#innovacion
#ayudascdti
#asesoramiento
#internacionalizacion

El Clúster 3 de Horizonte Europa “Seguridad civil para la sociedad” Convocatoria 2023 y aspectos prácticos

Maite Boyero
Delegada española y Punto de contacto nacional
Clúster 3 – Heuropa
Maite.boyero@cdti.es

@HorizonteEuropa

Horizonte Europa: El Programa Marco de I+D+I de la UE (2021-2027)

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI INNOVACIÓN

Estructura del programa

PILAR 1 – CIENCIA EXCELENTE	25.011
ERC - Consejo Europeo de Investigación	16.004
MSCA - Acciones Marie Skłodowska-Curie	6.602
Infraestructuras de investigación	2.406

PILAR 2 - RETOS MUNDIALES Y COMPETITIVIDAD INDUSTRIAL EUROPEA	53.516
Clúster 1 - Salud	8.246
Clúster 2 - Cultura, creatividad y sociedad inclusiva	2.280
Clúster 3 – Seguridad civil	1.596
Clúster 4 - Digital, industria y espacio	15.349
Clúster 5 - Clima, energía y movilidad	15.123
Clúster 6 - Alimentación, bioec. recursos naturales, agricultura y MA	8.952
JRC – Centro Común de Investigación	1.970

PILAR 3 – INNOVACIÓN ABIERTA	13.597
EIC- Consejo Europeo de Innovación	10.105
Ecosistemas de innovación europea	527
EIT - Instituto Europeo de Innovación y Tecnología	2.965

Ampliar la Participación y Fortalecer el Espacio Europeo de Investigación	3.393
Ampliar la participación y difundir la excelencia	2.955
Reformar y mejorar el sistema europeo de la I+i	438

Presupuesto en precios corrientes.

EU Security Union Strategy (2020-2025)

"Your security is our priority"

La Estrategia establece los **instrumentos y las medidas** que han de desarrollarse durante los próximos cinco años para **garantizar la seguridad en nuestro entorno físico y digital.**

Bases de la Estrategia de Seguridad de la UE

- Amenazas de seguridad en **constante cambio**, que pueden afectar a distintos países y producir inestabilidad en la sociedad Europea
- La Estrategia es parte de uno de los grandes objetivos de la Comisión (Von der Leyen) *"Protecting our European Way of Life"* – entre otros
- Seguridad **interior y exterior**
- **Autonomía estratégica** en términos de productos, servicios, infraestructuras y tecnologías vitales
- Necesidad de mejorar **la coordinación** en la gestión de crisis y otros retos de la UE
- **Conectar a todos los actores de los sectores público y privado en un esfuerzo común**

Nueva estrategia UE en Ciberseguridad

RESILIENCIA, SOBERANÍA TECNOLÓGICA Y LIDERAZGO

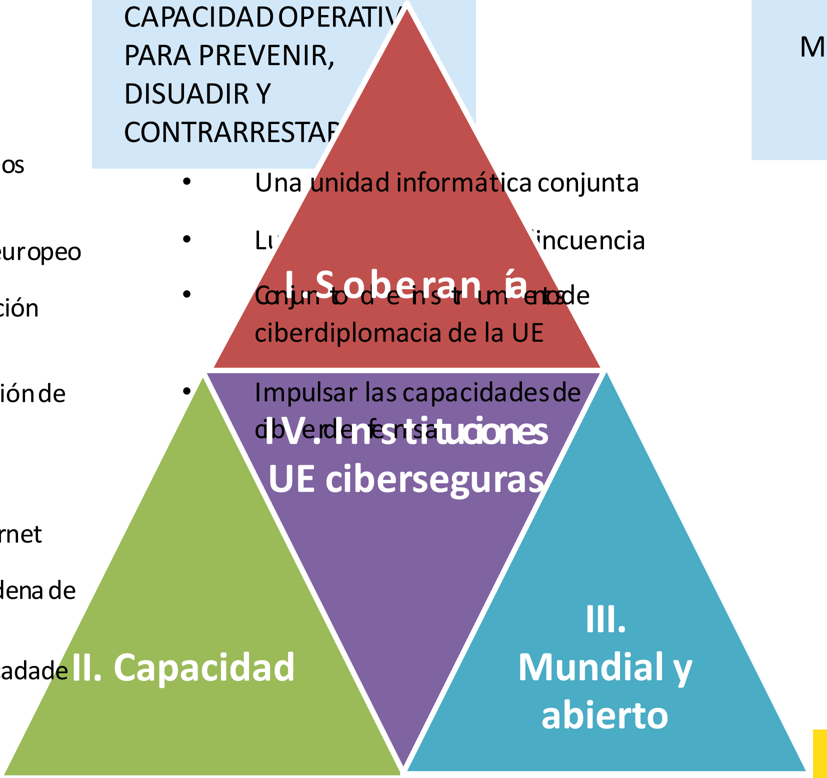
- Infraestructura resiliente y servicios críticos
- Construir un escudo cibernético europeo
- Una infraestructura de comunicación ultrasegura
- Protección de la próxima generación de redes móviles de banda ancha
- Una internet de las cosas seguras
- Mayor seguridad mundial en internet
- Una presencia reforzada en la cadena de suministro de tecnología
- Una población activa cibercualificada de la UE

DESARROLLO DE LA CAPACIDAD OPERATIV
PARA PREVENIR, DISUADIR Y CONTRARRESTAR

- Una unidad informática conjunta
- Lu [illegible] incuencia
- Conjunto de instrumentos de ciberdiplomacia de la UE
- Impulsar las capacidades de ciberdefensa

FOMENTAR UN CIBERESPACIO MUNDIAL Y ABIERTO

- Liderazgo de la UE en materia de estándares, normas y marcos en el ciberespacio
- Cooperación con los socios y la comunidad de múltiples partes interesadas
- Fortalecimiento de las capacidades globales para aumentar la capacidad de recuperación mundial



Estrategia UE en Ciberseguridad

- **Legislación:** Directiva NIS, Legislación sectores críticos, CyberAct

- **Coordinación:** Blueprint, Joint Cyber Unit, 5G toolbox

- **Financiación: Horizonte Europa**, CEF y Programa DIGITAL

- Puesta en marcha del CCCN

CYBER SECURITY · CYBER SECURITY · CYBER SECURITY · CYBER SECURITY

Particularidades Clúster 3

- Enfoque basado en **desarrollar capacidades para usuarios finales de seguridad → criterios de elegibilidad + *market uptake***

- Reforzar la colaboración con **industria y academia**

- **Factor social**

- **Impacto en políticas** de seguridad de la UE

- **Creación de mercado**

Aspectos de interés para Guardia Civil

- ✓ Orientación a **USUARIO FINAL → participación obligatoria***

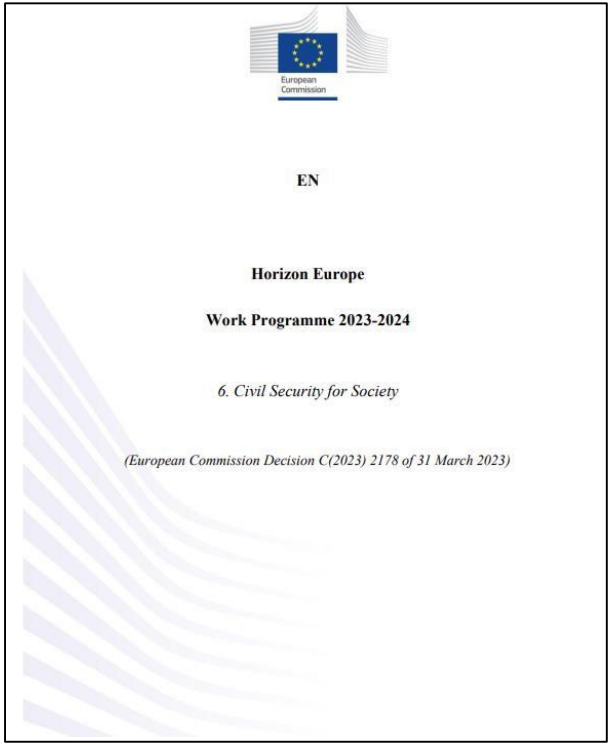
- ✓ **Proyectos cercanos a mercado** (TRL 4 a 8)

- ✓ Aplicación **civil**, exclusivamente, pero posible uso dual

- ✓ **Pilotos, demostraciones, “test-beds” en entornos reales o semi-reales**

Convocatoria 2023
Clúster 3

Convocatoria 2023 Clúster 3



European Commission

EN

Horizon Europe

Work Programme 2023-2024

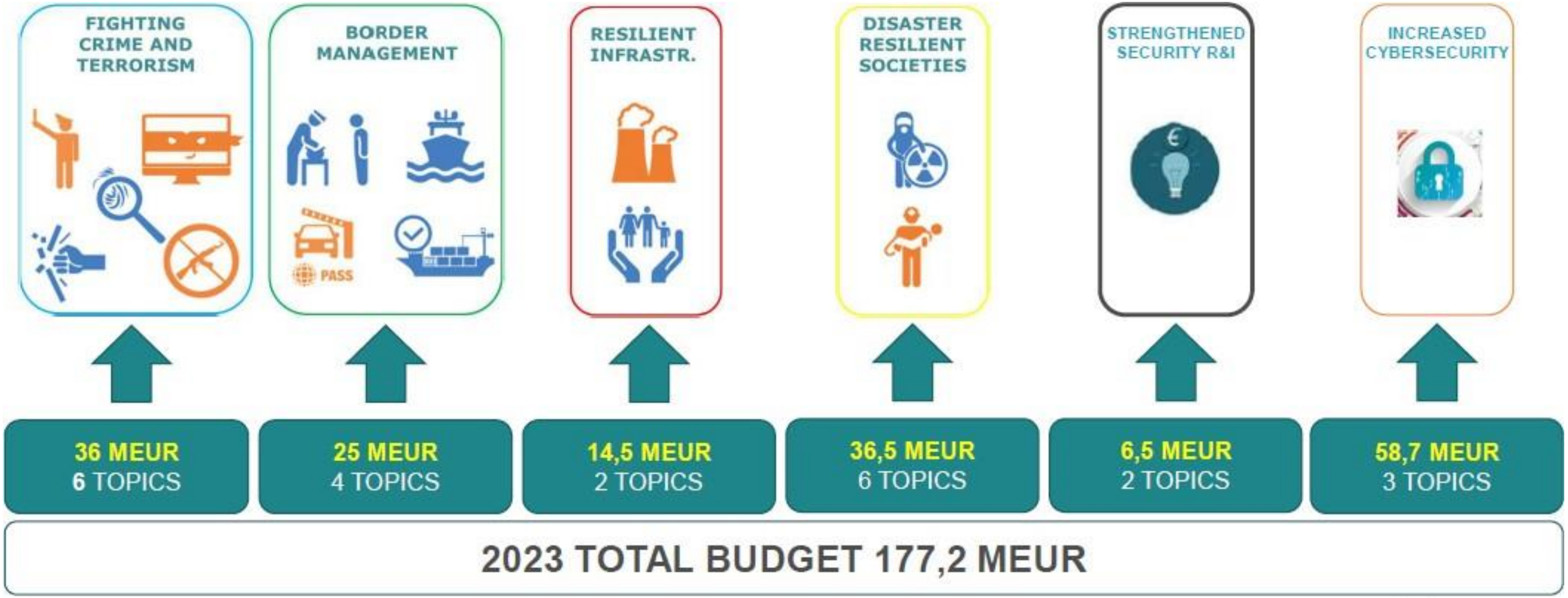
6. Civil Security for Society

(European Commission Decision C(2023) 2178 of 31 March 2023)

Fecha de cierre: 23 de Noviembre, 2023, 5pm CET

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf

6 "*Destinations*" / Convocatorias paralelas



FIGHTING CRIME AND TERRORISM

BORDER MANAGEMENT

RESILIENT INFRASTR.

