CL3 Civil Security
Work Programme 2023-24
eli
EU:n Horisontti Eurooppa-ohjelman Siviiliturvallisuus-tutkimuksen v. 2023(-24) hakuaiheet

23.1.2023

Tampere

Pauli Stigell, Business Finland

HORISONTTI EUROOPPA

EU:N TUTKIMUS- JA INNOVAATIO-OHJELMA

Kolmas haku aukeaa kesällä 2023

- Haun speksaava TYÖOHJELMA on julkaistu Komission toimesta mutta sen hyväksyminen jäsenmaiden toimesta on kesken. Jäsenmaat ovat suivaantuneet turvallisuusohjelman budjettileikkauksista.
- Asia selkiytyy talven aikana – ohjelmasta leikattiin pois lukuisia hankeaiheita ja nyttemmin olisi tulossa korvaavia aiheita… 50 M€ ”lisää”

Eurooppalaisia hankkeita tavoitellaan

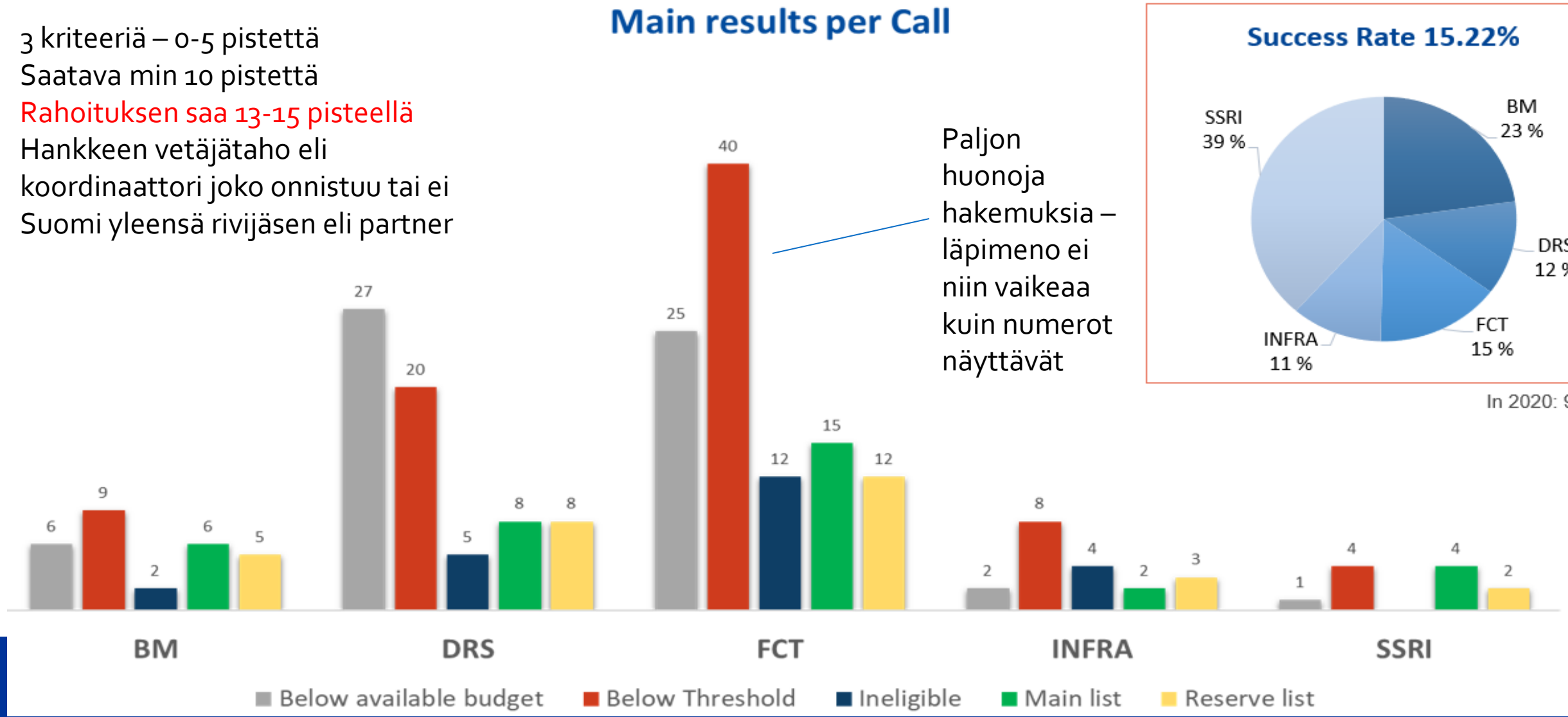
- This Cluster 3 Work Programme will support the implementation of EU policy priorities on security, including cybersecurity, and disaster risk reduction and resilience.

- The Work Programme will in particular support the implementation of Security Union Strategy, Counter-Terrorism Agenda, EU Strategy to tackle Organised Crime, EU Strategy on Combatting Trafficking in Human Beings, EU strategy for a more effective fight against child sexual abuse, EU Action Plan on firearms trafficking, border management and security dimensions of Pact on Migration and Asylum, EU Disaster Risk Reduction policies, EU Climate Adaptation Strategy, EU Maritime Security Strategy and EU Cybersecurity Strategy.

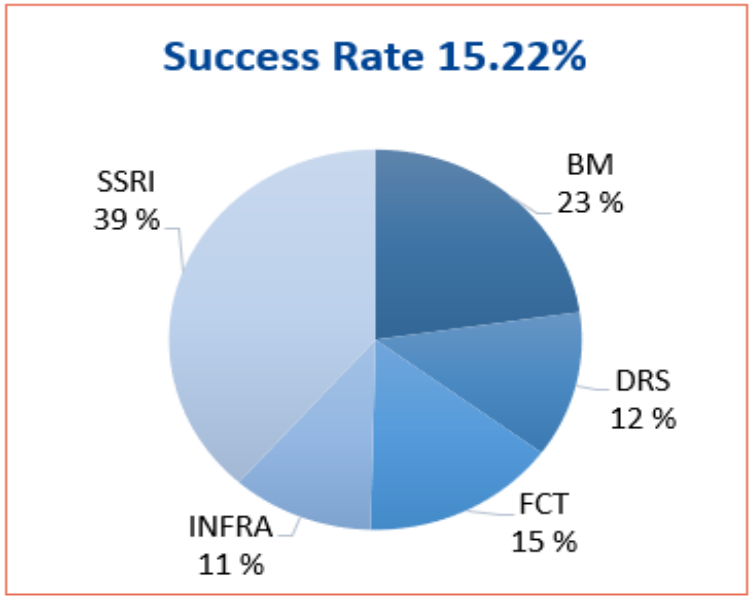
- Projects will develop new knowledge, technologies and/or other solutions to the identified requirements.
- Projects will **involve practitioner end-users** (usually relevant national authorities) alongside researchers and industry.
- *Projects need to show their contribution to a wider needs-driven capability development cycle that triggers research, steers its implementation and capitalises on its outcomes*

Evaluation Outcome Call 2021

3 kriteeriä – 0-5 pistettä
Saatava min 10 pistettä
Rahoituksen saa 13-15 pisteellä
Hankkeen vetäjätaho eli koordinaattori joko onnistuu tai ei
Suomi yleensä rivijäsen eli partner



Paljon huonoja hakemuksia – läpimeno ei niin vaikeaa kuin numerot näyttävät



In 2020: 9.5%

Evaluation criteria (RIAs and IAs)

Research and innovation action (RIA)

Activities to establish new knowledge or to explore the feasibility of a new or improved technology, product, process, service or solution.

This may include basic and applied research, technology development and integration, testing, demonstration and validation of a small-scale prototype in a laboratory or simulated environment.

Innovation action (IA)

Activities to produce plans and arrangements or designs for new, altered or improved products, processes or services.

These activities may include prototyping, testing, demonstrating, piloting, large-scale product validation and market replication.

EXCELLENCE

- ✓ Clarity and pertinence of the **project's objectives**, and the extent to which the proposed work is ambitious, and goes beyond the state-of-the-art.
- ✓ Soundness of the proposed **methodology**, including the underlying concepts, models, assumptions, inter-disciplinary approaches, appropriate consideration of the **gender dimension** in research and innovation content, and the quality of **open science practices** including sharing and management of research outputs and engagement of citizens, civil society and end users where appropriate.

IMPACT

- ✓ Credibility of the **pathways** to achieve the expected **outcomes and impacts** specified in the work programme, and the likely scale and significance of the contributions due to the project.
- ✓ Suitability and quality of the **measures to maximize expected outcomes and impacts**, as set out in the dissemination and exploitation plan, including communication activities.

