#innovacion
#ayudascdti
#asesoramiento
#internacionalizacion

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
CDTI INNOVACIÓN

Oportunidades Horizonte Europa Clúster 3
Convocatoria 2024

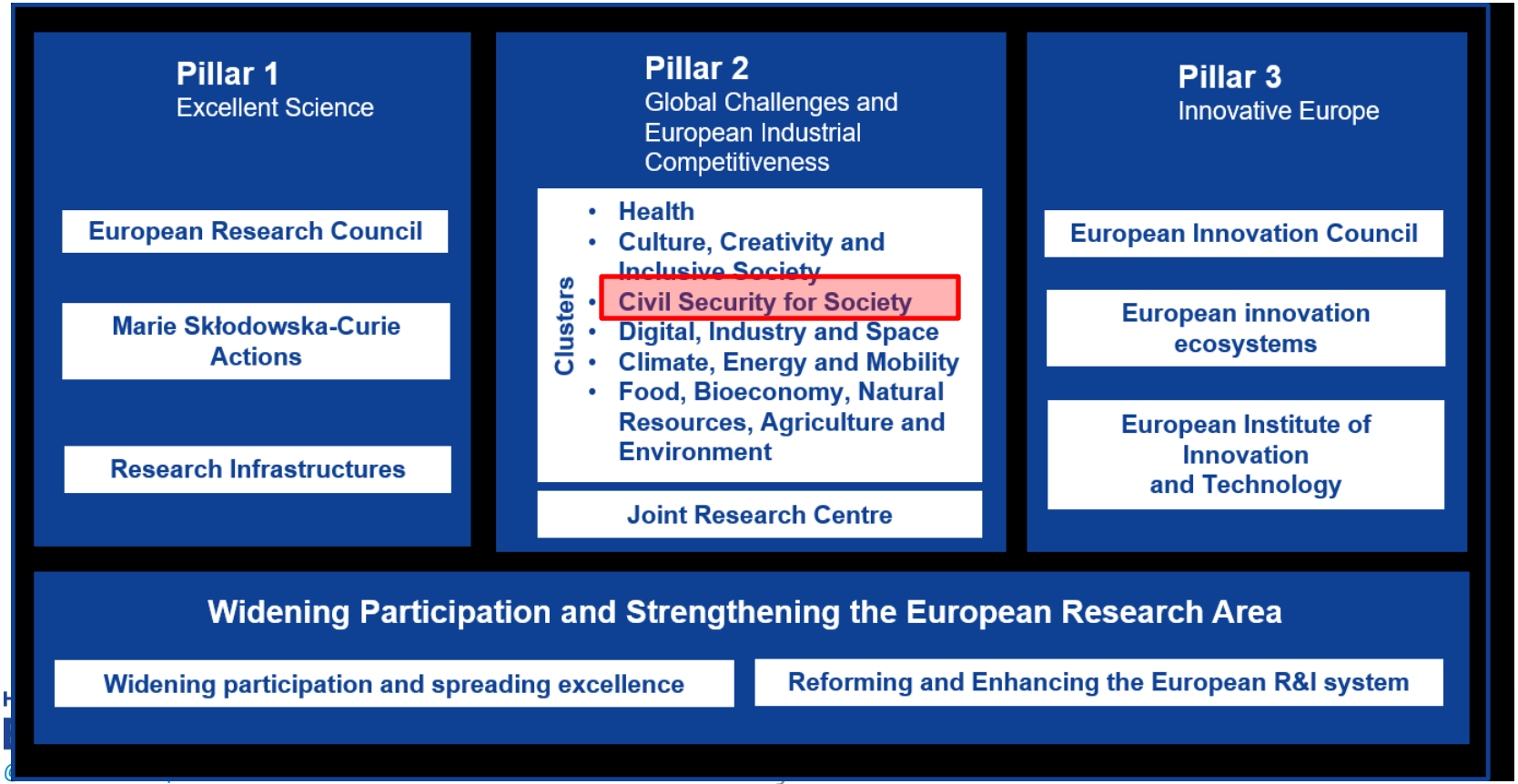
HORIZONTE EUROPA
@HorizonteEuropa

Dra Marina Martínez García
NCP Clúster 3
marina.cdti@sost.be

Centro para el Desarrollo Tecnológico y la Innovación


EUROPEAN UNION
#HorizonEU
HORIZON EUROPE
THE EU RESEARCH & INNOVATION PROGRAMME
2021 - 2027
© European Union, 2020

Cluster-3 en Horizonte Europa → 1.600 M€, de un total de 95.500 M€ (números finales para 2025-2027 pendientes de publicación)