DISASTER RESILIENT SOCIETIES

STRENGTHENED SECURITY R&I

INCREASED CYBERSECURITY

36 MEUR
6 TOPICS

25 MEUR
4 TOPICS

14,5 MEUR
2 TOPICS

36,5 MEUR
6 TOPICS

6,5 MEUR
2 TOPICS

58,7 MEUR
3 TOPICS

2023 TOTAL BUDGET 177,2 MEUR

Convocatoria FCT – Fight against crime and terrorism

- *"**Crime and terrorism** are more effectively tackled, while **respecting fundamental rights**, […] thanks to more powerful prevention, preparedness and response, a better **understanding** of related human, societal and technological aspects, and the development of cutting-edge capabilities for **police authorities** […] including measures against cybercrime."*

	Action Type	Funding /Project (M€)	TRL	Eligibility conditions
FCT01- Modern information analysis for fighting crime and terrorism				
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	IA	7	7 u 8	3 Police Authorities
FCT02- Improved forensics and lawful evidence collection				
HORIZON-CL3-2023-FCT-01-02: A harmonized European forensics approach on drugs analysis (sub-topics A & B)	IA	4.5 each	6 o 7	3 Police Authorities + 2 forensic institutes
FCT03- Enhanced prevention, detection and deterrence of societal issues related to various forms of crime				
HORIZON-CL3-2023-FCT-01-03: New methods and technologies in service of community policing and transferable best practices	RIA	4	6 o 7	3 Police Authorities
FCT04- Increased security of citizens against terrorism, including in public spaces				
HORIZON-CL3-2023-FCT-01-04: Open Topic	RIA	4	5 ó 7	3 Police Authorities
FCT05 - Organised crime prevented and combated				
HORIZON-CL3-2023-FCT-01-05: Crime as a service	RIA	4	5 ó 6	3 Police Authorities
FCT06- Citizens are protected against cybercrime				
HORIZON-CL3-2023-FCT-01-06: Enhancing tools & capabilities to fight advanced forms of cyber threats & cyber-dependent crimes	RIA	4	5 ó 6	3 Police Authorities

✓ **FOR TOPICs FCT-01-02 & 04,** If using satellite-based, positioning, navigation and/or related timing data and services, **THEN IT MUST BE Galileo/EGNOS & encourage Copernicus.**

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

Expected outcomes

- Improved capabilities of European Police Authorities and other relevant security practitioners for a **fast and flexible analysis** of **huge amounts of heterogeneous data**
- Enhanced and modern **analysis of heterogeneous data** as well as training curricula that take into account **legal and ethical** rules of operation
- Their work is supported by **big data analysis** that is in accordance with data minimisation principles and **high privacy standards**.

Scope

- Police Authorities need adequate technologies to properly **detect and counter emerging threat** while processing of **large complex and unstructured datasets**.
- 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, speech recognition and transcription into text, etc… (full list in WP)

Budget EUR 7M : 7M per action

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

Expected outcomes

- European Police Authorities, forensic institutes and other relevant security practitioners are equipped by modern **means of chemical analysis** aimed at facilitating the **cross-matching of seized drugs to labs**
- Improved and **uniform EU-wide approach** for the collection of evidence
- Improved collection and availability of forensic evidence, that could be **used in court by the authorities**
- Enhanced **perception of citizens** that Europe is an **area of freedom, justice and security**.

Scope

- **Option A**: A harmonised European approach on the study of chemical analysis in drugs, to
  - facilitate the **cross-matching of seized drugs to labs**, and
  - tackle forensic challenges related to **illicit drugs-related overdoses** (EU Drugs Strategy 2021-2025)
- **Option B**: A reliable and easy-to-use detection of chemical **submission drugs** in beverages and urine.
  - Modern methods and technologies that enable **better prevention** against and investigation of different forms of **violence and assault** supported by these drugs.

Budget EUR 9M : 4,5M per action

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

Expected outcomes

- Strengthened **resilience** of local communities **against crime and radicalisation**
- Negative factors in communities are **identified early**, possible threats are detected, and **crime reporting is enhanced**
- Better recognition for **community diversity** within neighborhoods
- Identification and dissemination of **community policing best practices**
- **Training curricula for Police Authorities** are developed on community policing in non-homogenous local milieus with social complexities

Scope

- Proposals should analyze its potential relations with introduction of innovative **alternatives to imprisonment**
- More **efficient solutions**, **tools and methodologies** are sought to cope with **growing communities**, **tighter budgets**, and diverse, **quickly evolving milieus**
- New approaches should cover internal review of **Police Authorities' personnel training**, possible change of attitudes and **communication language**, or countering existing **misconceptions and biases**.

Budget EUR 4M : 4M per action

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

Expected outcomes

- Enhanced ability of security practitioners to **identify and prevent emergent challenges**
- **Harmonised and modern tools** as well as procedures of the terrorism-related problem under consideration
- Improved **cooperation** between European Police Authorities
- **Training curricula** for Police Authorities

Scope

- Solutions for increasing security of citizens against terrorism, **that are not covered by the other topics of Horizon Europe** Calls FCT 2021-2022, FCT 2023 and FCT 2024
- Proposals should convincingly explain how they will plan and/or carry out **demonstration, testing or validation** of developed tools and solutions.
- Research proposals should consider, build on if appropriate and **not duplicate previous research**,
- Proposals funded under this topic are expected to engage with the **Europol Innovation Lab** during the lifetime of the project

Budget EUR 4M : 4M per action

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

Expected outcomes

- European Police Authorities and policy makers are provided with a **robust analysis of the evolution of the contemporary organised crime**

- Policy makers benefit from an **analysis of the legal framework** utilised for countering **organised crime**

- Methodology for the identification of the means of **advertising, communication, marketing and money flows** used for offering criminal services

- Improved knowledge within European security institutions regarding developments in the field of organised crime and prospects for the future.

Scope

- In order to enhance the fight against organised crime at the European level, there is a need for distinct research to gain **comprehensive insight** into the internal workings of **modern organised crime structures** and their marketplaces

- **Coordination** among the successful proposal from this topic as well as with the successful proposals under topics **HORIZON-CL3-2023-FCT-01-06 and HORIZON-CL3-2024-FCT-01-06** should be envisaged to avoid duplication, and to exploit complementarities as well as opportunities for increased impact.

Budget EUR 4M : 4M per action

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

Expected outcomes

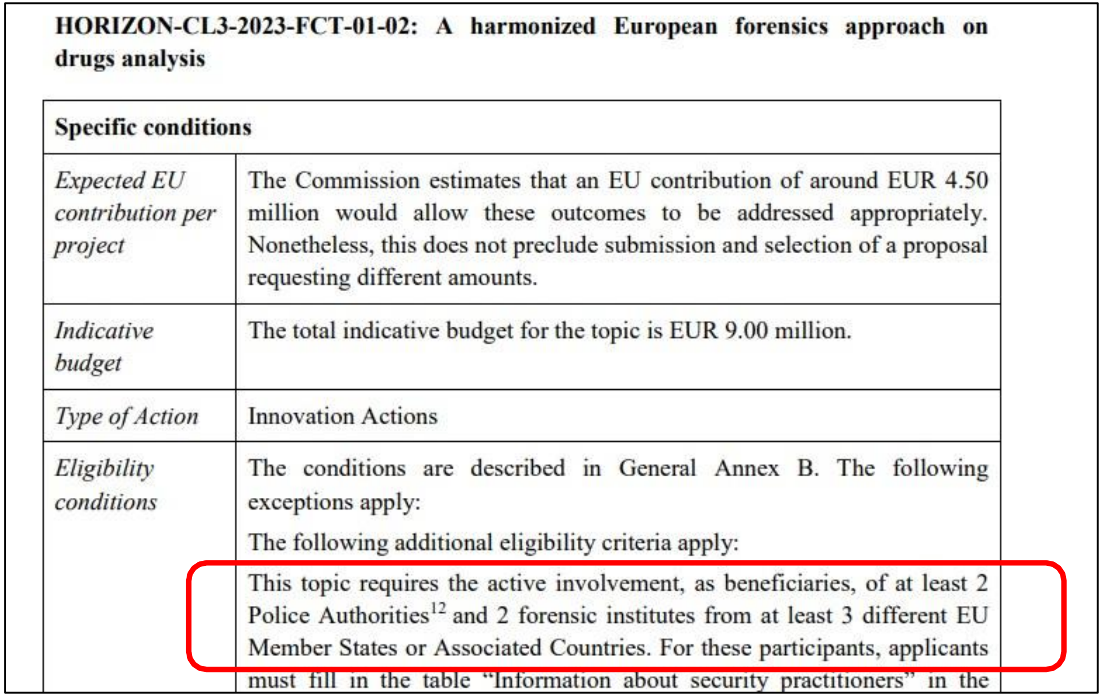
- Development of **modular toolbox for Police Authorities**
- Detection of **crypto-jacking, compromised registration forms, malware attacks and other cybercrimes perpetrated using cryptocurrencies;**
- Development **of training curricula**, for Police Authorities
- Recommendations on **public cybercrime awareness** actions contributing to early detection and prevention
- Identification of best practices of international law enforcement and judicial cooperation networks
- Development of multi-stakeholders strategies

Scope

- Investigators need **timely access to relevant data and expertise** of a different nature and belonging to different categories of stakeholders
- **The technical and organizational complexity together with the cross-border nature of cyberattacks** requires cutting-edge investigative approaches, gathering a large range of expertise as well as trusted information sharing mechanisms across communities
- Development of **multi-stakeholders strategies**, including novel investigation schemes and information sharing mechanisms, is necessary.
- Coordination among the successful proposals from this topic as well as with the successful proposal under **HORIZON-CL3-2023-FCT-01-05** should be envisaged

Budget EUR 8M : 4M per action

(EJEMPLO DE CONDICIONES DE ELEGIBILIDAD)– TOPIC HORIZON-CL3-2023-FCT-01-02



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

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.50 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 9.00 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[12] and 2 forensic institutes 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

Affiliated entities Y Associated partners

<u>NO CUENTAN</u> PARA LAS CONDICIONES DE ELEGIBILIDAD

Convocatoria BM – Border Management

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

Deadline 23-Nov-2023

	Action Type	Funding/Project (M€)	TRL	Eligibility conditions
BM01 – Efficient border surveillance and maritime security				
HORIZON-CL3-2023-BM-01-01: Capabilities for border surveillance and situational awareness (*)	IA	4	N/A	2 Border Authorities
HORIZON-CL3-2023-BM-01-02: Identify, inspect, neutralise Unexploded Ordnance (UXO) at sea (*)	RIA	5	N/A	2 Border Authorities
BM02 - Secured and facilitated crossing of external borders				
HORIZON-CL3-2023-BM-01-03: Beyond the state-of-the-art “biometrics on the move” for border check (*)	RIA	3	N/A	2 Border Authorities
BM03 – Better customs and supply chain security				

- ✓ **FOR ALL TOPICs,** If using satellite-based, positioning, navigation and/or related timing data and services, **THEN IT MUST BE Galileo/EGNOS & encourage Copernicus.**
- ✓ ***LUMP SUM funding format FOR ALL TOPICS IN BM THIS YEAR!**

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

Expected 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
- **More efficient and more flexible solutions** than physical barriers to deter and monitor irregular border crossings

Scope

- Proposed solutions should allow higher **interoperability cross border** among EU and Associated Countries practitioners
- 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: networked deployable, and possibly mobile, **semi-autonomous surveillance towers**; **IoT** and advanced mesh connectivity; **Virtual and Augmented Reality** for enhanced C2 and **situational awareness**;
- The proposed solutions should include, by design, the **protection of fundamental rights** such as privacy, and/or the application of **privacy-enhancing technologies**, and should contribute to cost and energy efficiency
- Proposals are expected to address the priorities of the European Border and Coast Guard and of its Agency (**Frontex**).

Budget EUR 8M : 4M per action

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

Expected 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.