QUALITY AND EFFICIENCY OF THE IMPLEMENTATION

- ✓ Quality and effectiveness of the **work plan**, assessment of risks, and appropriateness of the effort assigned to work packages, and the resources overall.
- ✓ Capacity and role of each **participant**, and extent to which the **consortium** as a whole brings together the necessary expertise.

Haut 2021-22

- Call 2021 toi 6 M€ (haku 216 M€) ja 23 hankeosallistumista.
- Call 2022 - tulokset saadaan tietoon maaliskuussa.
- 23.2. asti kysellään näkemyksiä vuosien 2025-27 hakuihin ja jopa seuraavan puiteohjelman (2028-34) sisältöön.
  - https://ec.europa.eu/eusurvey/runner/Horizon2020HorizonEuropeStrategicPlan2025-2027

Kuusi ”destinaatiota”

1. Destination – Better protect the EU and its citizens against **crime and terrorism**
2. Destination – Effective management of EU external **borders**
3. Destination – Resilient **infrastructure**
4. Destination – Increased **Cybersecurity**
5. Destination – A **Disaster**-Resilient Society for Europe
6. Destination – Strengthened Security Research and **Innovation**

Intérnational collaboration

Haku 2023

- **TOTAL 22 topics with 37 projects and 160 M€ budget**

• HORIZON-CL3-2023-FCT-01:	36 M€	6 topics	8 projects
• HORIZON-CL3-2023-BM-01	24 M€	4 topics	5 projects
• HORIZON-CL3-2023-INFRA-01	14 M€	2 topics	3 projects
• HORIZON-CL3-2023-CS-01	51 M€	3 topics	10 projects
• HORIZON-CL3-2023-DRS-01	28 M€	5 topics	6 project
• HORIZON-CL3-2023-SSRI-01	7 M€	2 topics	5 projects

- Open 29 June 2023
- Closes 23 Nobember 2023

- Calls 2021-22 were total 48 topics with 83 projects and 368 M€ budget

Fighting Crime and Terrorism

Matteo Messina Denaro is detained in Palermo, Sicily

Call - Fighting Crime and Terrorism 2023

- HORIZON-CL3-2023-FCT-01-01: Processing of large, complex and unstructured datasets resulting from criminal investigations, while reconciling big data analysis and data protection
  - Innovation Action – 7 M€ per project- 1 project

- HORIZON-CL3-2023-FCT-01-02: A harmonized European forensics approach on drugs analysis
  - IA - 4.5 M€ - 2 projects

- HORIZON-CL3-2023-FCT-01-03: New methods and technologies in service of community policing and transferable best practices
  - Research & Innovation Action - 4 M€ - 1 project

- HORIZON-CL3-2023-FCT-01-04: Open topic (teemassa**:** Increased security of citizens against terrorism**,** including in public spaces**)**
  - RIA - 4 M€ - 1 project

- HORIZON-CL3-2023-FCT-01-05: Crime as a service
  - RIA - 4 M€ - 1 project

- HORIZON-CL3-2023-FCT-01-06: Enhancing tools and capabilities to fight advanced forms of cyber threats and cyber-dependent crimes
  - RIA – 4 M€ - 2 projects

Call - Fighting Crime and Terrorism 2024

- **Call HORIZON-CL3-2024-FCT-01 : budget 34 M€ - deadline 20 Nov 2024**

- HORIZON-CL3-2024-FCT-01-01: Mitigating new threats and adapting investigation strategies in the era of Internet of Things
- HORIZON-CL3-2024-FCT-01-02: Open topic
- HORIZON-CL3-2024-FCT-01-03: Lawful evidence collection in online child sexual abuse investigations, including undercover
- HORIZON-CL3-2024-FCT-01-04: Radicalisation and gender
- HORIZON-CL3-2024-FCT-01-05: CBRN-E detection capacities in small architecture
- HORIZON-CL3-2024-FCT-01-06: Tracing of cryptocurrencies transactions related to criminal purposes

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

One Innovation Actions project - EUR 7 million
Eligibility criteria: This topic requires the active involvement, as beneficiaries, of **at least 3 Police Authorities** from at least 3 different EU Member States or Associated countries.

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

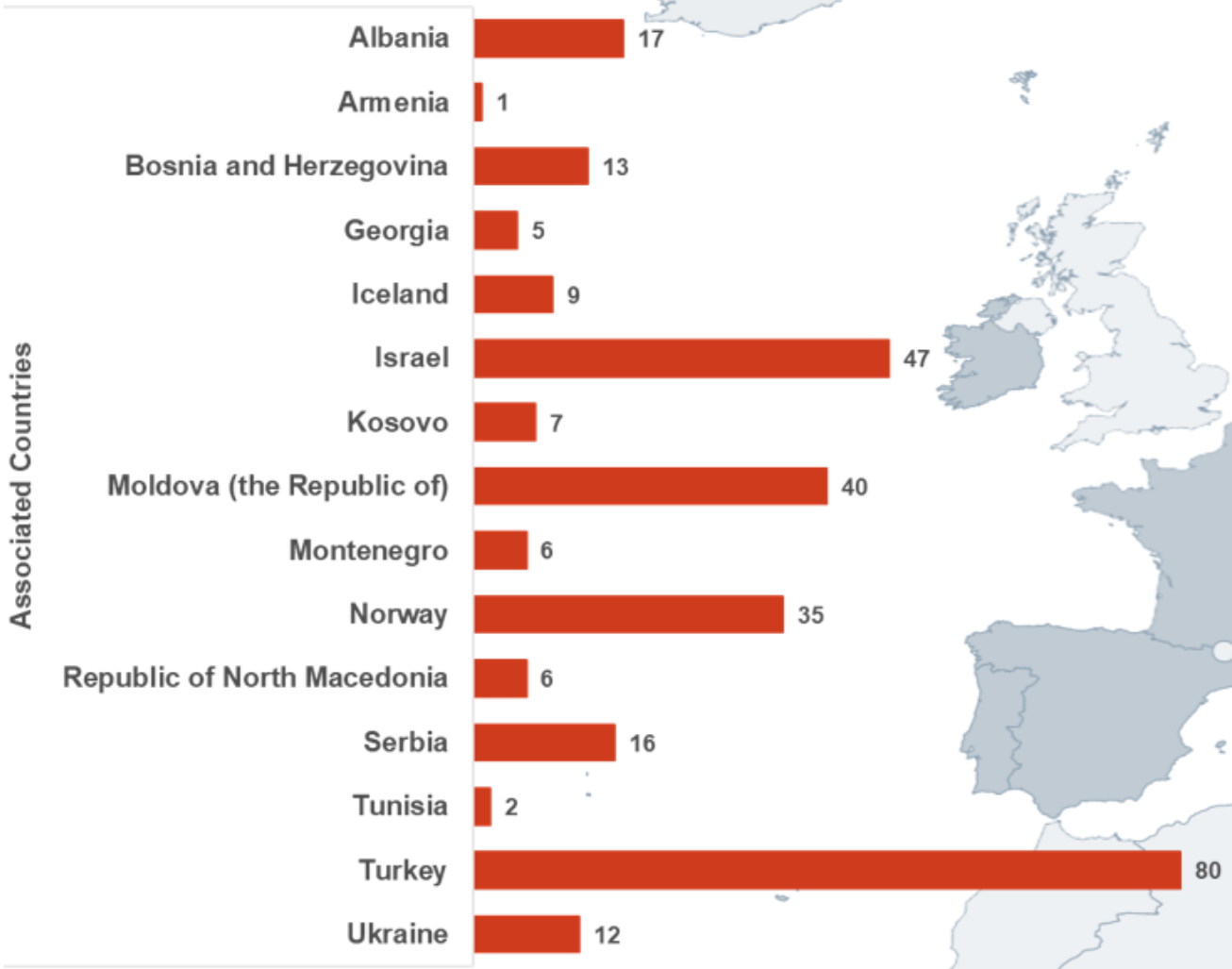
- Improved capabilities of European Police Authorities and other relevant security practitioners for a fast and flexible analysis of huge amounts of heterogeneous data through the application of robust and advanced tools, allowing them to efficiently fight criminals and terrorists who use novel technologies;
- Enhanced and modern analysis of heterogeneous data as well as training curricula that take **into account legal and ethical rules of operation, cost-benefit considerations**, as well as fundamental rights such as privacy and protection of personal data, providing reports that can be used in court;
- The work of European Police Authorities in the area of fighting crime and terrorism is supported by big data analysis that is in accordance with data minimisation principles and high privacy standards, with clearly identified challenges, adequate models and scientifically validated technical options for tackling the challenge proposed and solutions developed that meet the challenge.