Retos geo-políticos

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

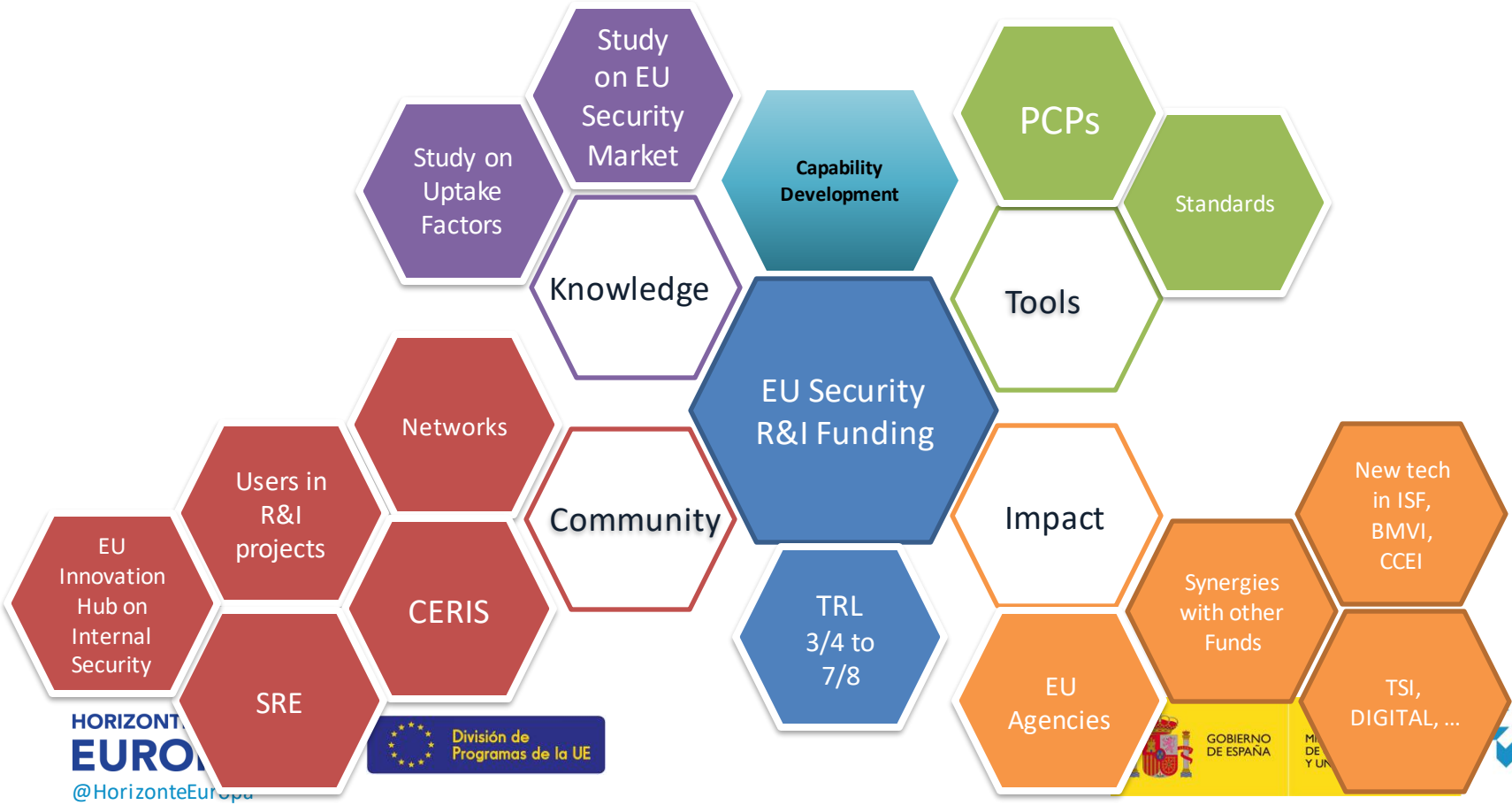
CDTI
INNOVACIÓN

Tendencias tecnológicas

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

El ecosistema de la Seguridad civil en la UE



HORIZONTE EUROPA

@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA

CDTI INNOVACIÓN

La Investigación y la Innovación son parte de la solución

- **Los Retos trans-nacionales** requieren **Cooperación trans-nacional**
  - Crimen organizado, terrorismo, cíber-amenazas/ataques, crisis y catástrofes, desastres naturales, gestión de las fronteras de la UE
  - Diferencia entre Seguridad (civil) y Defensa
- Alinear **los programas de I+D con las prioridades políticas de la UE**
- **Rol de la UE** como apoyo a los Estados Miembro, a través de los programas de I+D+i:
  - Claro valor añadido
  - Acciones que permitan la llegada a mercado de resultados de I+D e incrementar la competitividad del mercado y de la industria de la UE
  - Enfocar el programa en las necesidades de los Usuarios finales
  - Desarrollar un enfoque basado en dotar de "Capacidades" a Usuarios finales

Una Seguridad civil fuerte en la UE permite evitar una escalada hacia conflictos mayores → resulta esencial continuar con el Desarrollo de tecnologías y herramientas avanzadas para dotar de capacidades a los Usuarios finales de seguridad

HORIZONTE EUROPA
@HorizonteEuropa

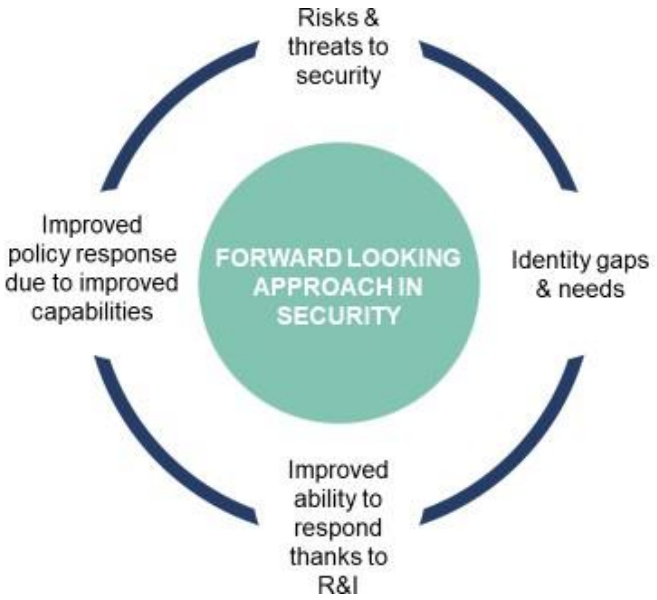
División de Programas de la UE

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

CDTI INNOVACIÓN

La ambición del programa: el “capability-driven approach”

- De una aproximación reactiva a una proactiva: **prospectiva, prevención y anticipación**



Challenges:

COVID, extreme weather events, pressure at external borders, crime, terrorist attacks, hybrid attacks etc.

Use tools & actors

referred to in Commission staff working document (2021) 422 final: CERIS, EU Innovation Hub for Internal Security, EU agencies etc.

Support policy response

response in disaster resilience, fight against crime & terrorism, critical infrastructure protection, border management, cyber security.

Principales Políticas y Estrategias de la UE en materia de Seguridad

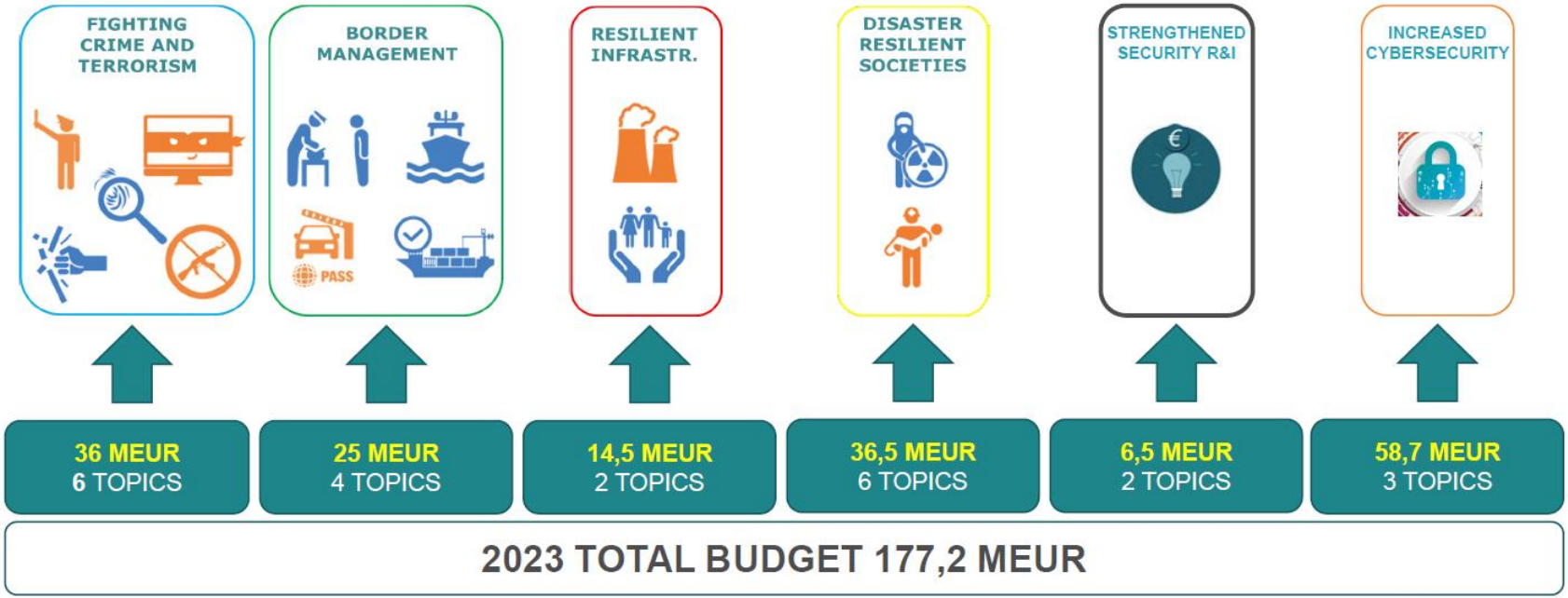
- **EU Security Strategy (2020-2025)**

- **EU Cybersecurity strategy (2020)**

- **EU Economic Security package (2023 – 2024…)**
  - **Research Security**
  - **Enhancing support for R&D involving technologies with dual-use potential**