Scope

- The proposed project should improve **civilian** capabilities on:
- a) analysis of legislation, roles and responsibilities in Member States;
- b) detecting UXO on and below the marine sediment/seabed, inorder to detect also buried objects;
- c) identifying, classifying, assessing
- d) inspecting and handling
- e) neutralising and disposing
- **The project should focus on civilian capability gaps and needs, rather than capabilities that are better addressed by defence instruments and tasks.**

Budget EUR 5M : 5M per action

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

Expected outcomes

- Knowledge and development on robust biometrics technologies that could be used for recognition of people crossing external EU borders
- Maximisation of security reassurances, minimizing handling of personal data and maximising accuracy, reliability and throughput of the recognition process
- Contribution to improving the operational response capacity of Frontex at border crossing points

Scope

- 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”**),
- This applies to the requirements on reliability, usability, scalability, throughput and strict minimization of risks to personal data protection and fundamental rights
- Proposed projects should investigate biometrics modalities that currently do not offer satisfactory performance
- The proposed solutions should comply with **EU data protection** law, and, amongst others, embed **data protection by design**.
- 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.
- **Examples**; 3D facial images, contactless friction-ridge biometrics (i.e. fingerprint, palmprint and finger-knuckle-print), iris recognition from long distances, palm vein, periocular biometrics

Budget EUR 6M : 3M per action

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

Expected outcomes

- Increased interoperability of existing customs control equipment
- More efficient and quicker availability, for EU customs practitioners, of reference data on threats anddangerous and/or illicit materials;
- Building capabilities for a more harmonised European application of customs controls

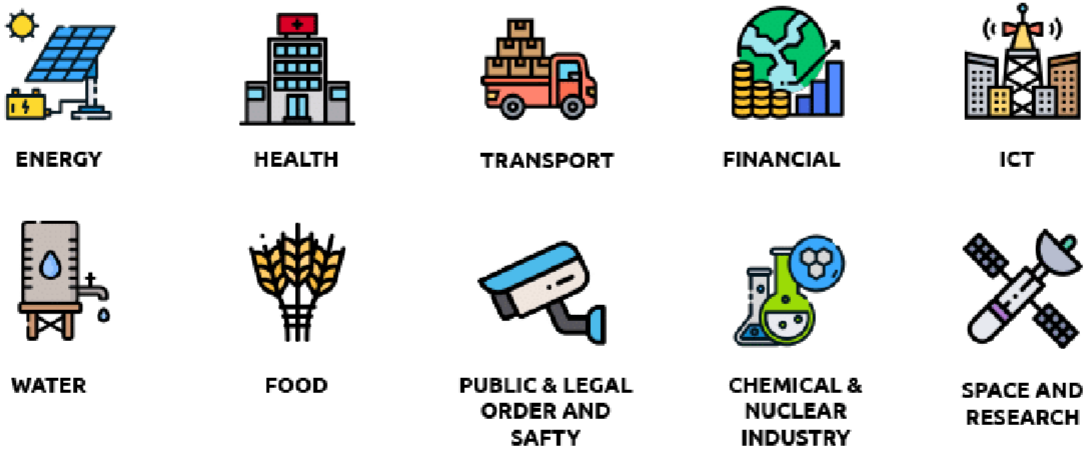
Scope

- research and innovation for solutions that prepare andincrease the interoperability of customs control equipment anddata at “tactical” level
- The solution(s) shoulddefine the requirements and way forward to enable andenhance the interoperability of customs control equipment and of data used in different Member States and/or by different authorities at national level, as well as Commission systems
- The proposed solution should include privacy enhancing techniques to allow the sharing of tools without the sharing of data beyondwhat is strictlynecessary
- EU customs authorities shouldtake up the results of the research with the support of the Customs Control Equipment Instrument

Budget EUR 6M : 6M per action

Convocatoria INFRA – Critical infrastructures' protection

- *"[…] **resilience and autonomy of physical and digital infrastructures** are enhanced and vital societal functions are ensured, thanks to more powerful **prevention, preparedness and response**, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for […] infrastructureoperators […]"*



ENERGY

HEALTH

TRANSPORT

FINANCIAL

ICT

WATER

FOOD

PUBLIC & LEGAL ORDER AND SAFTY

CHEMICAL & NUCLEAR INDUSTRY

SPACE AND RESEARCH

HORIZONTE EUROPA
@HorizonteEuropa

CDTI
INNOVACIÓN

Deadline 23-Nov-2023

TOTAL of 14,5M€ available for this call	Action Type	Funding/Project (M€)	TRL	Eligibility conditions
INFRA01 – Improved preparedness and response for large-scale disruptions of EU infrastructures				
HORIZON-CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services**	*IA	5	6-8	**3 National Gov. Authorities and**/or 3 CIO
HORIZON-CL3-2023-INFRA-01-02: Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures	*IA	9,5	6-8	3 CIO – critical infrastructures operator

FOR BOTH TOPICS:

- ✓ If using satellite-based, positioning, navigation and/or related timing data and services, **THEN IT MUST BE Galileo/EGNOS& encourage Copernicus.**
- ✓ ****Participation is limited to legal entities established in Member States only.**
- ✓ ***LUMP SUM funding format**

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

Expected outcomes

- Tools for the assessment and anticipationof relevant risks to the provisions of essential services
- Cooperationbetween authorities of EU Member States facilitated by providing solutions for data exchange and joint cross-border risk assessments;
- Simulation tools for large-scale exercises to test the resilience of operators
- Measures by MS authorities to facilitate risk assessments by operators
- Provide common Europeanguidance and support for the drafting of their resilience plans inorder to meet all the provisions of the proposed CER-Directive

Scope

- Proposals shouldsupport competent authorities in Member States to enhance the resilience of key sectors andimplement future EU legislation.
- Focus should be on delivering solutions that aid cooperation, communication, risk assessments, best practices, exercises, and training modules for overseeing sector resilience.
- Develop tools to analyze all hazards, manage interdependencies, and cover sectors mentioned inrelevant directives. Integration of the gender dimension should be considered if relevant, and collaboration with Commissionexpert groups and EU agencies is encouraged.

Budget EUR 5M : 5M per action

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

Expected outcomes

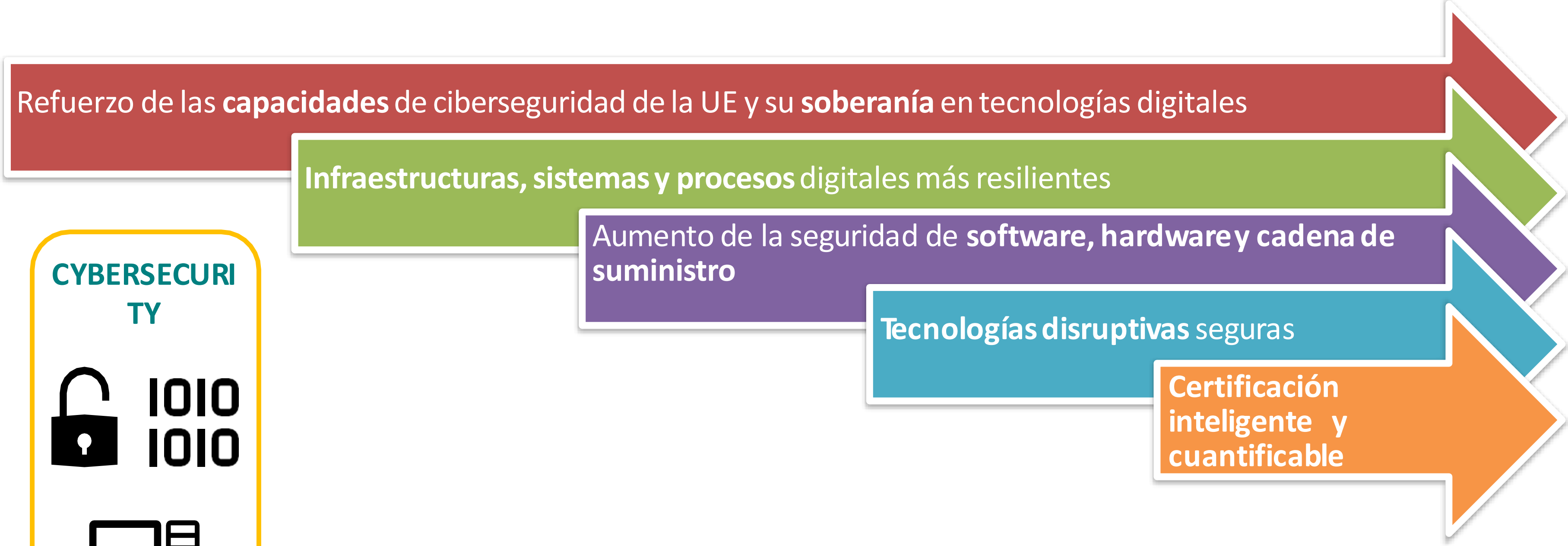
- Analysis of physical/cyber detection technologies for operators in sectors not covered by previous research projects.
- Strengthen cooperation to address natural or human-made threats and disruptions in critical infrastructures.
- Improve situational awareness, preparedness, and governance by enhancing detection, projection of threatening situations, and implementing prevention, preparedness/mitigation, response, and recovery interventions.
- Significantly reduce risks and exposures to anomalies or deliberate events on cyber-physical systems or complex critical infrastructures/ systems.
- Defining operational procedures for operators and public authorities, taking into account citizen behavior/reactions and societal impacts.

Scope

- Operators need to be equipped with effective means to prevent, resist, absorb, and recover from disruptive incidents, regardless of their cause.
- Efficient cybersecurity measures are needed to block access to critical infrastructures and protect against threats and vulnerabilities.
- Proposals should focus on increasing the combined cyber and non-cyber resilience of operators in priority sectors not previously covered in research, contributing to overall EU-level resilience.
- Proposals should develop methods for resilience planning, including risk analysis, cross-sector and cross-border analysis, standardized plans, and protection of sensitive information.
- Applicants are encouraged to explore and demonstrate synergies with the work conducted in the European Reference Network for Critical Infrastructure Protection (ERNCIP), as applicable.

Budget EUR 9,50M : 4,75M per action

Convocatoria CS - Cybersecurity



Refuerzo de las **capacidades** de ciberseguridad de la UE y su **soberanía** en tecnologías digitales

Infraestructuras, sistemas y procesos digitales más resilientes

Aumento de la seguridad de **software, hardware y cadena de suministro**

Tecnologías disruptivas seguras

Certificación inteligente y cuantificable

CYBERSECURI TY

1010
1010

	Action Type	Project (M€)	TRL	Eligibility conditions
CS01 - Systems security and security lifetime management, secure platforms, digital infrastructures				
HORIZON-CL3-2023-CS-01-01: Secure computing continuum (IoT, Edge, Cloud, Dataspaces)	IA	4 a 6	N/A	N/A
CS02 - Privacy-preserving and identity technologies				
HORIZON-CL3-2023-CS-01-02: Privacy-preserving and identity management technologies	IA	2 a 4	N/A	N/A
CS03 - Secured disruptive technologies				
HORIZON-CL3-2023-CS-01-03: Security of Robust AI systems	RIA	4 a 6	N/A	N/A

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

Expected 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

Scope

- **Cloud, edge computing, IoT** requires **advanced, smart security and privacy**. Their complexity underlines the need for **proactive and automated detection, analysis, and mitigation** of cybersecurity attacks, and in application domains such as, e.g., smart cities.
- **Identification and analysis of regulatory aspects** for the developed technologies or solutions is encouraged.

Budget EUR 28M : 4-6M per action

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

Expected outcomes

- Improved **scalable** and reliable **privacy-preserving and identity management** technologies for **federated processing and secure sharing** of personal and industrial data
- Improving privacy-preserving technologies for **cyber threat intelligence** (sharing)
- **Privacy by design**
- **Contribution to European data spaces** (insynergywith *DATA Topics of Horizon Europe Cluster 4*) and **eID** compliant Europeansolutions
- Researchanddevelopment of **self-sovereignidentity** management technologies and solutions
- Provide resource efficient and secure digital identity **solutions for SMEs**
- Strengthened Europeanecosystem of **open-source developers and researchers of privacy-preserving solutions**
- **Usability** of privacy-preserving and identity management technologies

Scope

- **Advanced privacy-preserving technologies** have the potential to **enable and foster the value** in personalandnon-personal (industrial) **data assets**. Further work is requiredto ensure and test their applicability in **real-world use case scenarios**.
- Proposed solutions should be **validated and piloted in realistic, federated data infrastructures**, e.g., Europeandata spaces. They should be **GDPR compliant by-design. Open-source** solutions are encouraged.
- Consortia should bring **interdisciplinaryexpertise** and capacity covering **the supplyand the demand** side. Participation of **SMEs** is strongly encouraged. The consortium should include **legal professionals.**
- **Identification and analysis of regulatory aspects** for the developed technologies or solutions is encouraged.

Budget EUR 15.7M : 2-4M per action

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

Expected outcomes

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

Scope

- **Concerns exist over the security and robustness of AI** algorithms including the risks of adversarial machine learning and data poisoning.
- Develop ***security-by-default*** **AI algorithms**, leading to possible **certification** schemes in the future.
- Proposals should demonstrate **awareness of the EU approach on AI** such as the proposed *Artificial Intelligence Act*.
- **Identification and analysis of regulatory aspects** for the developed technologies or solutions is encouraged.