Topicin määrittelytekstiin on vastattava. Jotkut hakijat ajavat topic-kuvauksen Word Cloud-ohjelmalla…

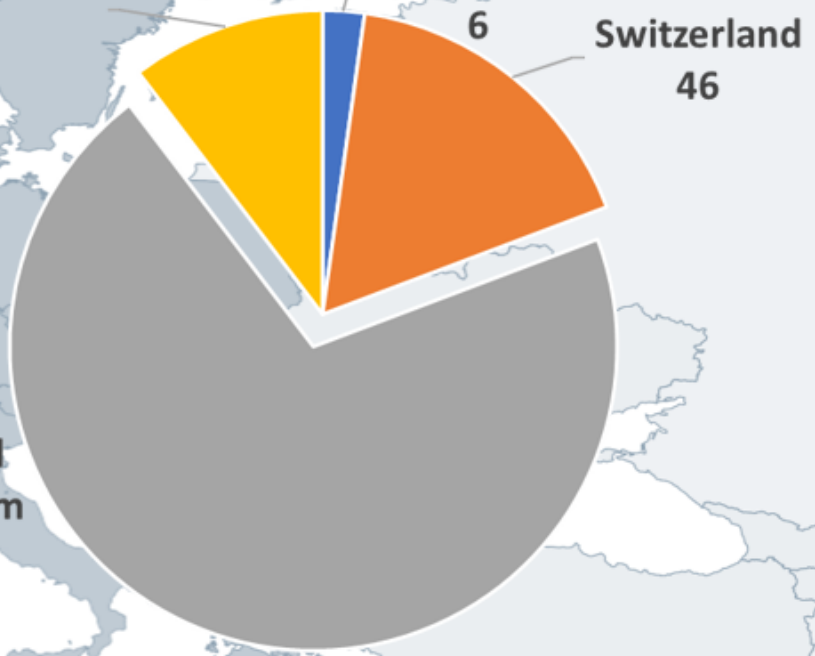
2021

Applications – Associated and Third Countries

296 applications from Associated Countries



270 applications from Third Countries



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

.

Scope:

With the constant increase of technological developments, the processing of large datasets is inevitable for police work in today's digital world.

In particular, there is a continuous need for handling large, complex and unstructured datasets, in order to gather, normalise, process, connect, prioritise, visualise the data (including text, image, audio and video) in ways that facilitate the extraction of actionable intelligence, while ensuring interoperability between existing systems and standards in different Member States.

Solutions to perform temporal and geospatial analyses are needed too. The successful proposal should have a clear strategy related to quality data sets to be used for training and testing.

The innovation efforts should provide support to web-based data analysis that can facilitate e.g. the fight against hate speech, human trafficking, terrorism or child sexual exploitation in an online environment.

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

.

…The work should include **surface, deep and dark web. Examples of relevant techniques include: examination of digitally captured signatures, identification of voice cloning and of deepfakes; detection and recognition of persons/objects/logos; speaker diarisation and identification; speech recognition and transcription into text; automatic classification of text based on risk factors; optical character recognition; named entity recognition; concept extraction, extraction of entities and relations between them in unstructured text; multimodal analytics, in order to discover insights and patterns in large volumes of data through clustering, as well as the identification of user communities and key actors in the social networks being formed online; automatic correlations among all available sources,** as well as cross-checking, cross-matching and mapping information between different cases.

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

.

In particular, key principles such as data minimisation should apply to ensure that Police Authorities conduct data analysis in full compliance with fundamental rights and EU privacy standards. For example, it may be necessary to filter and reduce large datasets to what is relevant for operational support activities and in investigations, and/or apply methods such as differential privacy. Possibilities of assessing and preventing bias and discrimination as a result of big data analysis should be analysed too. .

The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded project…

Possibilities of coordination with related activities funded through the Internal Security Fund (such as the European Anti-Cybercrime Technology Development Association) and the Digital Europe Programme should be analysed too.

HORIZON-CL3-2023-FCT-01-02: A harmonized European forensics approach on drugs analysis

2 x 4.5M€ IA project
The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of **at least 2 Police Authorities and 2 forensic institutes** from at least 3 different EU Member States or Associated countries.

Expected Outcome:

- European Police Authorities, forensic institutes and other relevant security practitioners are equipped by modern means of chemical analysis (composition) in drugs aimed at facilitating the cross-matching of seized drugs to labs and the establishment of links between cases.
- Improved and uniform EU-wide approach for the collection of evidence regarding illicit drugs-related overdoses, that would allow for choosing adequate responses in countering the drug-related problems;
- Improved collection and availability of forensic evidence, that could be used in court by the authorities, in direct violence, kidnapping or human trafficking cases, as well as reinforced prevention of such cases thanks to sensors/kits that are reliable, lawful, fast and easy-to-use;
- Enhanced perception of citizens in public and private spaces that Europe is an area of freedom, justice and security.

HORIZON-CL3-2023-FCT-01-02: A harmonized European forensics approach on drugs analysis

Scope: Proposals are expected to address one of the following options:
Option A: A harmonised European approach is needed on the study of chemical analysis (composition) in drugs, to

1) facilitate the cross-matching of seized drugs to labs and the establishment of links between cases, including by developing protocols to quickly exchange information on new substances;
2) tackle forensic challenges related to illicit drugs-related overdoses.

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

However, an obstacle in this process is the very limited or fully absent evidence, as it is the case in finding responses aimed at reducing overdose-related deaths. Namely, autopsies with full toxicology are underdeveloped in many Member States, making comparison at EU level difficult and aggregated numbers on overdose deaths not fully representative. Member States called to make this issue more comparable EU wide. To this end, a modern chemical analysis of the drugs composition and a unified EU-wide approach would provide a significant support, also in view of commitments of the EU Drugs Strategy 2021-2025.

HORIZON-CL3-2023-FCT-01-02: A harmonized European forensics approach on drugs analysis

Scope: Proposals are expected to address one of the following options:
Option B: A reliable and easy-to-use detection of chemical submission drugs in beverages and urine.

GHB (Gamma-hydroxybutyrate) is one of the drugs known as "club drugs" or "date rape drugs

Thus, Police Authorities and forensic practitioners need modern methods and technologies that enable better prevention against and investigation of different forms of violence and assault supported by these drugs. To this end, the successful proposal should aim at developing wearable, reusable, portable sensors and/or kits that would provide a fast response, without the need for additional instrumentation, and would be easy to use by Police Authorities in the field.

Gender-related impacts as well as legal and ethical challenges of such solutions should be fully considered in the development process.

HORIZON-CL3-2023-FCT-01-02: A harmonized European forensics approach on drugs analysis

Coordination among the successful proposals from this topic should be envisaged in order to avoid duplication and to exploit complementarities as well as opportunities for increased impact. Similarly, coordination with projects funded under HORIZON-CL3-2022-BM-01-03: Better, more portable and quicker analysis and detection for customs and HORIZON-CL3-2023-BM-01-04: Interoperability of systems and equipment at tactical level; between equipment and databases; and/or between databases of threats and materials would be welcome.

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.

HORIZON-CL3-2023-FCT-01-03: New methods and technologies in service of community policing and transferable best practices

One 4 M€ RIA project

The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities from at least 3 different EU Member States or Associated countries.

Expected Outcome:

- Strengthened resilience of local communities against crime and radicalisation, lowered feeling of insecurity and improved law enforcing;
- Negative factors in local communities are identified early, threats are detected, and crime reporting is enhanced;
- Better recognition for community diversity within neighborhoods…
- The interactions, and potential feedback between CP and alternatives to incarceration are explored;
- Identification and EU wide dissemination of validated community policing best practices;
- New methodologies, tools and adoption of technological support are developed;
- Training curricula for Police Authorities are developed on community policing in non-homogenous local milieus with social complexities, including balancing of majority needs while recognising expectations of minorities and/or sub-groups.

HORIZON-CL3-2023-FCT-01-03: New methods and technologies in service of community policing and transferable best practices

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

Scope
Community policing (CP) is an integral part of policing focusing on cooperation with local community for better understanding challenges and the given group needs and meeting them. Moreover, rapidly changing social, economic and political environment, both domestically and internationally, complicates these problems and fuels new tensions.

New approaches should cover internal review of Police Authorities' personnel training, possible change of attitudes and communication language, or countering existing misconceptions and biases. International exchange of validated best practices is encouraged.
Proposals should eventually integrate societal findings, relevant new or already existing technologies and legal framework into a comprehensive CP model. The successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects. Activities proposed within this topic should address both technological and societal dimensions of CP in a balanced way.

This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of the related innovation activities.