Algunos resultados de la convocatoria 2023

“Civil Security for Society” Work Programme 2023



European Commission

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

CDTI INNOVACIÓN

2023 Calls – Proposals overview

247 proposals submitted

- ✓ **1 Inadmissible**
- ✓ **32 Ineligible**
- ✓ **214 Evaluated**

13.36% ineligible/inadmissible

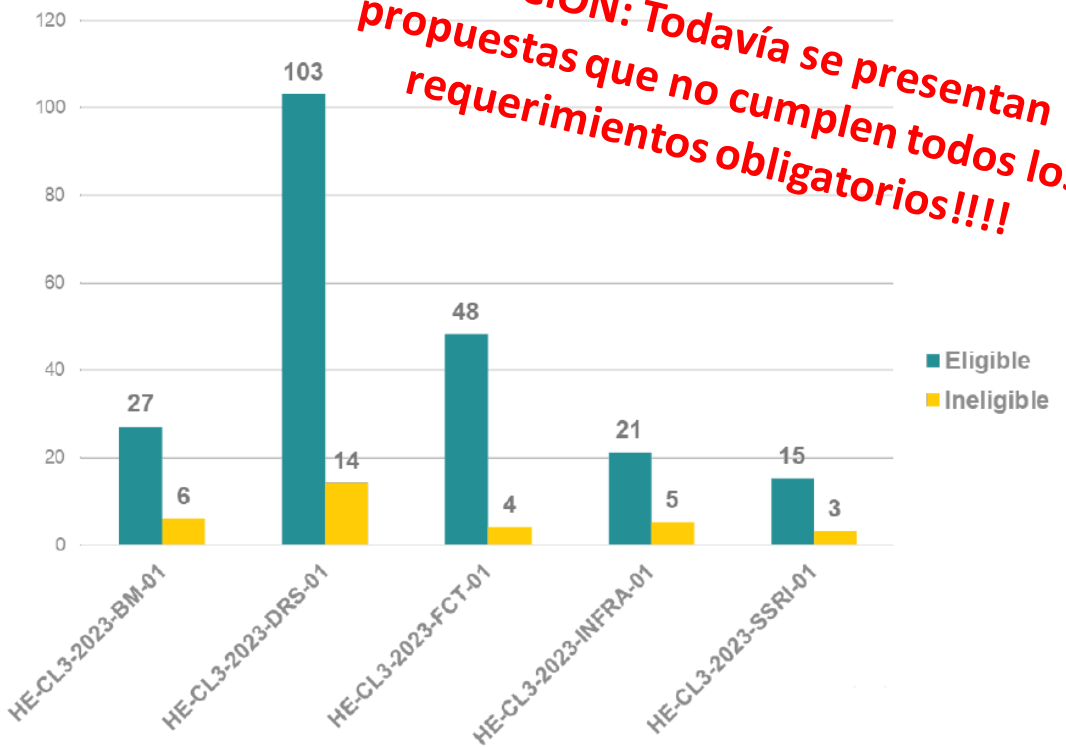
In 2022:

245 proposals submitted

- ✓ 4 Inadmissible
- ✓ 23 Ineligible
- ✓ 218 Evaluated

11% ineligible/inadmissible

ATENCIÓN: Todavía se presentan propuestas que no cumplen todos los requerimientos obligatorios!!!!



*(Not including: 32 Independent Rapporteurs, 35 Ethics Experts, 1 Observer)

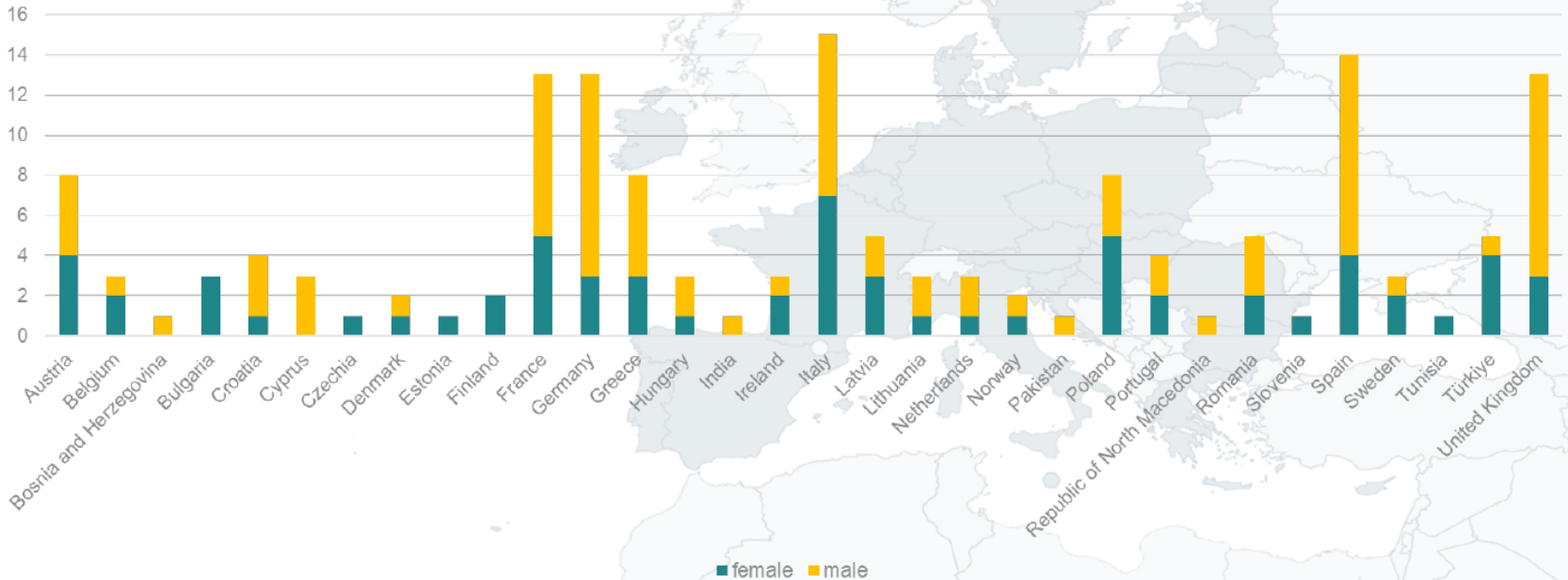
Evaluators – Nationality

Ya están pidiendo evaluadores para la call-2024!!