Budget EUR 15M : 4-6M per action

Convocatoria DRS – Disaster-resilient societies

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

Deadline 23-Nov-2023

TOTAL of 33.50 M€ available for this call	ACTION TYPE	FUNDING PROJECT (M€)	TRL	Eligibility conditions
HORIZON-CL3-2023-DRS-01-01: Improving social and societal preparedness for disaster response and health emergencies	RIA	2	N/A	3 organisations from at least 3 different MMSS or AC as follows: • at least 1 organisation representing citizens or local communities; • at least 1 organisation representing practitioners (1st and/or 2nd responders); and • at least 1 organisation representing local or regional authorities.
HORIZON-CL3-2023-DRS-01-02: Design of crisis prevention and preparedness actions in case of digital breakdown (internet, electricity etc.)	RIA	1	N/A	
HORIZON-CL3-2023-DRS-01-03: Operability and standardisation in response to biological toxin incidents	RIA	1	N/A	2 National standardisation organisations
HORIZON-CL3-2023-DRS-01-04: 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	IA	1	N/A	• 3 Training Centres located in EU MMSS or AC; • 2 CBRN Centres of Excellence from non-Assoc. 3rd countries; • 3 scientific stakeholders involved in training, validation & testing of CBRN-E tools & technologies & end-users (practitioners, policymakers).
HORIZON-CL3-2023-DRS-01-05: Robotics. Autonomous or semi-autonomous UGV systems to supplement skills for use in hazardous environments	RIA	2	6-8	
		1	N/A	

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

Expected outcomes

- Identify and address factors contributing to inequality, enhance communication with vulnerable groups, and establish the interconnection between resilience and vulnerability.
- Improve health literacy and promote public awareness of biosecurity.
- Enhance crisis communicationstrategies, analyze gender behaviors, and address barriers to vaccination readiness
- Incorporate information technologyin governance and decision-making processes
- Validate innovative technologies with diagnostic capabilities, suchas wearable devices and handheld PCR test devices, to enhance crisis response capabilities.
- Strengthen the One Health approach, considering physical and mental health, environmental health, andthe impacts of climate change on human health.
- Prioritize privacy safeguards to protect fundamental rights, including privacyandpersonal data protection, indisaster response systems.

Scope

- The COVID-19 pandemic highlighted the need for preparedness, addressing challenges related to protective gear, communication issues, and lack of local cooperation and prevention.
- Public communication efforts shouldreach all groups equally, considering social inequalities, local contexts, andcultural factors. Resilience should be fostered on individual, organizational, and systemic levels.
- Information technology and data processing playa crucial role in public health, but challenges such as data security and public skepticism need to be addressed. The One Healthapproach recognizes the interconnectedness of human, animal, and environmental health.
- The topic requires the incorporationof social sciences and gender expertise to enhance the societal impact. The involvement of citizens, civil society, andother stakeholders in the co-designandco-creation of solutions shouldbe promoted. International cooperationis encouraged to achieve the desired outcomes

Budget EUR 8M : 4M per action

HORIZON-CL3-2023-DRS-01-02: Design of crisis prevention and preparedness actions in case of digital breakdown (internet, electricity etc.)

Expected outcomes

- Development of prevention/preparedness actions based on the (existing) analysis of interdependencies between critical infrastructures and possible cascading effects

- Analysis of existing communication systems and assessment/development of alternative communication tools for Civil Protection and Crisis Management security authorities, including the communication with private sector and actors responsible for critical infrastructures, as well as representatives of regional / local authorities and citizen organisations.

Scope

- Focused research is needed to assess the consequences of a digital breakdown, designing appropriate crisis prevention and preparedness actions.

- Effective contribution from SSH disciplines is essential for meaningful societal impact. Promoting the involvement of citizens and societal stakeholders is encouraged, along with fostering international cooperation.

- Difference from INFRA calls? Here, the emphasis in risk management

Budget EUR 4M : 4M per action

HORIZON-CL3-2023-DRS-01-03: Operability and standardisation in response to biological toxin incidents

Expected 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 intersectorial 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.

Scope

- Recent incidents have emphasized the need for improved crisis management capabilities and standardized procedures to address the threat of biological toxins.

- Development of portable devices and technologies for on-site detection of biological toxins is necessary, along with training for responders and integration of emerging detection technologies.

- Risk assessment and appropriate protective equipment are crucial for responder safety, and a comprehensive evaluation of exposure risks, considering sex susceptibility, is needed.

- Decontamination procedures for biological toxins should be evaluated, and a consolidated platform for analytical tools, training, and intercomparisons among laboratories should be established. Collaboration with relevant authorities and organizations is essential for effective response.

Budget EUR 6M : 6M per action

HORIZON-CL3-2023-DRS-01-04: 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 outcomes

- Networking of training centres in Europe and CBRN Centres of Excellence in non-EU countries is being extended.
- Information about the capacities of networked CBRN-E training centres is compiled to enhance coordination of training and testing activities and support research and standard development.
- Cooperation and development of testing methodologies and protocols are improved to validate tools and technologies resulting from research actions and develop standards, addressing societal and technological challenges.
- An established forum of training centres promotes inter-cooperation to identify gaps in test and validation techniques, methodologies, and protocols and synchronize actions

Scope

- Strengthen networking, training and testing facilities including collaboration with non-EU CBRN Centres of Excellence, to provide robust opportunities for practicing, testing, and evaluating CBRN-E tools and technologies.
- Assessment of these facilities should identify gaps in training and testing opportunities and highlight dependencies on specific actors to strengthen capabilities.
- The involvement of SSH disciplines, experts, institutions, and citizens is crucial to enhance societal impact.

Budget EUR 4M : 4M per action

HORIZON-CL3-2023-DRS-01-05: Robotics: Autonomous or semi-autonomous UGV systems to supplement skills for use in hazardous environments

Expected outcomes

- Foster acceptance of autonomous systems in civil protection by first responders and affected individuals.
- Enhance safety and security standards for operational forces in hazardous environments.
- Increase first responder efficiency to address future personnel shortages.
- Enable remote on-scene operations to minimize risks to first responders.
- Strengthen the European robotics industry through engagement in civil protection research and innovation.
- Minimize false positive readouts from sensors carried by robots.

Scope

- Identification of fields and domains benefiting from robotic systems, especially in hazardous environments, is necessary to enhance task efficiency and reduce risks to human life.
- Proof-of-concept research and development studies should focus on autonomous or semi-autonomous systems, incorporating new sensing capabilities and intuitive human-machine interaction technologies.
- Robotic systems should be seen as an integral part of first responder ecosystems and not as a single technology
- Consideration of first responders' training, preparedness, and mindset, as well as infrastructure development, ethics, legal implications, and societal acceptance, are essential for successful integration of robotics in civil protection.
- SSH and international cooperation

Budget EUR 8M : 4M per action

HORIZON-CL3-2023-DRS-01-06: Increased technology solutions, institutional coordination and decision-support systems for first responders of last-kilometer emergency service delivery

Expected outcomes

- 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.

Scope

- Last-kilometer logistics problems hinder the efficient transportation of first responders and relief items in disaster-prone areas.
- Innovative technologies such as drones, AI, and sensors should be developed to assist in overcoming logistical challenges and to provide remote information gathering capabilities.
- Technology solutions, like navigation in smoky environments during wildfires, have the potential to enhance search operations and increase the efficiency of first responders.

Budget EUR 3,5M : 3,5M per action

Convocatoria SSRI – Strengthening security research and innovation

"Security threats are more effectively addressed thanks to better cross-cutting knowledge across different areas of security and diverse disciplines, included social sciences & humanities, enhanced implementation of the ***research & innovation cycle and improved uptake*** *at all levels of society."*

Deadline 23-Nov-2023

TOTAL of 6,5M€ available for this call	Action Type	Funding / Project (M€)	Eligibility conditions
SSRI 02 - Increased innovation uptake			
HORIZON-CL3-2023-SSRI-01-01: Open grounds for pre-commercial procurement of innovative security technologies (*)	CSA	1 (2 Projects)	6 end-user organisations + 3 public procurers
HORIZON-CL3-2023-SSRI-01-02: Accelerating uptake through open proposals for advanced SME innovation (*)	IA	1,5 (3	Consortia must include, as beneficiaries: • From 3 to 7 partners • Min 2 SMEs • Min 1 end-user from ONE of this options: ✓ Option A "Fighting Organised Crime and Terrorism" ✓ Option B '"Disaster-Resilient Society" ✓ Option C "Resilient Infrastructure" and ✓ Option D '"Border Management",

✓ FOR ALL TOPICS *LUMP SUM funding format

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

Expected outcomes

- Consolidated demand for innovative security technologies from public buyers based on common functional and operational needs, without specifying technical solutions.
- Improved decision-making on investment in innovative security technologies through a better understanding of EU-based technical alternatives and visibility of the EU market demand for common security technologies.
- Enhanced capacity of EU public procurers to align requirements with industry, attract innovation, and stimulate rapid innovation through common validation strategies, experimentation, and pre-commercial procurement.
- Increased innovation capacity of EU public procurers through the availability of tendering guidance, agreed validation strategies, and evidence-based prospects for joint procurement of common security solutions

Scope

- During the course of the project, the applicants are expected to deliver clear evidence on a number of aspects:
- The need for a PCP action is identified for the maturation of specific technologies
- A group of potential buyers with common needs is committed to conducting a PCP action to make decisions about future joint procurement
- There is a quantifiable community of potential buyers interested in exploring further adoption of similar solutions if they prove to be technologically mature by end of the project.
- The state of the art and market have been assessed, revealing various technical alternatives to the challenge at hand.
- The future PCP tendering process is well-defined, with a proposed draft planning and preparations for launching the call for R&D services.

Budget EUR 2M : 1M per action

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

Expected 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.

Scope

- Applicants are invited to submit proposals for technology development along with the following principles:
- Focus on mature technological solutions addressing EU security policy priorities in the areas addressed by the Cluster 3 work programme.
- Not overlapping with the scope of the topics included in the other destinations of this work programme.
- Fostering collaboration between SMEs from different MS and AC.
- 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.

Budget EUR 4,5M : 1,5M per action

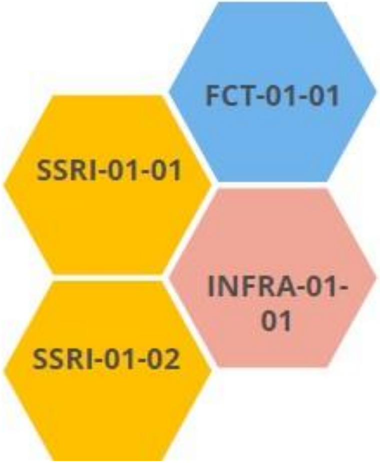
Aspectos transversales a tener en cuenta

Gender dimension in R&I content

Addressing the gender dimension in research and innovation entails taking into account sex and gender in the whole research & innovation process

The integration of the gender dimension into R&I content is **mandatory**, unless it is explicitly mentioned in the topic description

Topics flagged as not gender relevant



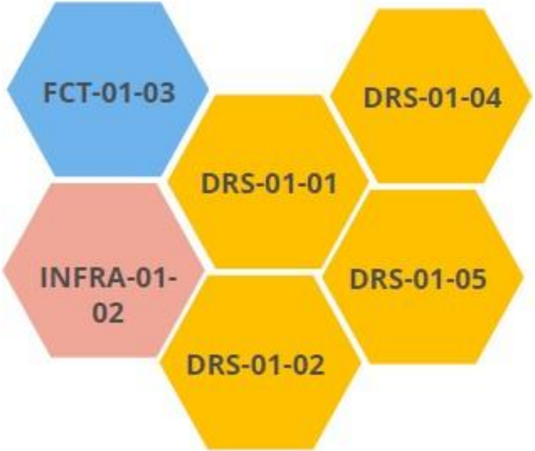
Social Sciences and Humanities (SSH)

Assessing the effective **contribution of social science and humanities disciplines** and expertise as part of the scientific methodology of the project.

When the integration of SSH is required, **applicants have to show the roles of these disciplines or provide a justification if they consider that it is not relevant for their project.**

A proposal without a sufficient contribution/integration of SSH research and competences will receive a lower evaluation score.