FCT04 – Increased security of citizens against terrorism, including in public spaces --- HORIZON-CL3-2023-FCT-01-04: Open topic

One 4 M€ RIA project

The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities from at least 3 different EU Member States or Associated countries.

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

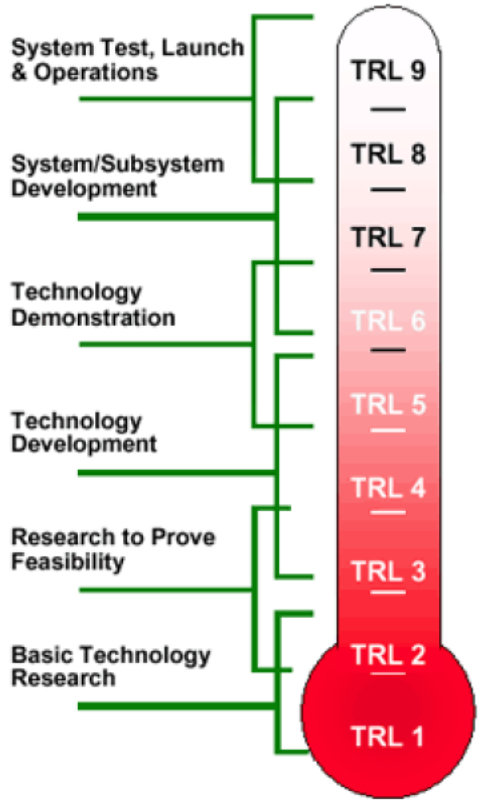
- Enhanced ability of security practitioners to identify and prevent emergent challenges in the terrorism-related topic under consideration;
- Harmonised and modern tools as well as procedures in the investigation of the terrorism-related problem under consideration, in full compliance with applicable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

Technology Readiness Level Defines Which Action Suits Your R&D Phase

TRL 1 – basic principles observed
TRL 2 – technology concept formulated
TRL 3 – experimental proof of concept

TRL 4 *– technology validated in lab*
TRL 5 *– technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)*
TRL 6 *– technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)* ***~"MVP"***
TRL 7 *– system prototype demonstration in operational environment* ***~"Pilot"***
TRL 8 *– system complete and qualified* ***~"Large-scale pilot"***

TRL 9 – actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)



Teknologian valmiustaso – NASA loi mittarin avaruuslentojen alkuaikoina. EU:ssa tutkimushanke (RIA) on tasolla 3-6, markkinaläheisempi IA-hanke TRL on korkampi, joskus 8 asti. Markkinaläheisiä rahoitetaan 70% tasolla (julkinen sektoria saa aina 100%), RIA 100%. 100% on osuus suorista kuluista, päälle 25% indirect costs (overhead).

HORIZON-CL3-2023-FCT-01-04: Open topic

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 citizens against terrorism, including in public spaces, that are not covered by the other topics of Calls Fighting Crime and Terrorism 2021-2022, Call Fighting Crime and Terrorism 2023 and Call Fighting Crime and Terrorism 2024.

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 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.

HORIZON-CL3-2023-FCT-01-05: Crime as a service

One EUR 4 million. Research and Innovation Actions project

This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities from at least 3 different EU Member States or Associated countries.

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

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

HORIZON-CL3-2023-FCT-01-05: Crime as a service

Scope:
The Crime-as-a-service (CaaS) model proliferates and becomes a prominent feature not only for the cybercriminal underground, but also for traditional criminals hiring specialised digital and financial services. Recently Malware-as-a-service (MaaS) offerings on the Dark Web increased, of which ransomware affiliate programs seem to be the most prominent.

The shape of the organised crime evolves, apart from traditionally closed, clandestine criminal structures, and investigators are increasingly confronted with modern, flexible, specialised and "multi-ethnic" organisations with a global operational range.

Actors in the shadow economy while seeking to maximise their profit, take instant advantage of new ways of operations, exploring and benefiting from modern technologies and organisational schemes to achieve their goals, thus resulting in dynamic transformation of subject networks.

Coordination among the successful proposal from this topic as well as with the successful proposals under topics HORIZON-CL3-2023-FCT-01-06: Enhancing tools and capabilities to fight advanced forms of cyber threats and cyber-dependent crimes and HORIZON-CL3-2024-FCT-01-06: Tracing of cryptocurrencies transactions related to criminal purposes should be envisaged to avoid duplication, and to exploit complementarities as well as opportunities for increased impact.

HORIZON-CL3-2023-FCT-01-06: Enhancing tools and capabilities to fight advanced forms of cyber threats and cyber-dependent crimes

Two 4 M€ RIA projects.

The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 Police Authorities from at least 3 different EU Member States or Associated countries.

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

- Development of modular toolbox for Police Authorities, facilitating gathering and processing of data relevant for cybercrime and cyber - enabled crime investigations;
- Detection of crypto-jacking, compromised registration forms, malware attacks and other cybercrimes perpetrated using cryptocurrencies;
- Development of training curricula, for Police Authorities, prosecutors, as well as judicial actors on major contemporary cybercriminal activities;
- Recommendations on public cybercrime awareness actions contributing to early detection and 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.
- Identification of best practices of international law enforcement and judicial cooperation networks
- Development of multi-stakeholders strategies, including novel investigation schemes and information sharing mechanisms.

HORIZON-CL3-2023-FCT-01-06: Enhancing tools and capabilities to fight advanced forms of cyber threats and cyber-dependent crimes

Scope:
While cyber-attacks, notably ransomware and distributed denials or services, are getting more sophisticated, law enforcement officers need to develop strategies to gain a comprehensive knowledge of the numerous elements contributing to the attack (Virtual Private Networks - VPNs, Bulletproof Hosting – BPH, Remote Access Trojans – RATs, botnets, Dark Web platforms, crypto-ransomware, Criminal Phone Banks, Pseudonyms, Advanced Persistent Threat groups – APTs, Internet infrastructure abuse (e.g. DNS), etc.).

As geographical boundaries become irrelevant in the commission of crime, criminal investigations have to become cooperative, joint actions. It does not seem feasible for a comprehensive investigation of contemporary organised crime to be conducted by a single investigator or even a single force.

Development of multi-stakeholders strategies, including novel investigation schemes and information sharing mechanisms, is necessary in order to enhance prevention and deterrence of these forms of cyber and cyber-dependent crime.

Project should also investigate the legal background and identify any related shortcomings so lawful access and processing of subject data has a valid legal foundation.


Border Management 200 BC

Call - Border Management 2023

- HORIZON-CL3-2023-BM-01-01: Capabilities for border surveillance and situational awareness
  - One 7 M€ IA project
- HORIZON-CL3-2023-BM-01-02: Identify, inspect, neutralise Unexploded Ordnance (UXO) at sea
  - One 4,9 M€ RIA project.
- HORIZON-CL3-2023-BM-01-03: Beyond the state-of-the-art "biometrics on the move" for border checks
  - One EUR 5 million Innovation Actions Project
- HORIZON-CL3-2023-BM-01-04: Interoperability of systems and equipment at tactical level; between equipment and databases; and/or between databases of threats and materials
  - One EUR 6 million Innovation Actions project.

Call - Border Management 2024

- HORIZON-CL3-2024-BM-01-01: Interoperability for border and maritime surveillance and situational awareness
- HORIZON-CL3-2024-BM-01-02: Advanced user-friendly, compatible, secure identity and travel document management
- HORIZON-CL3-2024-BM-01-03: Integrated risk-based border control that mitigates public security risk, reduces false positives and strengthens privacy
- HORIZON-CL3-2024-BM-01-04: Detection and tracking of illegal and trafficked goods

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

One 7 M€ IA project

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.

Eligible costs will take the form of a lump sum.

Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN).

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

- Increased border surveillance capabilities, better performing and more cost-efficient, with data and fundamental rights protection by design;
- Better surveillance of border areas, supporting fight against illegal activities across external borders, as well as safety of people and operators in the border areas, including favouring border crossings through border crossing points;
- More efficient and more flexible solutions (including for relocation, reconfiguration and rapid deployment capabilities) than physical barriers to deter and monitor irregular border crossings outside border crossing points.

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

Scope

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

The border surveillance capabilities' needs along borders may change in time, often just within a year or a season, and/or allow to respond and adapt within a relatively short notice. Solutions should hence allow re-orienting capacity and resources accordingly (through physical portability and/or other approaches).

Cooperation for surveillance along borders requires compatibility and interoperability among legacy and planned systems. Proposed solutions should allow higher interoperability cross-border among EU and Associated Countries practitioners, cross-systems and across the multiple authorities.