153 Evaluators* - 44% female

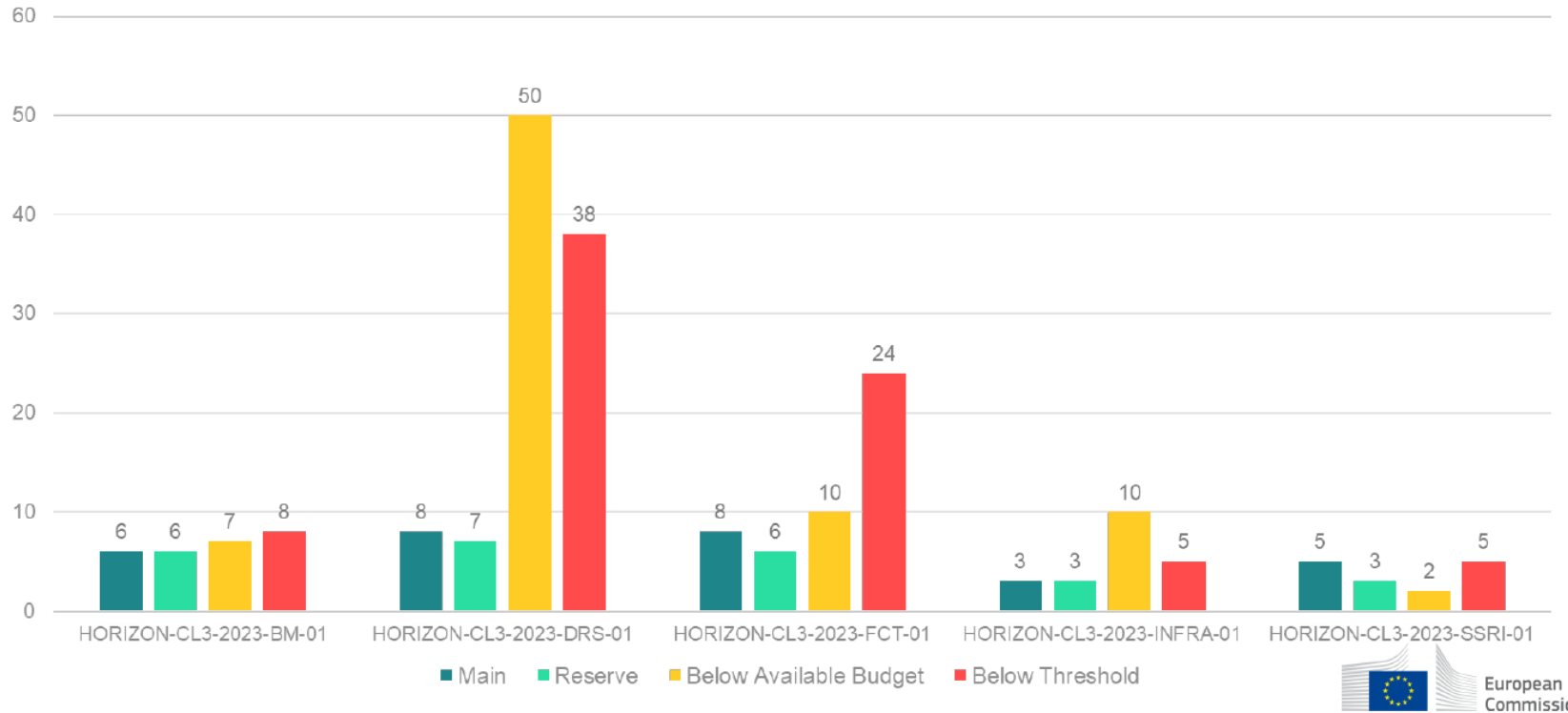
All EU MSs represented except Luxembourg, Malta, and Slovakia, 32 Countries in total

✓ 128 (83.7%) from EU Member States - 9 (5.9%) from Associated Countries - 16 (10.4%) from Third Countries



Evaluation Outcome per call

30 proposals in the main list, **25** in reserve list, **79** proposals below the available budget and **80** below threshold



European Commission

Participation – Main list (All Calls)

446 applications, 390 applications from EU Member States, 19 from Associated Countries, 37 from Third Countries

425 Coordinators and Beneficiaries – 15 Associated Partners – 6 Affiliated entities

Resultados **provisionales** de España en la convocatoria 2023 CL 3 (I)

- España participa en 27 proyectos, de los 42 financiados (64,3%)
- España coordina 4 de ellos (11,9%)
- **España: 3er país en términos de retorno económico (10,2% UE)**, tras Grecia (17,2%) y Alemania (11,1%)

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

Resultados **provisionales** de España en la convocatoria 2023 CL 3 (II)

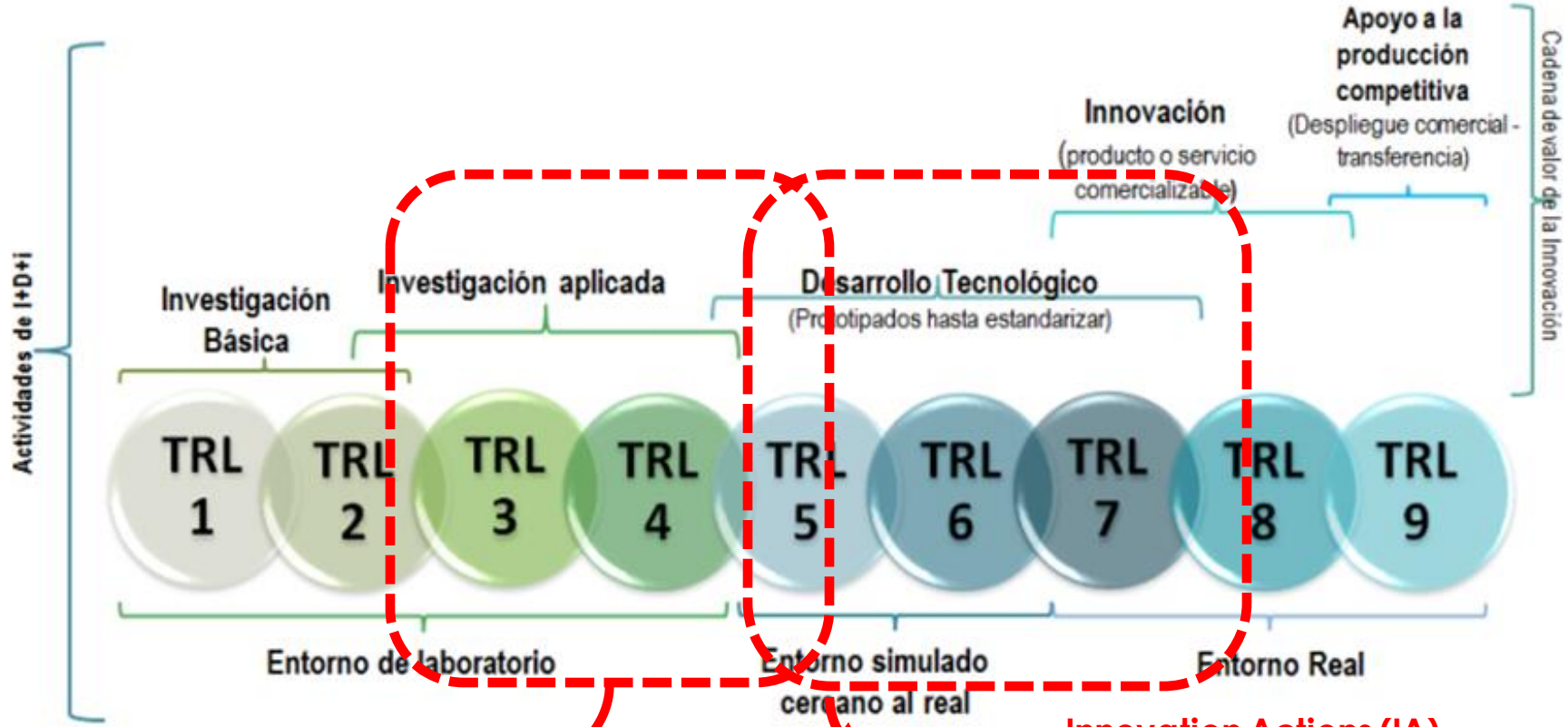
- **Resultados por convocatoria:**
  - **HORIZON-CL3-2023-SSRI-01** → **España ha sido el 1er país** con una tasa de retorno del **18 % UE**
  - **HORIZON-CL3-2023-FCT-01** → **España ha sido el 2º país** con un retorno de un **18,9% UE**.
  - **HORIZON-CL3-2023-CS-01** → **España ha sido el 3er país** con un retorno del **10,3 % UE**
- **Entidades más destacadas:** TELEFÓNICA I+D, GRADIANT y TREE TECHNOLOGY (todas por encima de 1M€), VICOMTECH, MION TECHNOLOGIES, POLICÍA LOCAL DE VALENCIA, **UNIVERSIDAD DE MURCIA**, **Policía de Murcia…**.
- **Resultados por tipo de entidad:** Empresas (44% de la financiación), centros de innovación y tecnología (15%), administraciones públicas (15%), universidades (13%), …