CL3 Topics flagged as SSH relevant



International Cooperation

To achieve the right balance between the need to exchange with key international partners (including with relevant international organisations) while at the same time ensuring the protection of the EU security interest

Cooperation can include sharing knowledge, experiences, expertise and mutual learning

International cooperation is explicitly encouraged only where appropriate and specifically supporting ongoing collaborative activities

Topics where International Cooperation is envisaged

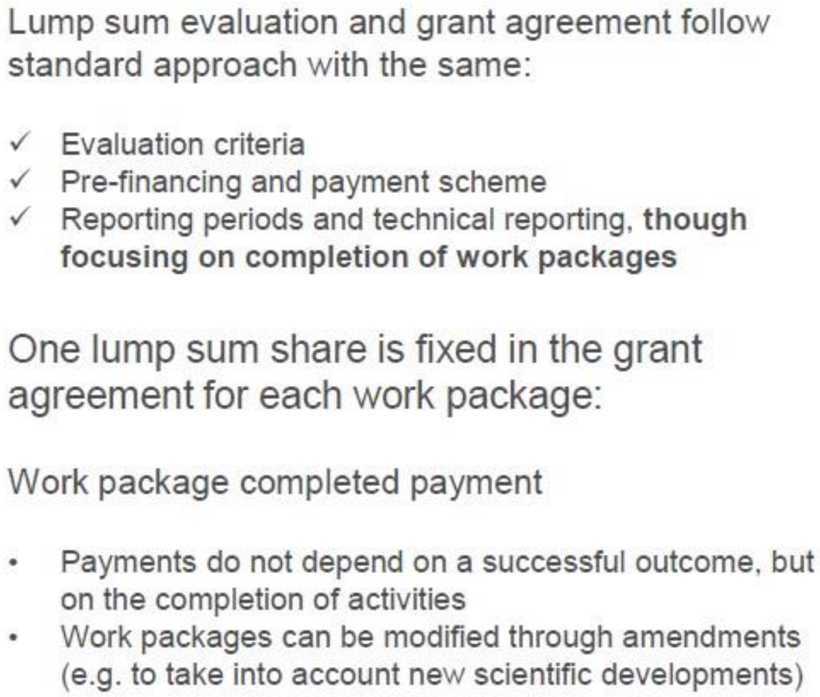
DRS-01-04

DRS-01-01

DRS-01-05

DRS-01-02

Lump Sum topics



Lump sum evaluation and grant agreement follow standard approach with the same:

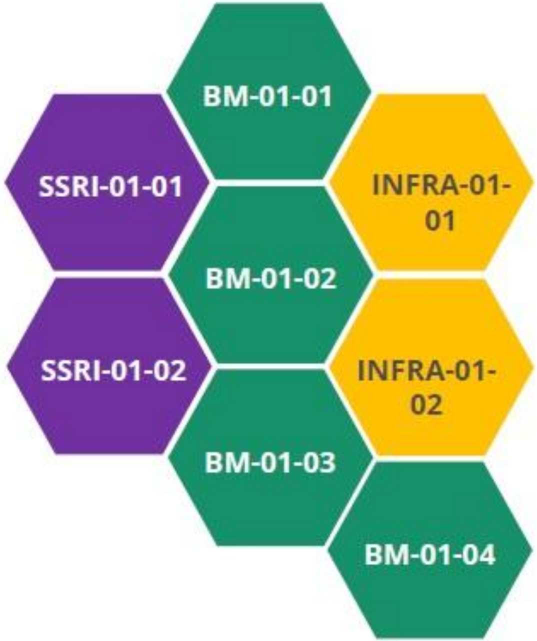
- ✓ Evaluation criteria
- ✓ Pre-financing and payment scheme
- ✓ Reporting periods and technical reporting, **though focusing on completion of work packages**

One lump sum share is fixed in the grant agreement for each work package:

Work package completed payment

- Payments do not depend on a successful outcome, but on the completion of activities
- Work packages can be modified through amendments (e.g. to take into account new scientific developments)

CL3 Topics flagged for Lumps SUM



Ethics review

Same criteria as in H2020

For all activities funded, ethics is an integral part of research from beginning to end, and ethical compliance is essential to achieve real research excellence. An ethics review process is carried out systematically in all Horizon Europe proposals, based on a self-assessment included in the proposal.

Adapted following lessons learnt

Possible simplification of the process by

- Focusing mainly on complex/serious cases
- Optimising the number of ethics requirements in funded projects

Security scrutiny

New in Horizon Europe

Security issues will be checked systematically in all Horizon Europe proposals (in H2020 only proposals submitted to topics flagged as 'security-sensitive' were checked). The checks are based on a self-assessment included in the proposal.

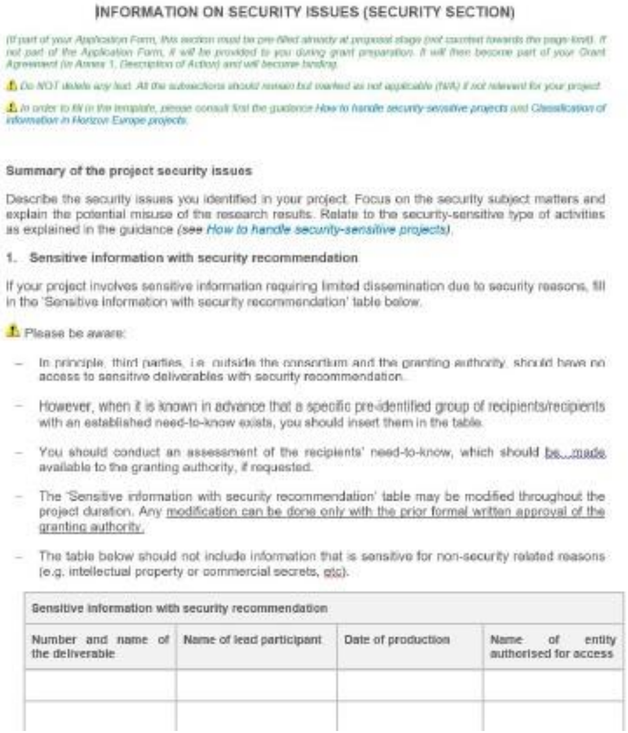
The checks based on the self-assessment may trigger an in-depth security scrutiny

Security scrutiny – Annex

Annex to fill in and include in your proposal (mandatory)

The focus is on:

- Whether the proposal uses or generates **EU classified information**
- Potential of **misuse of results** (that could be channeled into crime or terrorism)
- Whether activities involve information or materials **subject to national security restrictions**



INFORMATION ON SECURITY ISSUES (SECURITY SECTION)

(If part of your Application Form, this section must be pre-filled already at proposal stage (not counted towards the page limit). If not part of the Application Form, it will be provided to you during grant preparation. It will then become part of your Grant Agreement (in Annex 1, Description of Action) and will become binding.

⚠ *Do NOT delete any text. All the subsections should remain but marked as not applicable (N/A) if not relevant for your project.*

⚠ *In order to fill in the template, please consult first the guidance How to handle security-sensitive projects and Classification of information in Horizon Europe projects.*

Summary of the project security issues

Describe the security issues you identified in your project. Focus on the security subject matters and explain the potential misuse of the research results. Relate to the security-sensitive type of activities as explained in the guidance *(see How to handle security-sensitive projects)*.

1. Sensitive information with security recommendation

If your project involves sensitive information requiring limited dissemination due to security reasons, fill in the 'Sensitive information with security recommendation' table below.

⚠ Please be aware:

- In principle, third parties, i.e. outside the consortium and the granting authority, should have no access to sensitive deliverables with security recommendation.
- However, when it is known in advance that a specific pre-identified group of recipients/recipients with an established need-to-know exists, you should insert them in the table.
- You should conduct an assessment of the recipients' need-to-know, which should be made available to the granting authority, if requested.
- The 'Sensitive information with security recommendation' table may be modified throughout the project duration. Any modification can be done only with the prior formal written approval of the granting authority.
- The table below should not include information that is sensitive for non-security related reasons (e.g. intellectual property or commercial secrets, etc).

Sensitive information with security recommendation			
Number and name of the deliverable	**Name of lead participant**	**Date of production**	**Name of entity authorised for access**

Artificial intelligence (1/2)

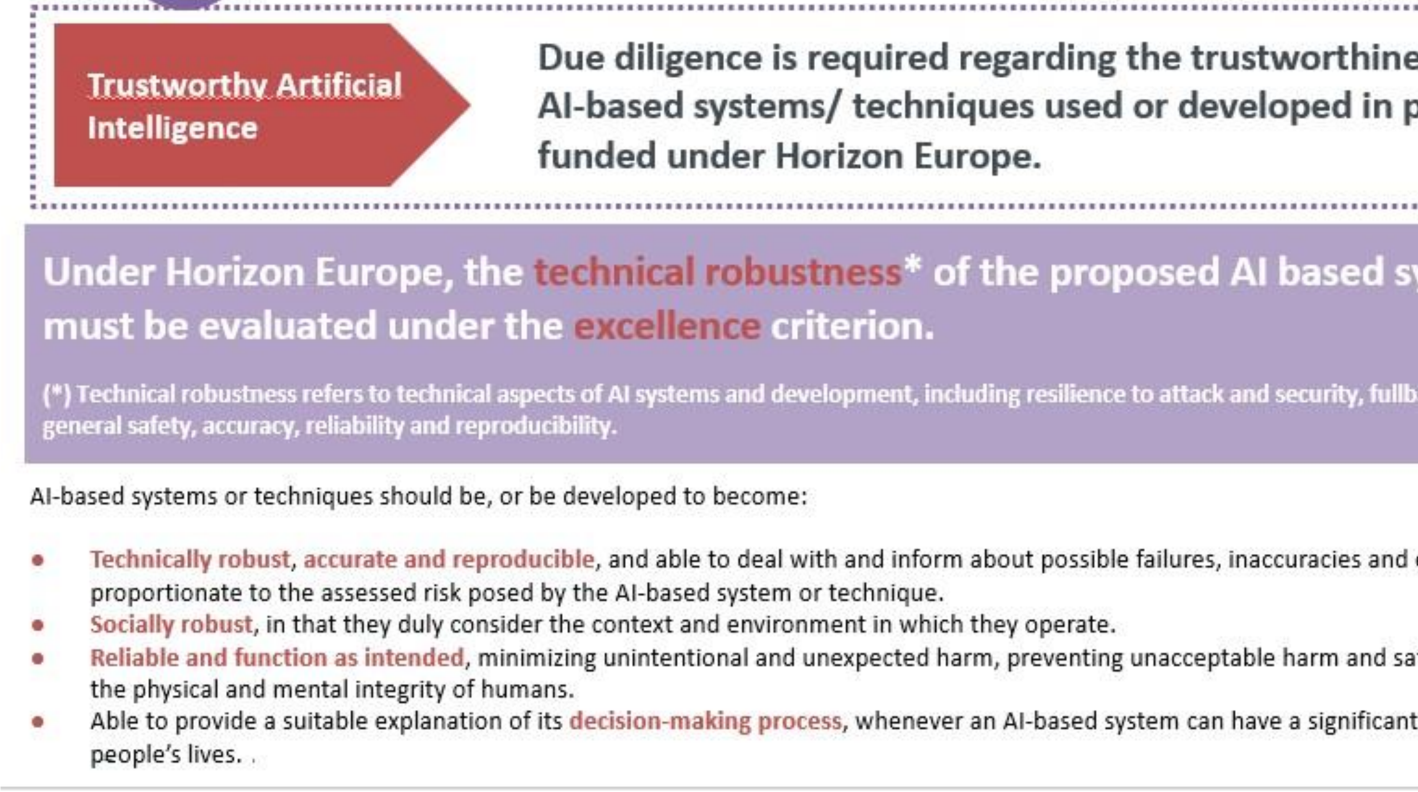
Attention with the ethical aspects and, i.e., software accountability, potential ethical biases, etc..

- Experts must answer an additional question as part of their individual evaluations on whether the activities proposed involve the **use and/or development of AI-based systems and/or techniques**.
- The aim is to bring to **experts' attention** that they must **assess the technical robustness** of the proposed AI-system as part of the excellence criterion (if applicable).
- Also the answer to this question aims at ensuring a **proper follow-up** of any aspects related to **Artificial Intelligence** in projects funded under Horizon Europe.

Under Horizon Europe, the technical robustness* of the proposed AI based systems is evaluated under the excellence criterion.

(*) Technical robustness refers to technical aspects of AI systems and development, including resilience to attack and security, fullback plan and general safety, accuracy, reliability and reproducibility.

Artificial intelligence (2/2)



Trustworthy Artificial Intelligence

Due diligence is required regarding the trustworthiness of all AI-based systems/ techniques used or developed in projects funded under Horizon Europe.

Under Horizon Europe, the technical robustness* of the proposed AI based systems must be evaluated under the excellence criterion.