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

Compatibility and integration with the European Border Surveillance System (EUROSUR) is essential, and compatibility and/or exploitation of other information sharing environments, including the Common Information Sharing Environment (CISE) would be an additional asset. Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): networked deployable, and possibly mobile, semi-autonomous surveillance towers; IoT and advanced mesh connectivity; Virtual and Augmented Reality for enhanced C2 and situational awareness; integrated wide area RPAS management; advanced sensors for geolocalisation; passive, low-energy systems; artificial intelligence.

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

Proposals submitted under this topic are expected to address the priorities of the European Border and Coast Guard and of its Agency (Frontex). This should start from the definition of requirements and the design phase of their work, including basing on the EBCG Capability Roadmap when available; and on the engagement with the Agency during the implementation of the project.

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

One 4,9 M€ RIA project.

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.

Eligible costs will take the form of a lump sum.

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

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

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

Scope:
A large amount of Unexploded Ordnance (UXO), estimated by experts in the tens of thousands of tons, lay in European seas and often close to European shores. Most of this material dates back to World War I and World War II.. These security threats could be linked directly to maritime security and infrastructures (to deny or ransom a port, for example), or be moved towards other illicit acts.

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

The proposed project should improve civilian capabilities on:

1. enabling existing knowledge (mapping and integrating data from historical maps and more recent data, including reports from sea operators); comparative analysis of legislation, roles and responsibilities in Member States;
2. detecting UXO on and below the marine sediment/seabed, in order to detect also buried objects;
3. identifying, classifying, assessing (identifying chemical and material aspects; sensing levels of corrosion);
4. inspecting and handling (grab and manipulate UXO under water, from intact shells to chunks to small parts; collect and recovery);
5. neutralising and disposing (containment of chemical spill overs and possible explosions).

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

Research projects should consider results and recommendations from the European Commission's 2022 "Study on underwater unexploded munitions: final report". Research projects should consider, build on and not duplicate previous research or findings of previous work.

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

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

Two EUR 3.00 million Research and Innovation Actions projects.

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.

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

- Updated, European-based, knowledge and development on robust biometrics technologies that could be used for recognition (identification and verification) of people crossing external EU borders, demonstrating a clear advancement beyond the current state-of-the-art;
- Maximisation of travellers' experience and of security reassurances, minimising handling of personal data and maximising accuracy, reliability and throughput of the recognition process;
- Contribution to improving the operational response capacity of the EBCG at border crossing points and to capabilities that strengthen the Schengen area, by providing security at its external borders that also reassure on maintaining the free movement within its borders.

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

Scope

Biometrics are one of the most usable and most reliable ways to validate the identity of an individual. Biometrics that are traditionally used in the context of border controls include fingerprints and 2D facial images; other biometrics are also used for identity management outside the European Union, or at national level, such as iris; and further others are used in other applications in the private sector and in consumer market.

As for many other technologies, applications of biometrics to improve capabilities in civil security, such as in the border management or law enforcement sectors, may have higher requirements than applications in the consumer market. This applies to the requirements on reliability, usability, scalability, throughput and strict minimization of risks to personal data protection and fundamental rights (including the elimination or minimisation of any risk of bias or discrimination).

Research should assess and develop the fit-for-purpose border management of biometric identification modalities beyond fingerprints and facial images, and/or innovative modalities of acquisition of those and other biometrics.

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

Any innovation in biometrics shall imply clear improvements on acquisition, processing and validation, compared to the state-of-the-art, "on-the-move" (i.e. while the travellers are moving and without cooperation from them), contactless and with stand-off biometric capturing from long-distances (ideally, but not mandatorily, more than 10 meters), and/or of when multiple travellers cross borders, on foot or inside the same vehicle. The solutions should also take into account the different nature and scenarios of BCP operations (e.g. open-air conditions, night, time, time constraints, space constraints, etc).

The proposed solution(s) should address modular integration with health checks – such as in the case of pandemics – as well as checks on people's temperature. At system-level, emphasis should be given to automated border check for the purpose of guiding travellers on-the-move while performing the seamless biometric acquisition.

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

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

Examples of technologies and approaches that can be explored by the research projects include (non-prescriptive and non-exhaustive): 3D facial images, contactless friction-ridge biometrics (i.e. fingerprint, palmprint and finger-knuckle-print), iris recognition from long distances, palm vein, periocular biometrics, novel algorithms embedding artificial intelligence as well as advanced hardware components like sensors, traveller tracking systems for high-quality on-the-move biometric acquisition, safe single wavelength or multispectral light sources (for the illumination of subjects) and document verification subsystems.

Proposals submitted under this topic are expected to address the priorities of 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).

The funded projects will likely have the opportunity of exploiting the core capabilities of the "Border Management Innovation Centre" (BoMIC), Frontex's future collaborative physical space for testing, demonstration, simulation and assessment of border-check prototype systems, processes and procedures with a focus on human-machine interaction and emulation of real operational environments.

HORIZON-CL3-2023-BM-01-04: Interoperability of systems and equipment at tactical level; between equipment and databases; and/or between databases of threats and materials

One EUR 6 million Innovation Actions project.

Eligible costs will take the form of a lump sum

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

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

HORIZON-CL3-2023-BM-01-04: Interoperability of systems and equipment at tactical level; between equipment and databases; and/or between databases of threats and materials

Scope

European customs, as all operators and citizens, also work in our digitalised and interconnected world of equipment, systems, and data. On the one hand, this opens opportunities to harness their capacity to facilitate trade while protecting the security and safety of citizens and benefiting the EU's economy. Furthermore, the strategy of the "European custom union acting as one" implies that other authorities beyond customs use that same equipment. It also means that equipment, including mobile one, is shared among Member States to increase cooperation and collaboration on checking flows of goods across European borders.

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


Resilient Infrastructure

Call - Resilient Infrastructure 2023

- HORIZON-CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services
  - One EUR 5 million Innovation Actions Project
- HORIZON-CL3-2023-INFRA-01-02: Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures
  - Two EUR 4.70 million IA projecs.

Call - Resilient Infrastructure 2024

- HORIZON-CL3-2024-INFRA-01-01: Resilient and secure urban planning and new tools for EU territorial entities
- HORIZON-CL3-2024-INFRA-01-02: Advanced real-time data analysis used for infrastructure resilience

HORIZON-CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services

One EUR 5 million Innovation Actions Project
This topic requires the active involvement, as beneficiaries, of at least 3 government entities responsible for security, which could include civil protection authorities, at national level from at least 3 different EU Member States.
Eligible costs will take the form of a lump sum

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

- Tools for EU Member State authorities and operators for the assessment and anticipation of relevant risks to the provisions of essential services are identified;
- The cooperation between authorities is facilitated by providing solutions for data exchange and joint cross-border risk assessments;
- Simulation tools are developed for large-scale exercises to test the resilience of operators and of specific sectors, and related training courses are designed;
- Measures by Member State authorities to facilitate risk assessments by operators are identified, including the assessment of dependencies on different sectors and cross-border interdependencies;
- Provide common European guidance and support for the drafting of resilience plans in order to meet provisions of the proposed CER-Directive: risk analysis, domino effects, cross-sector and cross-border analysis, standardised plans, training tools;
- An all-hazards framework is created to support Member States in ensuring improved concepts and instruments for the anticipation of risks to entities that provide essential services, resulting in an improved preparedness and response against disruptions of key sectors in the EU and enhanced resilience of the EU internal market.

HORIZON-CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services

Scope:

The EU Security Union Strategy for 2020-2025, Counter-Terrorism Agenda for the EU and the Cyber Security Strategy stress the importance of ensuring resilience in the face of various risks. The livelihoods of European citizens and the good functioning of the internal market depend on the reliable provision of services fundamental for societal or economic activities in many different sectors. Those services often are reliant upon one another, thus disruptions in one sector can generate severe and long-lasting effects on the provision of services in others.

Proposals should aim to cover the largest possible number of sectors described in the respective Annexes of the [proposals for a] directive on the resilience of critical entities (CER) and the directive on measures for high common level of cybersecurity across the Union (NIS-2).

Projects are expected to outline how results are fed into the work of relevant Commission expert groups – [for example the Critical Entities Resilience Group (CERG) and the NIS-2 Cooperation Group] – and to explore synergies with the actions undertaken by relevant EU agencies.