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA

La Convocatoria 2024



Resarch & Innovation actions (RIA)

Upto 100% funding rate for all

Innovation Actions (IA)

Upto 100% for Non-Profit & upto 70% for profit

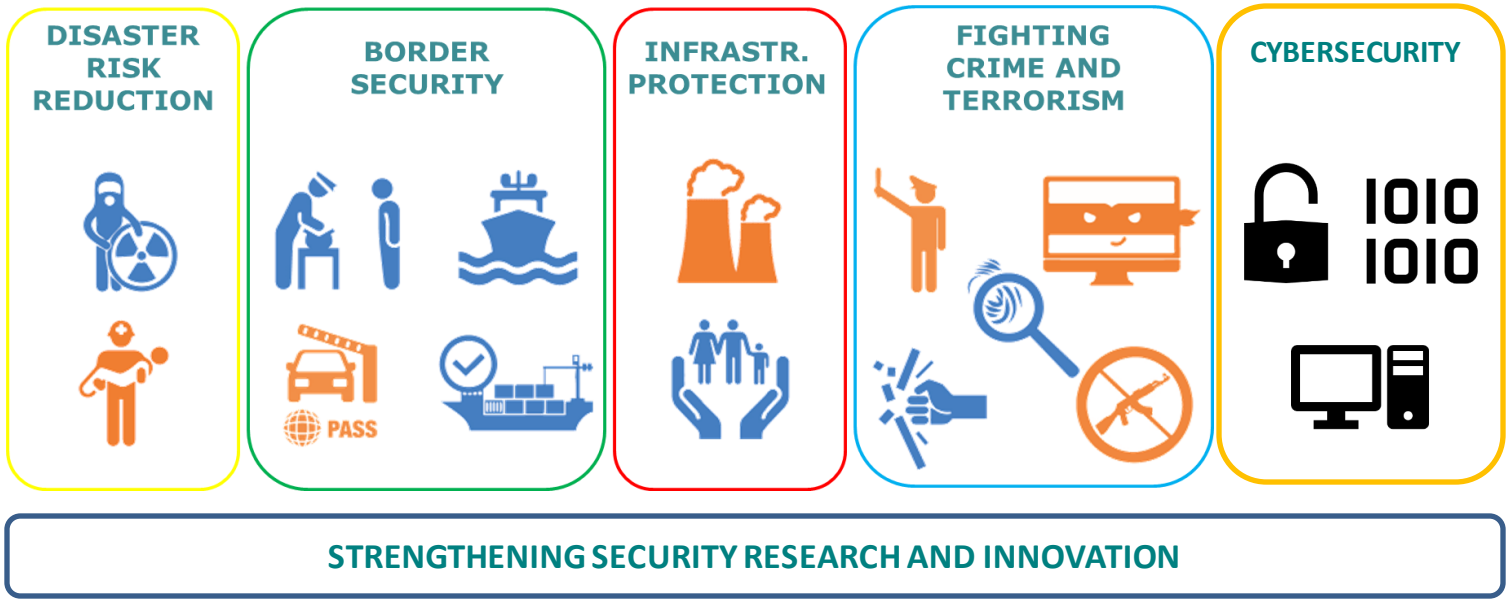
HORIZONTE EUROPA
@HorizonteEuropa

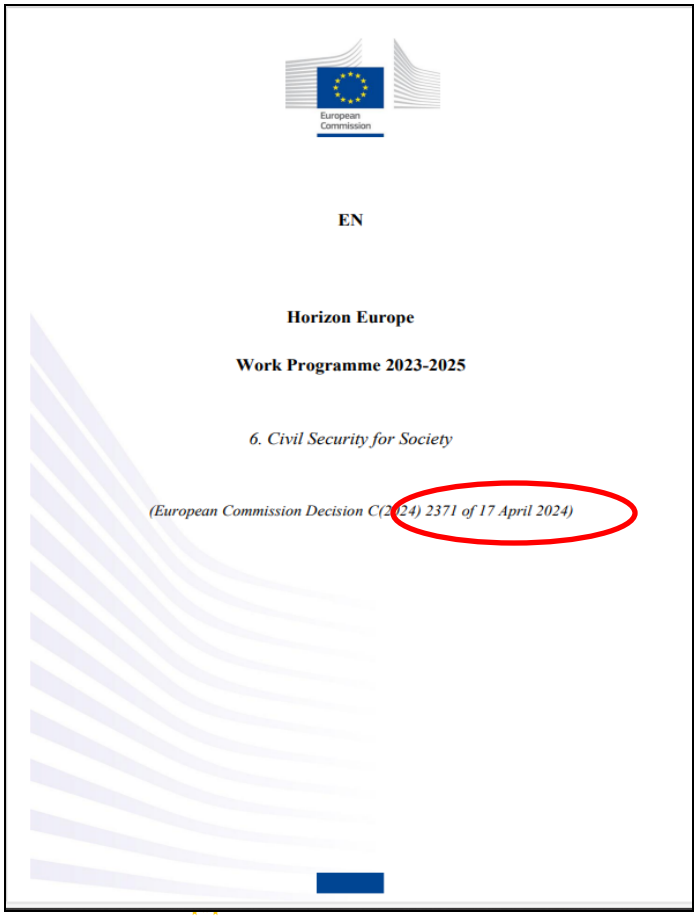
División de Programas de la UE

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

CDTI INNOVACIÓN

Estructura del Programa de Trabajo: 6 "*Destinations*"





- **Convocatoria 2024:**
  - Abre: 27 Junio de 2024
  - **Cierra: 20 Noviembre, 2024**, 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

OJO: VERSIÓN DEFINITIVA DESDE EL 17/04/2024

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

CDTI INNOVACIÓN

Principales modificaciones en el WP-2024: Limitaciones en la participación de los "High risk suppliers"

14-Mar-2024

[…]**New eligibility condition devised to prevent the participation of "high risk supplier entities" in actions that are relevant to the development of technologies linked to the evolution of European communication networks**.

This new eligibility condition, based on **article 22(6) of the Horizon Europe regulation […].**→ https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox

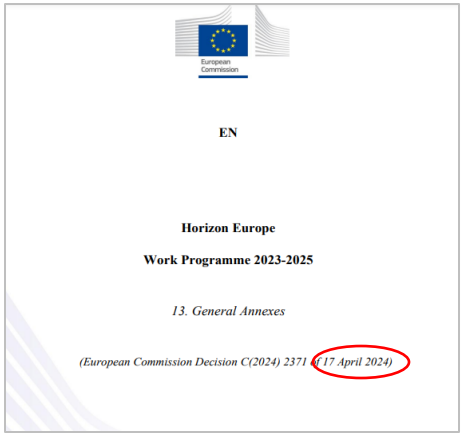
The protection of European communication networks has been identified as an important security interest of the Union and its Member States and the development of future network technologies and European capacities in this area by leveraging the EU research and innovation framework programme is seen as a strategic risk mitigation measure. This entails the need to avoid the participation of "high-risk supplier entities" in the development of technologies linked to the evolution of European communication networks to prevent technology transfer and the persistence of dependencies.