(*) Technical robustness refers to technical aspects of AI systems and development, including resilience to attack and security, fullbac general safety, accuracy, reliability and reproducibility.

AI-based systems or techniques should be, or be developed to become:

- Technically robust, accurate and reproducible, and able to deal with and inform about possible failures, inaccuracies and er proportionate to the assessed risk posed by the AI-based system or technique.
- Socially robust, in that they duly consider the context and environment in which they operate.
- Reliable and function as intended, minimizing unintentional and unexpected harm, preventing unacceptable harm and safe the physical and mental integrity of humans.
- Able to provide a suitable explanation of its decision-making process, whenever an AI-based system can have a significant i people's lives. .

INDEPENDENT
HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE
SET UP BY THE EUROPEAN COMMISSION
AI
ETHICS GUIDELINES FOR TRUSTWORTHY AI

file:///F:/W72/CCAAs/2021/03Jun_EVALUATION/ai_hleg_ethics_guidelines_for_trustworthy_ai-en_87F84A41-A6E8-F38C-BFF661481B40077B_60419.pdf

Gender dimension in R&I content (1/3)

Gender Dimension

Addressing the gender dimension in research and innovation entails taking into account sex and gender in the whole research & innovation process.

The integration of the gender dimension into R&I content is mandatory, unless it is explicitly mentioned in the topic description

Why is gender dimension important?

- Why do we observe differences between women and men in infection levels and mortality rates in the COVID-19 pandemic?
- Does it make sense to study cardiovascular diseases only on male animals and on men, or osteoporosis only on women?
- Does it make sense to design car safety equipment only on the basis of male body standards?
- **Is it responsible to develop AI products that spread gender and racial biases due to a lack of diversity in the data used in training AI applications?**
- Is it normal that household travel surveys, and thus mobility analysis and transport planning, underrate trips performed as part of caring work?
- Did you know that pheromones given off by men experimenters, but not women, induce a stress response in laboratory mice sufficient to trigger pain relief?
- And did you know that climate change is affecting sex determination in a number of marine species and that certain populations are now at risk of extinction?

Gender Equality Plan (2/3)

For calls with deadlines in 2022 and onwards, having a Gender Equality Plan (GEP) will be an eligibility criterion for all public bodies, higher education institutions and research organisations from EU Member States and associated countries wishing to participate in Horizon Europe.

Mandatory requirements for a GEP

1. Be a public document
2. Have dedicated resources
3. Include arrangements for data collection and monitoring
4. Be supported by training and capacity-building

Gender Equality Plan (3/3)

Five thematic areas are recommended for content:

1. **Work-life balance** and organisational culture
2. **Gender balance in leadership** and decision-making
3. **Gender equality in recruitment** and career progression
4. Integration of the **gender dimension into research** and teaching content
5. **Measures against gender-based violence** including sexual harassment

The Commission's gender equality strategy: https://ec.europa.eu/info/research-and-innovation/strategy/strategy-2020-2024/democracy-and-rights/gender-equality-research-and-innovation_en

Horizon Europe guidance on gender equality plans: https://op.europa.eu/en/publication-detail/-/publication/ffcb06c3-200a-11ec-bd8e-01aa75ed71a1

The Gender Equality Plan eligibility criterion in Horizon Europe: Who is concerned? How to comply with it? (23 June 2022) (europa.eu)

Frequently Asked Questions:
https://ec.europa.eu/info/sites/default/files/research_and_innovation/strategy_on_research_and_innovation/documents/ec_rtd_gep-faqs.pdf

Dual use and Exclusive focus on civil applications

- Participants will have to confirm, as part of the **declarations in proposal part A** that the proposal has an exclusive focus on civil applications. Activities intended to be used in military application or aiming to serve military purposes cannot be funded.

- In H2020 the assessment of the '**dual use**' and '**exclusive focus on civil applications**' was part of the ethics review of the proposal.

- **In Horizon Europe:**

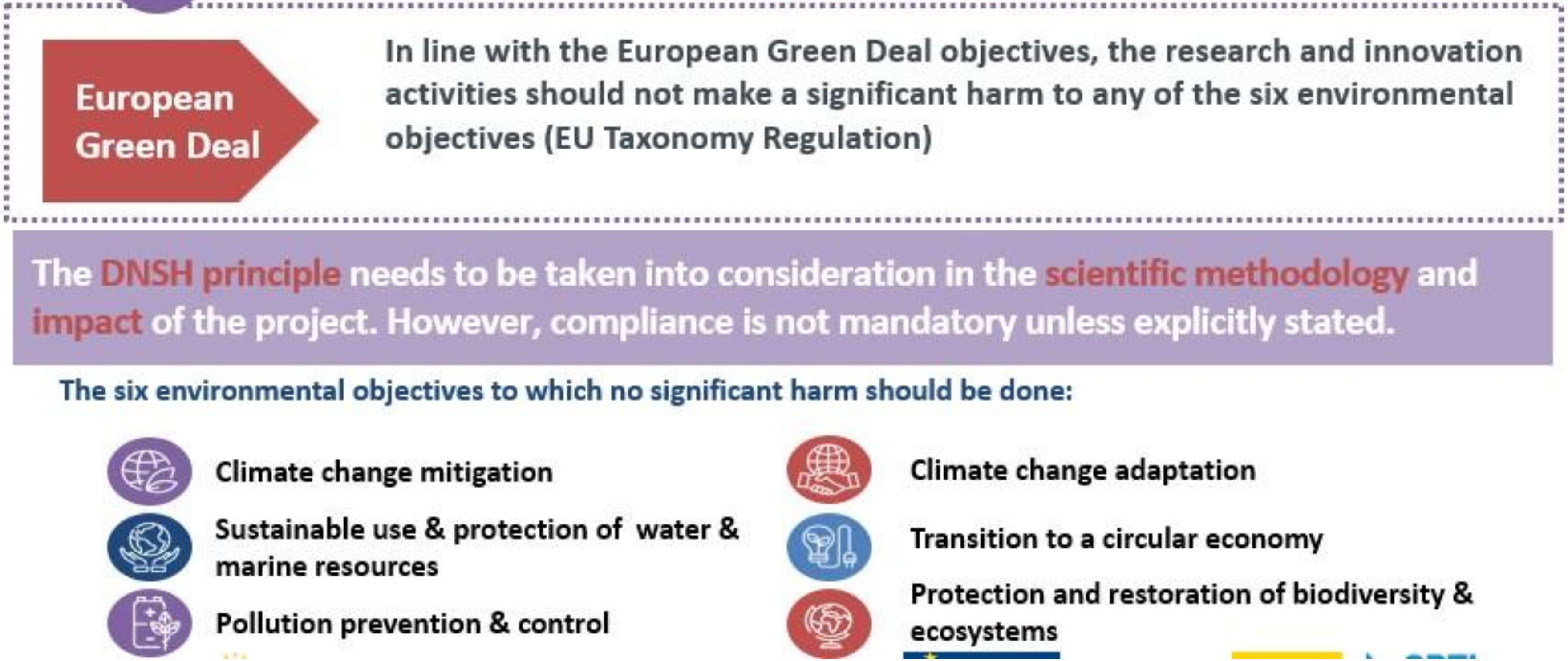
  - the assessment on '**exclusive focus on civil applications'** aspects is carried out by the technical evaluators in the form of additional question to their individual assessment of proposals.

  - For '**dual use**', we do not ask an additional question for experts in the evaluation. The declaration mentioned above will be sufficient with no further checks in evaluation or grant management.

- See also: [guidance-note-research-focusing-exclusively-on-civil-applications_he_en.pdf (europa.eu)]()

The approach to follow for the question on 'exclusive focus on civil applications' is the same as the process for activities not eligible for funding. Opinion of experts indicating if removing the activities that do not have an exclusive focus on civil applications would lead to lower evaluation scores.

El principio "Do no significant harm (DNSH)"



European Green Deal

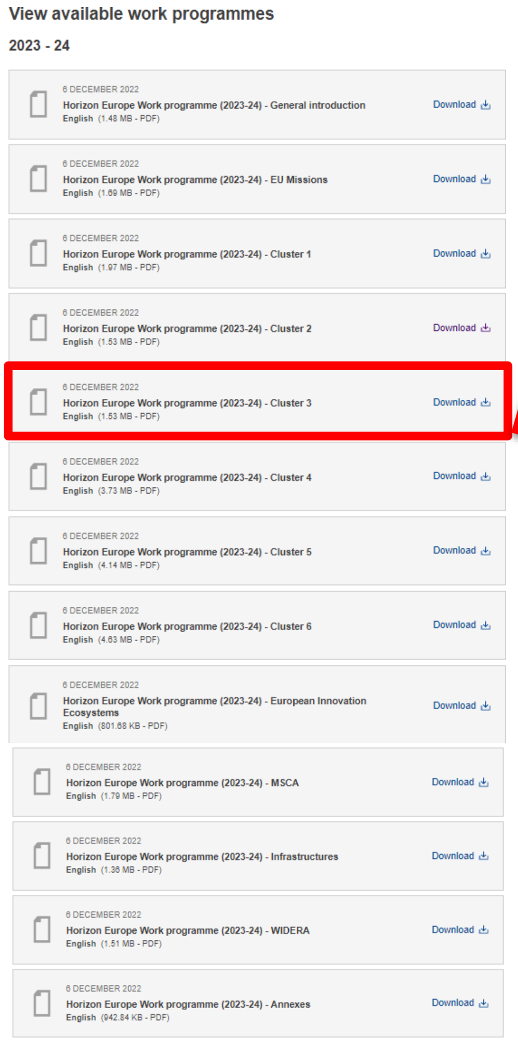
In line with the European Green Deal objectives, the research and innovation activities should not make a significant harm to any of the six environmental objectives (EU Taxonomy Regulation)

The DNSH principle needs to be taken into consideration in the scientific methodology and impact of the project. However, compliance is not mandatory unless explicitly stated.

The six environmental objectives to which no significant harm should be done:

- Climate change mitigation
- Sustainable use & protection of water & marine resources
- Pollution prevention & control
- Climate change adaptation
- Transition to a circular economy
- Protection and restoration of biodiversity & ecosystems

Documentación y enlaces de interés



View available work programmes

2023 - 24

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - General introduction
English (1.48 MB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - EU Missions
English (1.69 MB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - Cluster 1
English (1.97 MB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - Cluster 2
English (1.53 MB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - Cluster 3
English (1.53 MB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - Cluster 4
English (3.73 MB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - Cluster 5
English (4.14 MB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - Cluster 6
English (4.63 MB - PDF)
Download

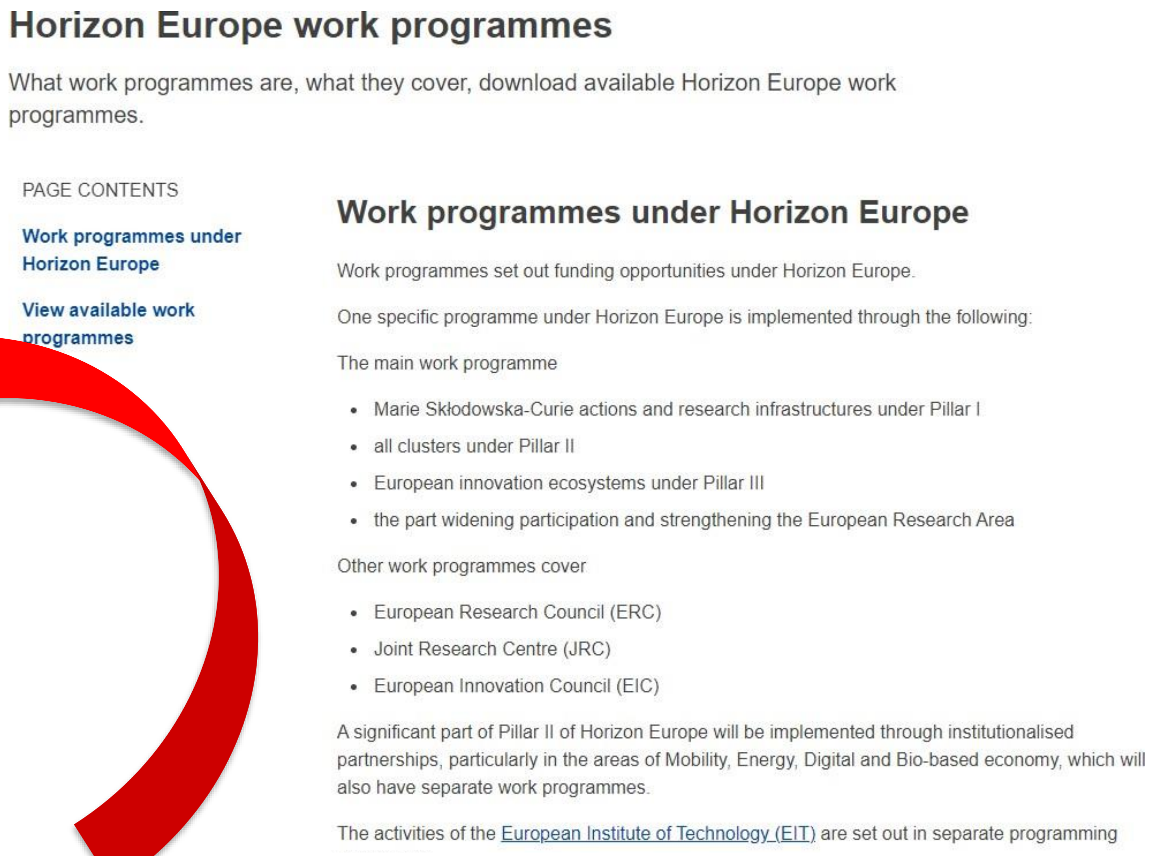
6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - European Innovation Ecosystems
English (801.68 KB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - MSCA
English (1.79 MB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - Infrastructures
English (1.36 MB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - WIDERA
English (1.51 MB - PDF)
Download

6 DECEMBER 2022
Horizon Europe Work programme (2023-24) - Annexes
English (942.84 KB - PDF)
Download



Horizon Europe work programmes

What work programmes are, what they cover, download available Horizon Europe work programmes.