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

Two EUR 4.70 million IA projecs.
Eligible costs will take the form of a lump sum

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

- Support is provided to the resilience of operators against cyber and non-cyber threats in specific sectors;
- A reliable state-of-the-art analysis of physical/cyber detection technologies and risk scenarios is created, in the context of an operator in a specific sector in sectors that have not yet been covered by previous research projects;
- Strengthened cooperation against natural or human-made threats and subsequent disruptions of infrastructures in Europe, allowing for operational testing in real scenarios or realistic simulations of scenarios with specific regard to disruptions in a specific sector of critical entities;
- Improved situational awareness, preparedness and governance by the implementation of effective solutions that enhance detection and anticipated projection of a determined threating situation, as well as implementation of prevention, preparedness/mitigation, response, and recovery types of intervention;

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

Scope

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

A disruption affecting the service provision by one operator in one sector has the potential to generate cascading effects on service provision in other sectors

A possible project focusing on the protection of critical infrastructures against such threat should consider gaps and vulnerabilities that need to be identified and overcome (e.g. protection of drinking water supply systems from high chemical levels, nuclear facilities, etc.).

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

The successful proposal, following a sector-based approach and identifying a specific priority sector, should work on how to increase the combined cyber and non-cyber resilience operators. It should do so by orienting itself on sectors that have not been covered in previous research, out of the list of sectors described in the respective Annexes of the of the [proposals for a] directive on the resilience of critical entities (CER) and the directive on measures for high common level of cybersecurity across the Union (NIS-2) and thus contribute to enhancing the overall resilience on EU-level, in line with the EU Security Union Strategy.

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

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.

Disaster-Resilient Society

(大東京シン害火災の實況)　淺草公園六區燒ア ト

Call - Disaster-Resilient Society 2023

- HORIZON-CL3-2023-DRS-01-01: Improving social and societal preparedness for disaster response and health emergencies
  - Two EUR 4 million Research and Innovation Actions projects
- HORIZON-CL3-2023-DRS-01-02: Operability and standardisation in response to biological toxin incidents
  - One EUR 6 million Research and Innovation Actions project.
- HORIZON-CL3-2023-DRS-01-03: Internationally coordinated networking of training centres for the validation and testing of CBRN-E tools and technologies in case of incidents, with consideration of human factors
  - One EUR 4 million Innovation Actions project.
- HORIZON-CL3-2023-DRS-01-04: Robotics: Autonomous or semi-autonomous UGV systems to supplement skills for use in hazardous environments
  - One EUR 6 million Research and Innovation Actions project
- HORIZON-CL3-2023-DRS-01-05: Increased technology solutions, institutional coordination and decision-support systems for first responders of last-kilometer emergency service delivery
  - One EUR 3.50 million Research and Innovation Actions project.

Call - Disaster-Resilient Society 2024

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

- HORIZON-CL3-2024-DRS-01-02: Harmonised / Standard protocols for the implementation of alert and impact forecasting systems as well as transnational emergency management in the areas of high-impact weather / climatic and geological disasters

- HORIZON-CL3-2024-DRS-01-03: Hi-tech capacities for crisis response and recovery after a natural-technological (NaTech) disaster
- HORIZON-CL3-2024-DRS-01-04: Cost-effective sustainable technologies and crisis management strategies for RN large-scale protection of population and infrastructures after a nuclear blast or nuclear facility incident

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

Two EUR 4 million Research and Innovation Actions projects

This topic requires the active involvement, as beneficiaries, of at least 3 organisations representing citizens or local communities, practitioners (first and/or second responders), and local or regional authorities and private sector from at least 3 different EU Member States or Associated countries.

Expected Outcome:

- Identification of different factors in inequality and ways to communicate with vulnerable groups, of individual, organisational, and systemic resilience factors and pathways to support these, and of ways to address vulnerabilities in acute crisis as well as during prevention, in order to elaborate an interconnectedness of resilience and vulnerability;
- Improvement of populations health literacy and basic understanding of how medicine and vaccines work and how they are developed and produced;

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

Expected Outcome:

- Putting the citizen at the centre of the crisis management process, increasing their capacity to access, read and interpret scientifically sourced information, analysing gender behaviors regarding unpopular measures (e.g., quarantine) and vaccination attitudes and identification and relieving of barriers for vaccination readiness:
- Incorporation of information technology and bias-free data processing into crisis management through improved information processing in transformative governance, illustrating possibilities, challenges, and limits of digitalisation and enabling usage of data for political decision making;
- Incorporation of machine learning and artificial intelligence in governance and political decision making based on interdisciplinary discussions on definitions on problems; areas of application; and definition of responsibilities and competences in data governance;
- Validation of novel, smartphone sized or wearable technologies with laboratory-level diagnostics capability (e.g., wearables with integrated digital dosimeters, handheld PCR test devices);

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

Scope:

Challenges during the pandemic included difficulties of working with protective gear such as insecurities and usage mistakes; additional disadvantages for vulnerable groups among others due to communication issues; and lack of local cooperation and prevention regarding equipment, stocks, and coordination.

Currently, different groups are not reached equally by public communication efforts. Risk communication especially fails to contact vulnerable groups. Social inequalities are present in different forms and on different levels. On the other hand, resilience can protect against negative effects of crises.

HORIZON-CL3-2023-DRS-01-02: Operability and standardisation in response to biological toxin incidents

One EUR 6 million Research and Innovation Actions project.

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

- Improved European crisis management in case of an incident with biological toxins through the development of a pan-European task force of security practitioners, taking into consideration existing intersectoral actions on bioterrorism;
- New and existing portable devices, technologies and methods for responders to perform on-site detection of biological toxins are brought to the market;
- Recommendations of effective decontamination measures for personnel, equipment and facilities exposed to biological toxins are provided based on solid experimental testing;
- Development of an operational European response network of specialised and forensic laboratories, taking into account existing initiatives such as e.g. the HERA Laboratory Network and harmonised procedures/guidelines for forensic analysis of biological toxins applicable to a range of relevant technologies and toxins;
- The risks for responders from exposure to biological toxins in the hot-zone are assessed and recommendations of protective equipment for working with biological toxins in the hot-zone are developed;
- Building on existing initiatives and networks, a consolidated platform is established providing support for standardisation efforts in the analysis of biological toxins.

HORIZON-CL3-2023-DRS-01-02: Operability and standardisation in response to biological toxin incidents

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

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

This action is also expected to engage with the European Health Emergency Preparedness and Response Authority (HERA).

HORIZON-CL3-2023-DRS-01-03: Internationally coordinated networking of training centres for the validation and testing of CBRN-E tools and technologies in case of incidents, with consideration of human factors

One EUR 4 million Innovation Actions project.

This topic requires the active involvement, as beneficiaries, of:

- at least 3 Training Centres located in the European Union;
- In addition, the consortium must include at least 2 CBRN Centres of Excellence from targeted non-associated third countries;
- and representatives of scientific stakeholders involved in training, validation and testing of CBRN-E tools and technologies and end-users (both practitioners and policymakers).

HORIZON-CL3-2023-DRS-01-03: Internationally coordinated networking of training centres for the validation and testing of CBRN-E tools and technologies in case of incidents, with consideration of human factors

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

- Extended networking of training centres in Europe and selected CBRN Centres of Excellence in non-EU countries;
- Compilation of information of capacities of networked CBRN-E training centres in view of better coordination of training and testing actions in support of research and standard developments;
- Improved cooperation and development of testing methodologies and protocols for the validation of tools and technologies resulting from research actions and proofs of concepts for developing standards, combining societal and technological challenges;
- Inter-cooperation through an established forum of training centres to synchronize actions for identifying gaps in test and validation techniques, methodologies and protocols.

HORIZON-CL3-2023-DRS-01-03: Internationally coordinated networking of training centres for the validation and testing of CBRN-E tools and technologies in case of incidents, with consideration of human factors

Scope:
In case of a CBRN-E incident, it is of outmost importance that personnel involved in handling the situation, i.e., rescue services and polices, are well educated and trained and that they are using equipment and tools that are reliable with validated capabilities.

To achieve a more robust and consistent opportunity to practice, test and evaluate CBRN-E tools and technologies within Europe and beyond, it is necessary to strengthen networking of existing training and testing facilities and centres and to extend it to relevant CBRN Centres of Excellence located in non-EU countries.

This will indicate what type of facilities are ready to be used for specific training / validation needs and which developments are required to strengthen the testing end exercise capabilities to be better prepared in the event of a CBRN-E incident. It will also give the existing centres a possibility to cooperate to compare, enhance, develop and extend the range of tests, exercises and training to achieve a robustness that will benefit the whole European CBRN-E community. Along validation / testing actions, training exercises should consider societal aspects (vulnerable groups, human factors) in combination of CBRN technological response in case of an incident. It should be considered

HORIZON-CL3-2023-DRS-01-04: Robotics: Autonomous or semi-autonomous UGV systems to supplement skills for use in hazardous environments

One EUR 6 million Research and Innovation Actions project

The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 first responders' organisations or agencies and representatives of local or regional authorities in charge of managing hazardous environmental sites from at least 3 different EU Member States or Associated countries.