Following in-depth discussions within the Commission and with Member State representatives in the Horizon Europe strategic programme committee, this new eligibility condition will be inserted in the General Annexes of the amended 2023-2024 Horizon Europe work programme. […] **A specific topic condition, namely "Subject to restrictions for the protection of European communication networks",** will also be added to those upcoming actions in the various work programme parts that have been identified by Commission services as being relevant for this new eligibility condition.

As a result, "high risk supplier entities" will not be eligible to participate in 35 top-down topics of the amended work programme and in a number of bottom-up MSCA actions.

Topics afectados call-2024 por las limitaciones de participación de « high-risk supplier entities » en Horizon Europe

- ✓ 35 actions concerned
  - Cluster 1 – 1 action concerned
  - **Cluster 3 – 19 actions concerned within the call-2024**
  - Cluster 4 – 1 action concerned
  - Cluster 5 – 8 actions concerned
  - Cluster 6 – 1 action concerned
  - Missions – 5 actions concerned



EN

Horizon Europe

Work Programme 2023-2025

13. General Annexes

(European Commission Decision C(2024) 2371 of 17 April 2024)

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-13-general-annexes_horizon-2023-2024_en.pdf

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

CDTI INNOVACIÓN

Qué dicen los General Annexes sobre los "High risk suppliers" …

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-13-general-annexes_horizon-2023-2024_en.pdf

Restrictions for the protection of European communication networks — The protection of European communication networks has been identified as an important security interest of the Union and its Member States.[10] In line with the Commission Recommendation on the cybersecurity of 5G networks of 2019[11] and the subsequent report on EU coordinated risk assessment of the cybersecurity of 5G networks of 2019, [12] the EU Toolbox on 5G cybersecurity, [13] the second report on Member States' progress in implementing the EU toolbox on 5G cybersecurity of 2023,[14] and the related Communication on the implementation of the 5G cybersecurity toolbox of 2023,[15] the Commission together with the Member States has worked to jointly identify and assess cyberthreats and security risks for 5G networks.[16] The toolbox also recommends adding country-specific information (e.g. threat assessment from national security services, etc.). This work is an essential component of the Security Union Strategy and supports the protection of electronic communications networks and other critical infrastructures.

Entities assessed as "high-risk suppliers", are currently set out in the second report on Member States' progress in implementing the EU toolbox on 5G cybersecurity of 2023[17] and the related Communication on the implementation of the 5G cybersecurity toolbox of 2023[18].

The toolbox also underlines that further developing European capacities in the area of 5G and post-5G technologies by leveraging EU Research & Innovation Funding programmes is a strategic risk mitigating measure. This entails the need to avoid the participation of high-risk supplier entities in the development of other technologies linked to the evolution of European communication networks to prevent technology transfer and the persistence of dependencies in materials, semiconductor components (including processors), computing resources, software tools and virtualisation technologies, as well as related cybersecurity.

In order to protect the specific policy requirements of the Union and/or its Member States, it is therefore appropriate that the following additional eligibility criteria apply to actions identified as "subject to restrictions for the protection of European communication networks" and to proposals within the MSCA part [19] that concern the evolution of European communication networks (5G, post-5G and other technologies linked to the evolution of European communication networks):

Entities that are assessed as high-risk suppliers of mobile network communication equipment (and any entities they own or control) are not eligible to participate as beneficiaries, affiliated entities and associated partners.

The assessment is based on the following criteria:

- likelihood of interference from a non-associated third country, for example due to:
  - the characteristics of the entity's ownership or governance (e.g. state-owned or controlled, government/party involvement);
  - the characteristics of the entity's business and other conduct (e.g. a strong link to a third country government);
  - the characteristics of the respective third country (e.g. legislation or government practices likely to affect the implementation of the action, including an offensive cyber/intelligence policy, pressure regarding place of manufacturing or access to information).
- (cyber-)security practices, including throughout the entire supply chain;
- risks identified in relevant assessments of Member States and third countries as well as other EU institutions, bodies and agencies, if relevant.

Exceptions may be requested from the granting authority and will be assessed case-by-case, taking into account the criteria provided for in the 5G cybersecurity toolbox, the security risks and availability of alternatives in the context of the action.

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

CDTI INNOVACIÓN

Pero, ¿quiénes son los “high risk suppliers”?

https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox

HORIZONTE EUROPA
@HorizonteEuropa

POLICY AND LEGISLATION | Publication 15 June 2023

Communication from the Commission: Implementation of the 5G cybersecurity Toolbox

The Commission has adopted a Communication on the implementation of the toolbox by Member States and in the EU's own corporate communications and funding activities.

The Commission takes note of and welcomes the adoption of the Second Progress report on the implementation of the EU Toolbox by the NIS Cooperation Group.

In light of this report, the Commission is strongly concerned by the risks posed by certain suppliers of mobile network communication equipment to the security of the Union, as reflected also by decisions taken by some Member States. The NIS Report highlights the ‘clear risk of persisting dependency on high-risk suppliers in the internal market with potentially serious negative impacts on security for users and companies across the EU and the EU’s critical infrastructure’.

As mentioned in the NIS Progress Report and in an earlier report by the European Court of Auditors, it is evident that 5G suppliers exhibit clear differences in their characteristics, in particular as regards their likelihood of being influenced by specific third countries which have security laws and corporate governance that are a potential risk for the security of the Union. As also indicated in the NIS report, Huawei and ZTE have been subject to public decisions and advice in certain Member States, based on national security concerns, including assessments by those Member States’ intelligence services.

In other Member States, decisions to restrict or exclude certain suppliers from their 5G networks have been made confidentially, based on their assessment. The findings of those Member States are similar to the analysis of the competent authorities of certain third countries.

Due to these high risks, and based on an assessment of the criteria set out in the Toolbox for identifying ‘high-risk suppliers’, the Commission considers that decisions adopted by Member States to restrict or exclude Huawei and ZTE are justified and compliant with the 5G Toolbox. Without prejudice to the Member States’ competences as regards national security, the Commission has also applied the Toolbox criteria to assess the needs and vulnerabilities of its own corporate communications systems and those of the other European institutions, bodies and agencies, as well as the implementation of Union funding programmes in the light of the Union’s overall policy objectives.

In this context, consistently with certain Member States’ application of the 5G Toolbox, the Commission considers, that Huawei and ZTE represent in fact materially higher risks than other 5G suppliers.