PAGE CONTENTS

Work programmes under Horizon Europe

View available work programmes

Work programmes under Horizon Europe

Work programmes set out funding opportunities under Horizon Europe.

One specific programme under Horizon Europe is implemented through the following:

The main work programme

- Marie Skłodowska-Curie actions and research infrastructures under Pillar I
- all clusters under Pillar II
- European innovation ecosystems under Pillar III
- the part widening participation and strengthening the European Research Area

Other work programmes cover

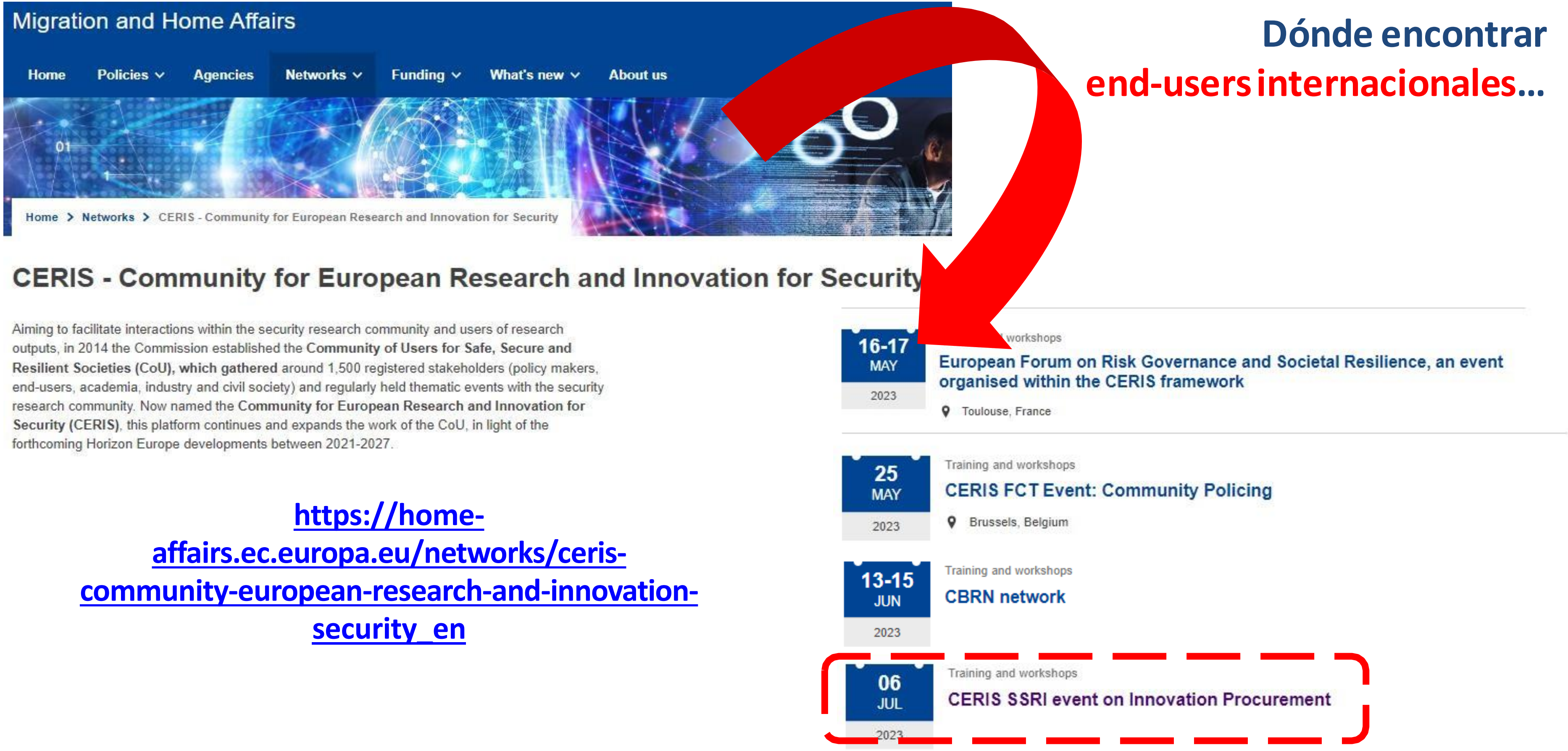
- European Research Council (ERC)
- Joint Research Centre (JRC)
- European Innovation Council (EIC)

A significant part of Pillar II of Horizon Europe will be implemented through institutionalised partnerships, particularly in the areas of Mobility, Energy, Digital and Bio-based economy, which will also have separate work programmes.

The activities of the European Institute of Technology (EIT) are set out in separate programming

https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/horizon-europe-work-programmes_en

Dónde encontrar
end-users internacionales…



Migration and Home Affairs

Home > Networks > CERIS - Community for European Research and Innovation for Security

CERIS - Community for European Research and Innovation for Security

Aiming to facilitate interactions within the security research community and users of research outputs, in 2014 the Commission established the **Community of Users for Safe, Secure and Resilient Societies (CoU), which gathered** around 1,500 registered stakeholders (policy makers, end-users, academia, industry and civil society) and regularly held thematic events with the security research community. Now named the **Community for European Research and Innovation for Security (CERIS)**, this platform continues and expands the work of the CoU, in light of the forthcoming Horizon Europe developments between 2021-2027.

16-17 MAY 2023
workshops
European Forum on Risk Governance and Societal Resilience, an event organised within the CERIS framework
Toulouse, France

25 MAY 2023
Training and workshops
CERIS FCT Event: Community Policing
Brussels, Belgium

13-15 JUN 2023
Training and workshops
CBRN network

06 JUL 2023
Training and workshops
CERIS SSRI event on Innovation Procurement

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

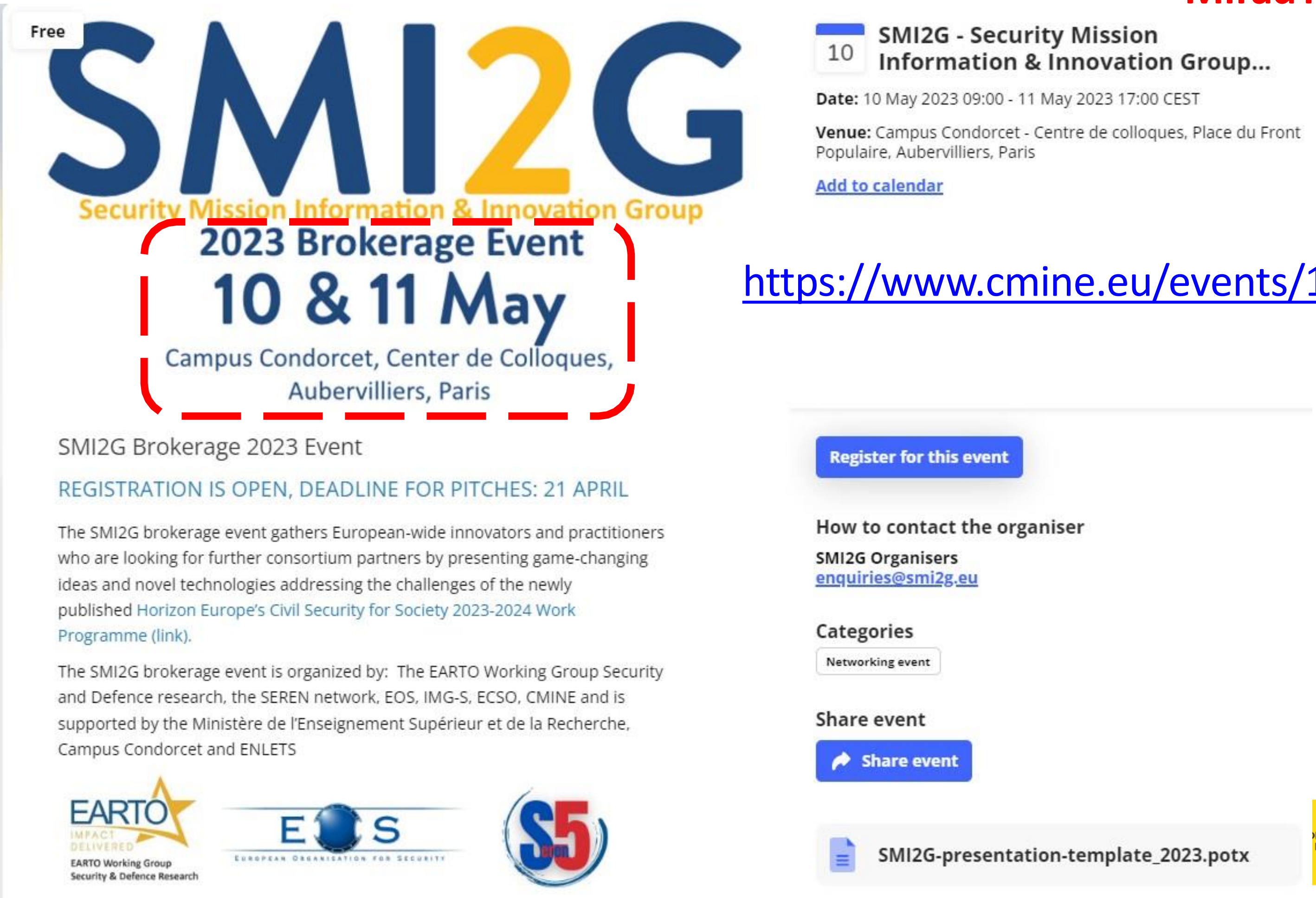
HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI INNOVACIÓN

Mirad los "elevator pitches"!



Free

SMI2G

Security Mission Information & Innovation Group

2023 Brokerage Event

10 & 11 May

Campus Condorcet, Center de Colloques,
Aubervilliers, Paris

SMI2G Brokerage 2023 Event

REGISTRATION IS OPEN, DEADLINE FOR PITCHES: 21 APRIL

The SMI2G brokerage event gathers European-wide innovators and practitioners who are looking for further consortium partners by presenting game-changing ideas and novel technologies addressing the challenges of the newly published Horizon Europe's Civil Security for Society 2023-2024 Work Programme (link).

