secure and lawful data processing.
- Promote Privacy by Design and by Default including technologies and solutions for enhancing user control over personal data. Exploring mechanisms such as differential privacy, zero-knowledge proofs, and secure multi-party computation to enhance user-centric privacy protections while maintaining usability.
- Enhance interoperability of measures across different computing layers and facilitate secure data sharing mechanisms that allow secure sharing of data between multiple parties without exposing sensitive information, also supporting the deployment of European Data Spaces.

Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

Specific Conditions	
Expected EU Contribution per Project:	The Commission estimates that an EU contribution of between EUR XXX and XXX 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 XX million.
Type of Action:	Innovation Actions (IA)
Security Sensitive Topics:	Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Enhanced resilience against distributed cyber threats and adversarial attacks targeting interconnected systems.
- Development of security solutions tailored for distributed computing systems including for example IoT and edge computing environments.
- Improved interoperability of security measures and cross-layer security.

Scope: This topic aims to advance security across the entire computing continuum, spanning IoT devices, edge computing, cloud infrastructures, and dataspaces. Proposals should address critical challenges such as ensuring data integrity in highly distributed and dynamic environments, implementing robust zero-trust architectures to secure interconnected and heterogeneous systems, and enabling comprehensive protection for sensitive data and processes. Solutions are expected to deliver tangible and measurable security improvements across all layers of the continuum, prioritizing scalability, interoperability, security and resilience against emerging threats. The topic is expected to:

- Develop security solutions for edge to cloud. For example, investigating lightweight cryptographic techniques, zero-trust architectures, and decentralized security models to ensure end-to-end protection from edge to cloud.
- Enhance interoperability of security measures across different computing layers. Exploring standardized security protocols, identity and access management solutions, and cross-domain authentication mechanisms to seamlessly integrate security controls across diverse computing ecosystems.
- Improve resilience against distributed cyber threats. Exploring anomaly detection, including AI-driven anomaly detection, intrusion prevention techniques, and automated response mechanisms to counter emerging threats targeting interconnected infrastructures and dataspaces.

Emerging challenges: Human aspects of Cybersecurity

Specific Conditions	
Expected EU Contribution per Project:	The Commission estimates that an EU contribution of between EUR XXX and XXX 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 XX million.
Type of Action:	Innovation Actions (IA)
Security Sensitive Topics:	Some activities resulting from this topic may involve using classified background and/or producing security-sensitive results (EUCI and SEN). Please refer to the related

	provisions in section B Security — EU classified and sensitive information of the General Annexes.

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

- Development of user-friendly and transparent cybersecurity technologies and solutions.
- Enhanced detection and mitigation strategies for social engineering attacks.
- Strengthened user and community awareness of cybersecurity risks and best practices.

Scope: Cybersecurity is not only a technological challenge but also a human-centered one. Threat actors increasingly exploit human vulnerabilities through social engineering, misinformation campaigns, and poor security awareness. Addressing the human aspects of cybersecurity requires interdisciplinary approaches that integrate psychological, sociotechnical, and behavioral models into security frameworks. This topic examines the intersection of cybersecurity and human factors, including social engineering attacks, behavioral cybersecurity, usable cybersecurity and decision-making in high-risk environments. Proposals should leverage psychological sociotechnical and sociolinguistic models to enhance cybersecurity awareness and resilience. The topic is expected to:

- Develop usable cybersecurity technologies and solutions. Exploring how human-centered design, behavioral cybersecurity, and cognitive sciences can contribute to the development of security tools that are intuitive, effective, and widely adopted by end-users.
- Improve detection and mitigation of social engineering attacks. Investigating adversarial behavioral analysis, including AI-driven behavioral analysis, automated phishing detection, and deception technologies to identify and neutralize social engineering threats.
- Develop solutions for enhancing user and community awareness of cybersecurity risks. Examining best practices for cybersecurity education, gamified learning environments, and awareness campaigns tailored to different user groups to foster a security-conscious culture.