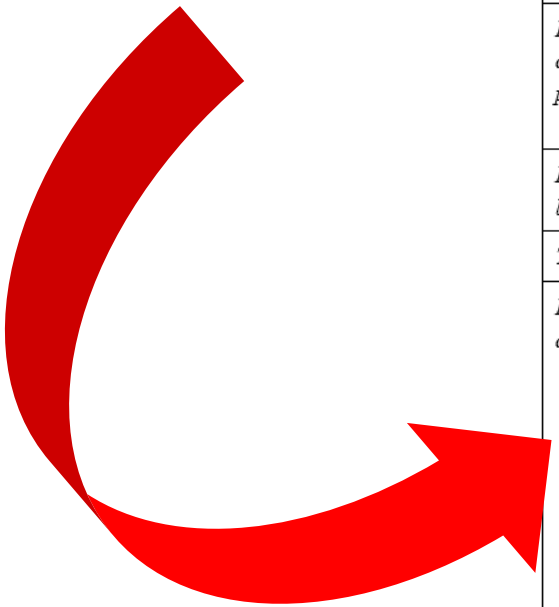
Related topics

Cybersecurity

Topics afectados call-2024 CL3 por las limitaciones de participación de « high-risk supplier entities » en Horizon Europe

TOPIC	TITLE
HORIZON-CL3-2024-BM-01-02	Interoperability for border and maritime surveillance and situational awareness
HORIZON-CL3-2024-BM-01-03	Advanced user-friendly, compatible, secure identity and travel document management
HORIZON-CL3-2024-BM-01-04	Integrated risk-based border control that mitigates public security risk, reduces false positives and strengthens privacy
HORIZON-CL3-2024-BM-01-05	Detection and tracking of illegal and trafficked goods
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-CL3-2024-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-01-03	Harmonised / Standard protocols for the implementation of alert and impact forecasting systems as well as transnational emergency management in the areas of high-impact weather / climatic and geological disasters
HORIZON-CL3-2024-DRS-01-04	Hi-tech capacities for crisis response and recovery after a natural-technological (NaTech) disaster
HORIZON-CL3-2024-DRS-01-05	Cost-effective sustainable technologies and crisis management strategies for RN large-scale protection of population and infrastructures after a nuclear blast or nuclear facility incident
HORIZON-CL3-2024-DRS-01-02	Open Topic
HORIZON-CL3-2024-FCT-01-01	Mitigating new threats and adapting investigation strategies in the era of Internet of Things
HORIZON-CL3-2024-FCT-01-03	Lawful evidence collection in online child sexual abuse investigations, including undercover
HORIZON-CL3-2024-FCT-01-07	CBRN-E detection capacities in small architecture
HORIZON-CL3-2024-FCT-01-08	Tracing of cryptocurrencies transactions related to criminal purposes
HORIZON-CL3-2024-INFRA-01-02	Resilient and secure urban planning and new tools for EU territorial entities
HORIZON-CL3-2024-INFRA-01-03	Advanced real-time data analysis used for infrastructure resilience
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

¿Dónde está la modificación de los topics afectados?



HORIZON-CL3-2024-FCT-01-03: Lawful evidence collection in online child sexual abuse investigations, including undercover

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 3.70 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 3.70 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility conditions apply: This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities[22] 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 application form with all the requested information, following the template provided in the submission IT tool. The following exceptions apply: subject to restrictions for the protection of European communication networks.
Technology Readiness Level	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

HE - Eligibility - Specific restrictions

- **Restrictions on participation in Innovation Actions**

Legal entities established in **China** are **not eligible** to participate in **Horizon Europe Innovation Actions** in any capacity. This includes participation as beneficiaries, affiliated entities, associated partners, third parties giving in-kind contributions, subcontractors or recipients of financial support to third parties (if any).

- **Restrictions for the protection of European communication networks**

Entities that are assessed as high-risk suppliers of mobile network communication equipment (and any entities they own or control) **are not eligible to participate as beneficiaries, affiliated entities and associated partners**. Entities assessed as "high-risk suppliers", are currently set out in the second report on Member States' progress in implementing the EU toolbox on 5G cybersecurity of 2023 and the related Communication on the implementation of the 5G cybersecurity toolbox of 2023.

HE - Eligibility - Specific restrictions

- **EU restrictive measures**

Entities subject to EU restrictive measures under Article 29 of the Treaty on the European Union (TEU) and Article 215 of the Treaty on the Functioning of the EU (TFEU)20 as well as Article 75 TFEU21, are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, third parties giving in-kind contributions, subcontractors or recipients of financial support to third parties (if any).

- **Other restrictive measures**

Legal entities established in Russia, Belarus, or in non-government controlled territories of Ukraine

Measures for the protection of the Union budget against breaches of the principles of the rule of law in Hungary

Others

Destination FCT:
Better protect the EU and its citizens against Crime & Terrorism

Destination Fighting Crime and Terrorism (FCT)

- **Prevención, investigación y mitigación** de los impactos de actos criminales (tb. cíber) y terroristas
- Seguridad en **espacios públicos urbanos**
- Apoyar a Fuerzas y Cuerpos de Seguridad

FCT sub-areas	Topics call-2024	EUR (M€)	EUR (M€) per grant	Type of Action / TRL	Eligibility Conditions (min)
Modern information analysis for fighting crime and terrorism	Mitigating new threats and adapting investigation strategies in the era of Internet of Things*	5	5	RIA / 5-6	3 Police Authorities
Improved forensics and lawful evidence collection	Open topic	9	4.5	RIA / 5-7	2 Police Authorities & 2 forensic institutes
	Lawful evidence collection in online child sexual abuse investigations, including undercover*	3.7	3,7	RIA / 5-6	2 Police Authorities & 2 forensic institutes
Enhanced prevention, detection and deterrence of societal issues related to various forms of crime	Radicalisation and gender	3	3	RIA / 5-6	3 Police Authorities
	Combating hate speech online and offline	3	3	IA / 6-7	2 Police Authorities & 2 Civil Society Organisations
	Open Topic	6	3	RIA / 5-6	3 Police Authorities
Increased security of citizens against terrorism, including in public spaces	CBRN-E detection capacities in small architecture*	6	6	IA / 6-8	2 Police Authorities & 2 urban municipalities
Citizens are protected against cybercrime	Tracing of cryptocurrencies transactions related to criminal purposes*	6	6	IA / 6-7	3 Police Authorities

***The following exceptions apply: subject to restrictions for the protection of European communication networks.**

HORIZONTE EUROPA
@HorizonteEuropa

Destination BM: Effective management of EU external borders

Destination BM/BS

- **Tráfico de pasajeros** (*flow of people*) **y Tráfico de mercancías** (*flow of goods*) en la UE

- Prevenir y contrarrestar el tráfico ilícito, la piratería y otros actos criminales y terroristas

- **Fronteras aéreas, terrestres y marítimas**

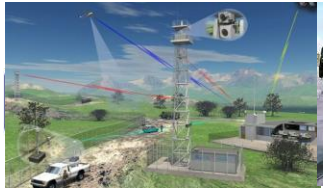
LUMP SUM funding format FOR ALL TOPICS IN BM THIS YEAR!

BM sub-areas	Topics – call 2024	EUR (M€)	EUR (M€) per grant	Type of Action / TRL	Eligibility Conditions (min)
	Open topic*	6	3	RIA / 4-6	2 Border or Coast Guards Authorities and/or Customs Authorities from at least 2 different EU Member States or Associated Countries.
Efficient border surveillance and maritime security	Interoperability for border and maritime surveillance and situational awareness**	6	6	IA	
Secured and facilitated crossing of external borders	Advanced user-friendly, compatible, secure identity and travel document management**	6	6	IA	
	Integrated risk-based border control that mitigates public security risk, reduces false positives and strengthens privacy**	5	5	IA	
Better customs and supply chain security	Detection and tracking of illegal and trafficked goods**	6	3	RIA	

***ATTENTION:** Proposals that address R&I themes or challenges already covered by other topics in HE Calls BM 2022-23-24 cannot be submitted.

****The following exceptions apply: subject to restrictions for the protection of European communication networks.**

HORIZONTE EUROPA
@HorizonteEuropa





Destination INFRA: Protected infrastructure

Destination Infrastructures

- **Resiliencia y autonomía**, ámbito físico y cíber de las Infraestructuras Críticas. **Sistemas de gran escala interconectados**

- **Seguridad en grandes eventos, smart cities, Infraestructuras urbanas**

- Abarca todo tipo de amenazas: **físicas, cíber e híbridas**.