The SMI2G brokerage event is organized by: The EARTO Working Group Security and Defence research, the SEREN network, EOS, IMG-S, ECSO, CMINE and is supported by the Ministère de l'Enseignement Supérieur et de la Recherche, Campus Condorcet and ENLETS

EARTO IMPACT DELIVERED EARTO Working Group Security & Defence Research

EOS European Organisation for Security

S5 seren

10 SMI2G - Security Mission Information & Innovation Group...

Date: 10 May 2023 09:00 - 11 May 2023 17:00 CEST

Venue: Campus Condorcet - Centre de colloques, Place du Front Populaire, Aubervilliers, Paris

Add to calendar

Register for this event

How to contact the organiser

SMI2G Organisers
enquiries@smi2g.eu

Categories

Networking event

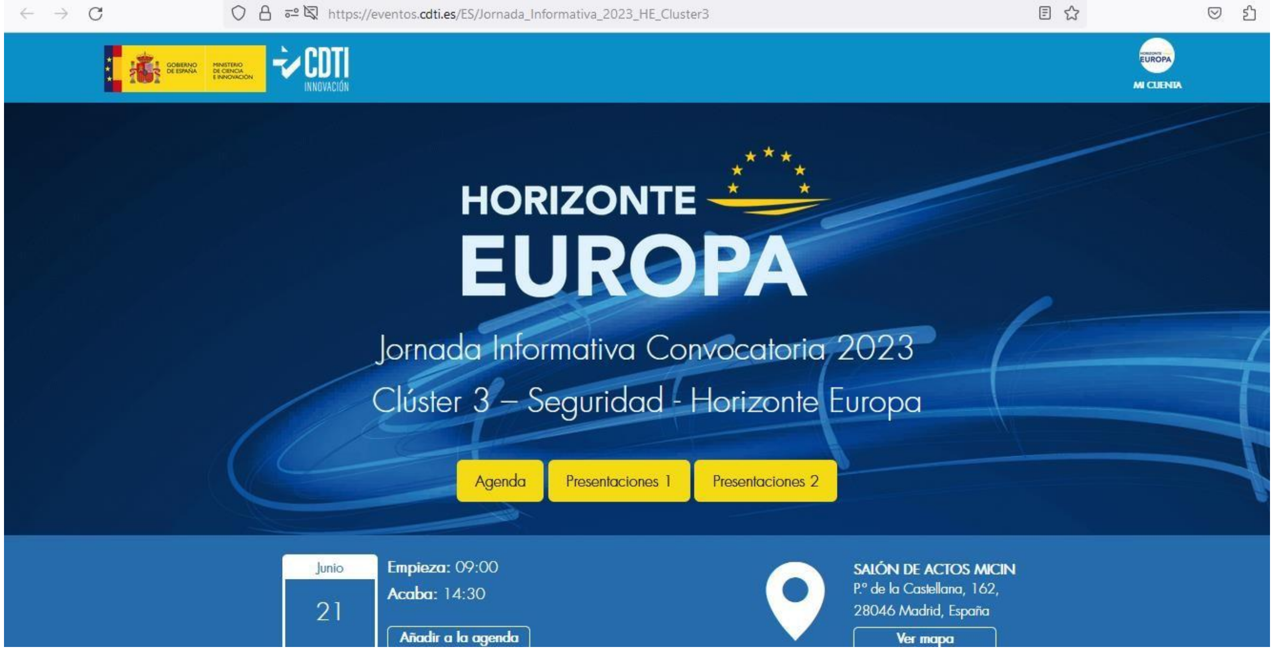
Share event

Share event

SMI2G-presentation-template_2023.potx

https://www.cmine.eu/events/107590

Infoday nacional CDTI – 21/6/2023



https://eventos.cdti.es/ES/Jornada_Informativa_2023_HE_Cluster3

HORIZONTE EUROPA

Jornada Informativa Convocatoria 2023

Clúster 3 – Seguridad - Horizonte Europa

Junio 21

Empieza: 09:00

Acaba: 14:30

SALÓN DE ACTOS MICIN
P.º de la Castellana, 162,
28046 Madrid, España

https://eventos.cdti.es/ES/Jornada_Informativa_2023_HE_Cluster3

Save the Date - Info Days for Horizon Europe Cluster 3 (Civil Security for Society) to take place on 27-28 June 2023 in Brussels

security research

27 June 2023, 09:30 CEST - 28 June 2023, 17:00 CEST

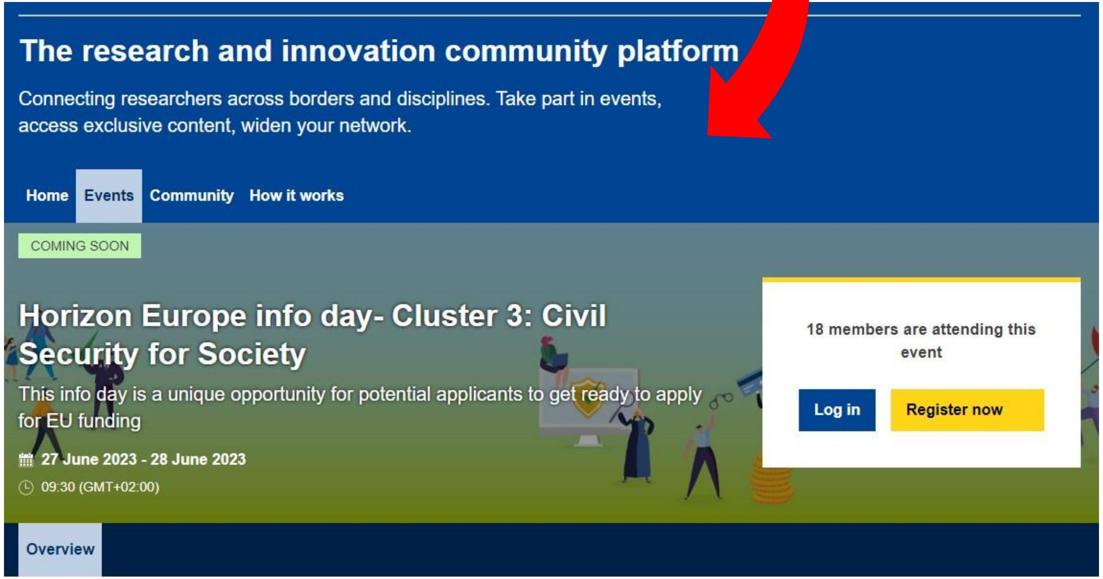
Country Belgium

Through Horizon Europe Cluster 3 "Civil Security for Society", the European Commission funds research and innovation projects to address the challenges arising from persistent security threats. These projects relate to the fight against crime and terrorism, external and border security, disaster resilience, cybersecurity and the protection of critical infrastructure.

The European Commission adopted the Cluster 3 Work Programme 2023 – 2024 in December 2022, and then revised in March 2023 to increase available budget by €50 to add new research topics and fund more projects, over the next two years.

The Calls for proposals under the Work Programme 2023 are now due to open on 29 June this year.

Researchers who wish to know more about the different research topics and the application procedure, including the legal and financial aspects to be taken into consideration, are invited to participate to the yearly "Cluster 3 Info Days and Brokerage Event" on 27 and 28 June 2023 respectively, in Brussels.



The research and innovation community platform

Connecting researchers across borders and disciplines. Take part in events, access exclusive content, widen your network.

COMING SOON

Horizon Europe info day- Cluster 3: Civil Security for Society

This info day is a unique opportunity for potential applicants to get ready to apply for EU funding

27 June 2023 - 28 June 2023

09:30 (GMT+02:00)

18 members are attending this event

https://home-affairs.ec.europa.eu/whats-new/events/save-date-info-days-horizon-europe-cluster-3-civil-security-society-take-place-27-28-june-2023-2023-06-27_en

Resultados de la convocatoria 2022

Resultados **provisionales** de España en la convocatoria 2022 CL 3 (I)

- España participa en: 29 proyectos, de los 43 financiados (67,4%)
- España coordina 5 de ellos (11,6%)
- Los **usuarios españoles están presentes en 19 de los 29 proyectos con participación española (66%)**
- **España: 2º país en términos de retorno económico (14,10% UE)**, tras Grecia (14,8%)

Resultados **provisionales** de España en la convocatoria 2022 CL 3 (II)

- **Resultados por convocatoria:**
  - **HORIZON-CL3-2022-CS-01-01** → **España ha sido el 1er país** con una tasa de retorno del **16,36 % UE**
  - **HORIZON-CL3-2022-DRS-01-01** → **España también ha sido el 1er país** con un retorno de un **15,3% UE**.
  - **HORIZON-CL3-2022-BM-01-01** →**España ha sido el 2º país** con un retorno del **16,9 % UE**
- **Entidades más destacadas:** FUNDACIÓN TECNALIA y la UNIVERSIDAD POLITÉCNICA DE CATALUNYA (ambas con 1,6 M€), la UNIVERSIDAD DE ALCALÁ DE HENARES, la UNIVERSIDAD DE MURCIA, el CSIC, TELEFÓNICA I+D y la UNIVERSIDAD POLITÉCNICA DE MADRID, todas ellas por encima del millón de euros en retornos.
- **Resultados por tipo de entidad:** Empresas (37% de la financiación), universidades (29,3%), centros de innovación y tecnología (11,6), administraciones públicas (7,4%), asociaciones de investigación (6,2 %), centros públicos de investigación (6%) y asociaciones (2,5%).

HORIZONTE EUROPA
@HorizonteEuropa

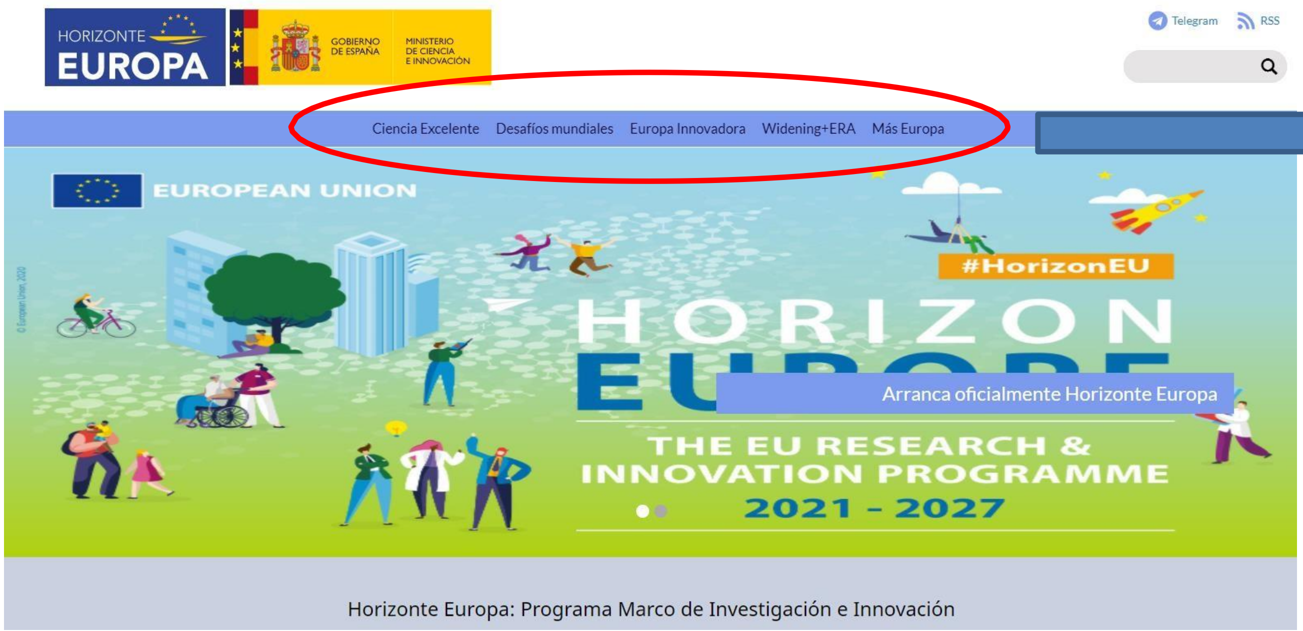
División de Programas de la UE

GOBIERNO DE ESPAÑA | MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI INNOVACIÓN

Cómo os ayudamos

Portal Horizonte Europa en español



Ciencia Excelente Desafíos mundiales Europa Innovadora Widening+ERA Más Europa

Arranca oficialmente Horizonte Europa

Horizonte Europa: Programa Marco de Investigación e Innovación

Eventos

Noticias

Documentos de interés

Enlaces de interés

www.horizonteeuropa.es

maite.boyero@cdti.es

marina.cdti@sost.be

ripaca@inta.es

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI INNOVACIÓN

LinkedIn

Grupo: Horizonte Europa Clúster 3 “Seguridad civil para la sociedad”

www.horizonteeuropa.es

maite.boyero@cdti.es

marina.cdti@sost.be

ripaca@inta.es

Canal de Telegram de Horizonte Europa

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI INNOVACIÓN

+info sobre programas y ayudas CDTI para proyectos de I+D empresarial e innovación

@CDTI_innovacion

HORIZONTE EUROPA

@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA

MINISTERIO DE CIENCIA E INNOVACIÓN

CDTI INNOVACIÓN