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

- Broad acceptance of autonomous systems by first responders and affected people in civil protection;
- Higher safety and security standards for operational forces working in hazardous environments;
- Get ahead of future shortcomings of trained first responder personnel by increasing first responder efficiency
- Increased ability to conduct on-scene operations remotely without endangering first responders;
- European robotics industry is strengthened through engagement in the civil protection research as well as an economic and political advantage through building up know-how for innovative technologies;
- Reduction of false positive redouts from various sensors carried by robots.

- In order to achieve the expected outcomes, international cooperation is encouraged.

HORIZON-CL3-2023-DRS-01-05: Increased technology solutions, institutional coordination and decision-support systems for first responders of last-kilometer emergency service delivery

One EUR 3.50 million Research and Innovation Actions project.

The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 first responders' organisations or agencies and representatives of local or regional authorities in charge of disaster response from at least 3 different EU Member States or Associated countries.

Expected Outcome:

- Identification and evaluation of existing technologies supporting first and second responders in their immediate response to natural disasters (e.g. drones, AI, sensors), highlighting their strengths and weaknesses;
- Testing and implementation of most promising user-centred technologies in real-world conditions;
- Innovative technology solutions to improve searching operations in smoky environments in the case of wildfires.

HORIZON-CL3-2023-DRS-01-05: Increased technology solutions, institutional coordination and decision-support systems for first responders of last-kilometer emergency service delivery

Scope:

Supplying relief items to various demand spots in disaster-prone areas is a critical task due to last-kilometer logistics problems that hamper the process of and efficient transportation of first responders and their equipment.

Blocked roads, heavy terrain and bad weather conditions are factors that are faced by first and second responders (e.g. fire brigade, emergency medical services) in the immediate response to disasters. Innovative technologies (e.g. drones, AI, sensors etc.) are considered to support emergency workers in overcoming challenges related to relief items delivery without endangering responders.


Increased Cybersecurity

Call - Disaster-Resilient Society 2023

- HORIZON-CL3-2023-CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)
  - Budget 23 M€ - per one IA project 4-6 M€
- HORIZON-CL3-2023-CS-01-02: Privacy-preserving and identity management technologies
  - Budget: 15,7 M€ - 2 to 4 M€ per project – IA type
- HORIZON-CL3-2023-CS-01-03: Security of robust AI systems
  - Per project EUR 4 and 6 million -- Budget EUR 12 million.

Call - Increased Cybersecurity 2024

- HORIZON-CL3-2024-CS-01-01: Approaches and tools for security in software and hardware development and assessment
- HORIZON-CL3-2024-CS-01-02: Post-quantum cryptography transition

HORIZON-CL3-2023-CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

Budget 23 M€ - per one IA project 4-6 M€

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

- Tools to support cybersecurity resilience, preparedness, awareness, and detection within critical infrastructures and across supply chains;
- Cloud infrastructures vulnerabilities mitigation;
- Secure integration of untrusted IoT in trusted environments;
- Use of Zero-Trust architectures;
- Trust & Security for massive connected IoT ecosystems & lifecycle management;
- Secure interoperability and integration of systems;
- AI-based automation tools for cyber threat intelligence;
- Secure infrastructure, secure Identities and usability for a security chain covering communication, data collection, data transport, and data processing.

HORIZON-CL3-2023-CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

Scope

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

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.

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

Budget: 15,7 M€
2 to 4 M€ per project – IA type
Eligible costs will take the form of a lump sum

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

- Improved scalable privacy-preserving and identity management technologies for federated and secure sharing and for processing of personal and industrial data and their integration in real-world systems;
- Improving privacy-preserving technologies for cyber threat intelligence and data sharing solutions;
- Privacy by design;
- Contribution to promotion of GDPR compliant European data spaces for digital services and research, Contribution to the promotion of eID Regulation compliant European solutions;
- Research and development of self-sovereign identity management technologies and solutions;
- Provide resource efficient and secure digital identity solutions for Small and medium sized enterprises;
- Strengthened European ecosystem of open-source developers of privacy-preserving solutions;
- Usability of privacy-preserving and identity management technologies.

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

Scope

Using big data for digital services and scientific research brings about new opportunities and challenges. For example, machine-learning methods process medical and behavioural data in order to find causes and explanations for diseases or health risks. However, a large amount of this data is personal data. Leakage or abuse of this kind of data, potential privacy risks and identity compromises pose threats to individuals, society and economy.

Advanced privacy-preserving technologies such as, for example, cryptographic anonymous credentials, homomorphic encryption, secure multiparty computation, and differential privacy have the potential to address these challenges.

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

The eID Regulation provides the legal framework on which to build technological solutions that address the user needs concerning their digital identity. With regards to personal data, it is also important to develop self-sovereign identity solutions that give users complete control on their personal data and use.
Proposals should address usability, scalability and reliability of secure and privacy-preserving technologies in supply chain and take integration with existing infrastructures and traditional security measures into account. They should further take into account, whenever needed, the legacy variation in data types and models across different organizations.

Consortia should bring together interdisciplinary expertise and capacity covering the supply and the demand side, i.e. industry, service providers and, where relevant, end-users. The use of authentication and authorisation infrastructure framework tools developed for data spaces, and notably with the European Open Science Cloud, could be considered. Participation of SMEs is strongly encouraged. Legal expertise should also be added to ensure compliance of the project results with data regulations and the GDPR.
The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged.

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

Per project EUR 4 and 6 million
Budget EUR 12 million.
Type of Action Research and Innovation Actions

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

- Security-by-design concept and resilience to adversarial attacks;
- Inclusion of context awareness in machine learning in order to boost resiliency.

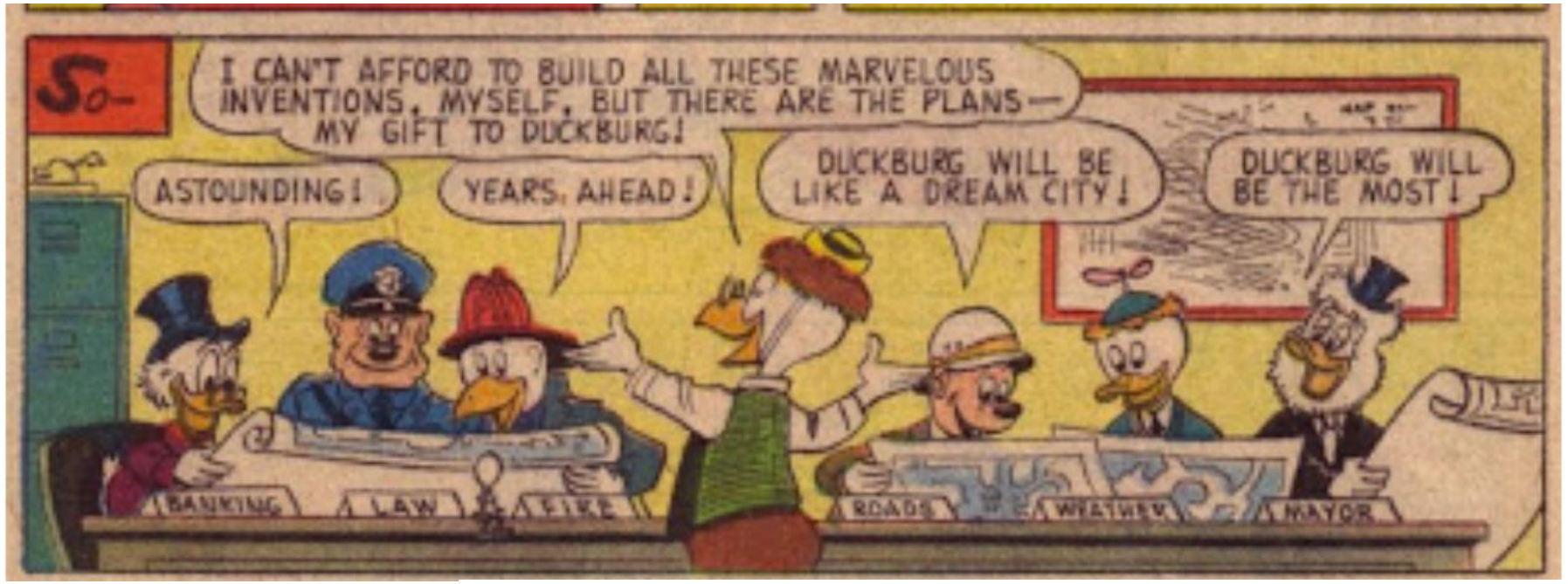
HORIZON-CL3-2023-CS-01-03: Security of robust AI systems

Scope:

Proposals received under this topic will address the security of AI systems, in the line with the following considerations. The availability of very large amounts of data, together with advances in computing capacity, has allowed the development of powerful Artificial Intelligence applications (in particular Machine Learning and Deep Learning). At the same time, concerns have been raised over the security, robustness of the AI algorithms (including AI at the edge), including the risks of adversarial machine learning and data poisoning.

Proposals should demonstrate awareness of the EU approach on Artificial Intelligence, such as the proposed Artificial Intelligence Act.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.



Support to Security Research and Innovation

Disney, Monsterville, 1961

Call - Support to Security Research and Innovation 2023

- HORIZON-CL3-2023-SSRI-01-01: Open grounds for pre-commercial procurement of Innovative security technologies
  - Two 1 M€ CSA projests (Action Coordination and Support Actions)
- HORIZON-CL3-2023-SSRI-01-02: Accelerating uptake through open proposals for advanced SME innovation
  - Three 1.5 M€ IA projects

Call - Support to Security Research and Innovation 2024

- HORIZON-CL3-2024-SSRI-01-01: Demand-led innovation through public procurement
- HORIZON-CL3-2024-SSRI-01-02: Accelerating uptake through open proposals for advanced SME innovation

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

Two 1 M€ CSA projests (Action Coordination and Support Actions)

The following additional eligibility conditions apply: This topic requires the participation of at least 6 relevant end-user organisations as well as at least 3 public procurers from at least 3 different EU Member States or Associated Countries.

Open market consultations carried out during this project must take place in at least three EU Member States or Associated Countries.

Eligible costs will take the form of a lump sum.

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

.

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

Expected Outcome:

- Consolidated demand for innovative security technologies built on the aggregation of public buyers with a common need expressed in functional and/or operational terms without prescribing technical solutions;
- Better informed decision-making related to investment in innovative security technologies based on a better understanding of the potential EU-based supply of technical alternatives that could address common needs of EU public buyers;
- Better informed decision-making related to investment in innovative security technologies based on an improved visibility of the potential demand in the EU market for common security technologies;
- Increased capacity of EU public procurers to align requirements with industry and future products and to attract innovation and innovators from security and other sectors through common validation strategies, rapid innovation, experimentation and pre-commercial procurement;
- Increased innovation capacity of EU public procurers through the availability of innovative tendering guidance, commonly agreed validation strategies and evidence-based prospects of further joint procurement of common security solutions. .

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

Scope: End-users and public procurers from several countries are invited to submit proposals for a preparatory action that should build the grounds for a future Pre-Commercial Procurement action.

Programme 2025-2027 (subject to budget availability and priorities of the Work Programme 2025-2027). In preparing the grounds for a possible future PCP action, the outputs of this CSA should take into consideration:

- The policy priorities described in this Work Programme Part for the security areas mentioned above;
- The EU Directive for public procurement and in particular with the provisions related to PCP;
- The specific provisions and funding rates of PCP actions and the specific requirements for innovation procurement (PCP/PPI) supported by Horizon Europe grants, as stated in the General Annex H of the Horizon Europe Work Programme;
- The guidance for attracting innovators and innovation, as explained in the European Commission Guidance on Innovation Procurement C(2021) 4320, in particular those measures oriented to reduce the barriers to high-tech start-ups and innovative SMEs.

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

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:

- 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;
- There is a quantifiable and identifiable community of potential buyers 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
- Technology developments to be conducted in the future PCP can be done in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data.
- That in developing technology solutions, societal aspects can be taken into account in a comprehensive and thorough manner.

HORIZON-CL3-2023-SSRI-01-02: Accelerating uptake through open proposals for advanced SME innovation

Three 1.5 M€ IA projects

Consortia must include:
- A minimum of three (3) to a maximum of seven (7) partners.
- At least 2 SMEs from 2 different Member States.
- At least 1 end-user organisation relevant per area.
- At least 3 Member States or Associated Countries must be represented in the consortium.

Participation of non-SME industries and RTOs is not excluded, but it must be limited to 15% of the budget.
At least 50% of the budget must be allocated to SMEs.

To ensure a balanced portfolio, grants will be awarded to applications not only in order of ranking but at least also to one project that is the highest ranked within each of the four options

- Option A ''Fighting Organised Crime and Terrorism''
- Option B ''Disaster Resilience''
- Option C ''Resilient Infrastructure'' and
- Option D ''Border Security'', provided that the applications attain all thresholds.

Eligible costs will take the form of a lump sum
The projects should have a maximum estimated duration of 2 years.

HORIZON-CL3-2023-SSRI-01-02: Accelerating uptake through open proposals for advanced SME innovation

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

- Development of a mature technological solution addressing EU security policy priorities in the areas addressed by the Cluster 3 work programme.
- Facilitated access to civil security market for small and medium innovators and enhanced links between suppliers and public buyers;
- Improved cooperation between public buyers and small supply market actors for a swifter uptake of innovation in response to short to mid-term needs;
- Stronger partnerships between small and medium EU security industry and technology actors to ensure the sustainability of the EU innovation capacity in the civil security domain and increase technological sovereignty of the EU in critical security areas.

HORIZON-CL3-2023-SSRI-01-02: Accelerating uptake through open proposals for advanced SME innovation

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

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

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

Corrections coming?

Revised draft version

The revised Cluster 3 next two-year Work Programme:

- Absorbs the full 50 mil frontloading
- Introduces open topics
- Reinstates topics
- Increases certain topics' budget and number of grants

Topics / grants / budget:

- ~~42~~ 48 topics / ~~71~~ 83 expected grants / Euro ~~317,8~~ 367,8 mil.

2 YEARS

2023 Borders

- Topic on 'Capabilities for border surveillance and situational awareness': 2 grants of 4 mil each.

2023 DRS

- Reinstated topic on 'Design of crisis prevention and preparedness actions in case of digital breakdown (internet, electricity etc.). Budget: increased to 4 mil.
- Topic on 'Robotics: Autonomous or semi-autonomous UGV systems to supplement skills for use in hazardous environments' Budget increased to 8 mil (2 grants of 4 mil each).

2023 Cyber

- Topic on 'Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)': increased budget by 5 mil.
- Topic on 'Security of robust AI systems': increased budget by 3 mil.

Participant Portal

- Latest Call text – the proposal must answer to its requirements
- Other documents that help, give guidance
- Lists interested parties but not all are relevant actors!
  - https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/topic-announcements/44114300
- 3 countries minimum (EU and e.g. Norway, not e.g. UK, CH, USA – they can be a part but not in the minimum), typically 6-12 countries with one or two actors per country

- Business Finland kouluttaa –esim. kustannusasiat https://www.businessfinland.fi/ajankohtaista/tapahtumat/horisontti-eurooppa/2022/save-the-date-horisontti-eurooppa-kustannusasioiden-masterclass

- EU infopäivä kevätkesällä, SMI2G brockerage event

https://cordis.europa.eu/
Vanhat projektit

SEREN tai SEREN5 – Horisontin turvallisuustutkimuksen tukiprojekti

SECURITY FUNDING ELSEWHERE

Horisontti Euroopan CL4:n Space-osiossa on pari satelliittitietoliikenteen ja –kaukokartoituksen hanketta siviiliturvallisuusteemassa, CL5:n automaattiliikenteessää on joskus turvallisuustopic …

Migration and Home Affairs

Home | Policies | Agencies | Networks | Funding | What's new | About us

HOME > Funding > Internal security funds > Internal Security Fund (2021-2027)

Internal Security Fund (2021-2027)

Digital Europe Programme

- Funding ratio 50% (SME's 75%)
- Also one entity/country projects

- 2nd Cybersecurity Call 15 Nov 2022 – 15 Feb 2023

- https://www.youtube.com/watch?v=AdKhbnElcyk Austrian presentation on this Call

- See also: Internal Security Fund - https://home-affairs.ec.europa.eu/funding/internal-security-funds/internal-security-fund-2021-2027_en

Topic	Budget
EU cybersecurity recilience and cybersecurity ranges	15 M€
Capacity building of Security Operations Centers (SOCs)	72,5 M€
Secure 5G and other strategic digital infrastructures and technology	10 M€
Uptake of innovative cybersercurity solutions in SMEs	32 M€
(Network og National Coordination Centers – for government agencies, e.g. Traficom in Finland)	(22 M€)
Supporting the NIS Directive implementation and national cybersecurity strategies	20 M€
Training and certification capabilities	5 M€

Kiitos

HORISONTTI EUROOPPA

EU:N TUTKIMUS- JA INNOVAATIO-OHJELMA