LUMP SUM funding format FOR ALL TOPICS IN INFRA THIS YEAR!

INFRA sub-areas	Topics call-2024	EUR (M€)	EUR (M€) per grant	Type of Action / TRL	Eligibility Conditions (min)
Improved preparedness and response for large-scale disruptions of European infrastructures	Open topic	5	5	IA / 6-8	2 critical infrastructure operators & 2 civil protection authorities
Resilient and secure urban areas and smart cities	Resilient and secure urban planning and new tools for EU territorial entities*	6	6	IA / 6-8	2 local or regional government authorities
	Advanced real-time data analysis used for infrastructure resilience*	5	5	RIA / 5-6	3 infrastructure operators, which could include civil protection authorities **at national level**

***The following exceptions apply: subject to restrictions for the protection of European communication networks.**

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

Destination DRS:
A Disaster-resilient society for Europe

Destination DRS

- Prevención, mitigación, respuesta y recuperación ante **crisis y desastres (naturales, NBRQ-E, provocados por el hombre, asociados a cambio climático, pandemias, etc.)**
- **Coordinación** transfronteriza
- Servicios de emergencias y Protección civil europeos (NBRQ-E, eventos extremos, pandemias, etc.)




GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
CDTI INNOVACIÓN

DRS sub-areas	Topics call-2024	EUR (M€)	EUR (M€) per grant	Type of Action / TRL	Eligibility Conditions (min)
Improved Disaster Risk Management & Governance	Prevention, detection, response and mitigation of chemical, biological and radiological threats to **agricultural production, feed and food processing, distribution and consumption***	8	4	RIA	3 organisations: • at least 1 representing **citizens or local communities**; • at least 1 representing **practitioners** (1st and/or 2nd responders); • at least 1 representing **local or regional authorities**
	Open topic*	6	3	RIA	5 organisations: • At least 1 EU **city's crisis risk manager**; • at least 1 representing **citizens or local communities**; • at least 1 representing **practitioners** (1st and/or 2nd responders); • at least 1 representing **local or regional authorities**; • **Private sector**

***The following exceptions apply: subject to restrictions for the protection of European communication networks.**

DRS sub-areas	Topics call-2024	EUR (M€)	EUR (M€) per grant	Type of Action / TRL	Eligibility Conditions (min)
Improved harmonisation and/or standardisation in the area of crisis management & CBRN-E	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***	6	3	IA	3 organisations: • at least 1 representing Standardisation organisations,; • at least 1 representing practitioners (1st and/or 2nd responders); • at least 1 representing local or regional authorities
Strengthened capacities of first & second responders	Hi-tech capacities **for crisis response and recovery after a natural-technological (NaTech) disaster***	4	4	RIA / 5-7	• at least 1 local or regional authorities in charge of managing NaTech events; • at least 2 first responders' organisations or agencies
	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***	6	6	RIA / 6-8	• at least 1 local or regional authorities in charge of disaster response; • at least 2 first responders' organisations or agencies

***The following exceptions apply: subject to restrictions for the protection of European communication networks.**

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

Destination SSRI: Strengthened Security Research and Innovation

Destination Strengthening Security R&I

- Mejorar la **llegada a mercado** de los resultados de la I+D+i
- Incrementar el **impacto**
- Planificación y análisis de **necesidades** a medio-largo plazo

For ALL 2024-SSRI TOPICS: The following exceptions apply: subject to restrictions for the protection of EU communication networks.

SSRI sub-area	Topics call-2024	EUR (M€)	EUR (M€) per grant	Type of Action / TRL	Eligibility Conditions (min)
Increased innovation uptake	Demand-led innovation through public procurement (*)	10.5	5.25	**PCP** / 6-8	**3 end-user organisations & 3 public procurers from 3 different EU MS or AS**
	Accelerating uptake through open proposals for advanced SME innovation (**) 	6	1.5	IA / 6-7	Consortia must include, as beneficiaries: • From 3 to 7partners partners • **Min 2 SMEs** • Min 1 end-user At least 2 MS must be represented in the consortium

(*) Beneficiaries must ensure that the subcontracted work is performed in at least 3 MS — unless otherwise approved by the granting authority. → PCPs/PPIs based on the previous CSAs (i.e. call 2022).

(**) LUMP SUM funding format and 50% of the budgest must be allocated to SMEs; Participation of non-SME industries and RTOs must be limited to 15% of the budget.

Destination CS:
Increased Cybersecurity

Destination Cybersecurity

- Capacidades para la **autonomía estratégica**
- Reforzar las infraestructuras digitales, **ante ataques cíber e híbridos**
- Protección de datos, privacidad y ética

For ALL 2024-CS TOPICS: The following exceptions apply: subject to restrictions for the protection of EU communication networks.

Cybersecurity sub-areas	Topics call-2024	EUR (M€)	EUR (M€) per grant	Type of Action / TRL	Eligibility Conditions
Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures	Approaches and tools for security in software and hardware development and assessment **(*)**	37	4-6	IA	NA
Cryptography	Post-quantum cryptography transition	23,4	4-6	RIA	Topic limited to MS, AC & and OECD countries**(**)**

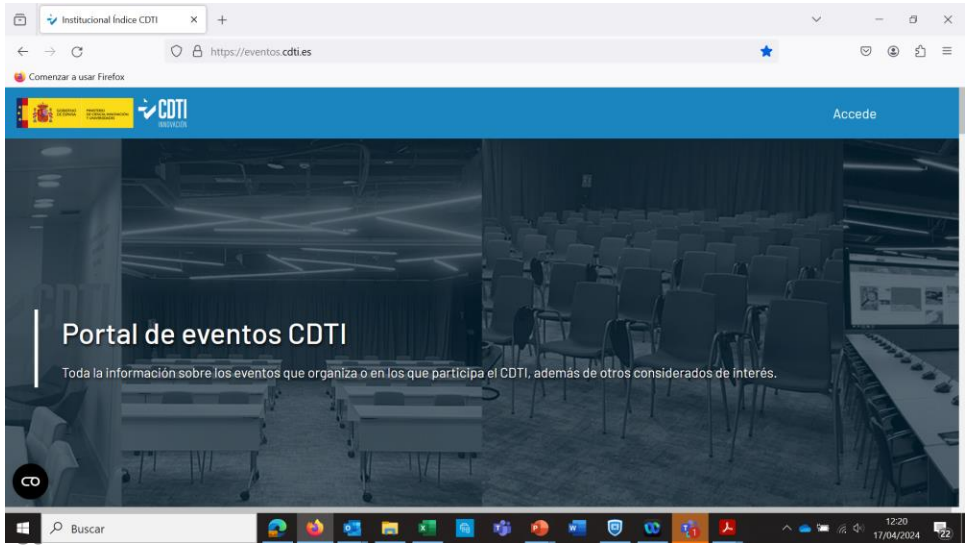
***LUMP SUM funding format**

****Proposals** including legal entities which are **not established in these countries will be ineligible**.

Last but not least…

Próximos eventos / infodays

- ✓ **Infoday nacional** → Madrid, **MAÑANA**, en el MCIU
- **Infodays regionales en Mayo-Junio** → Galicia (**HOY**), Cataluña, País Vasco, Andalucía… y Murcia!
- **Infoday Europeo + brokerage event (convocatoria 2024)** → Bruselas, **12 y 13 de junio**
- **eventos.cdti.es**



HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

https://www.cmine.eu/networks/events/123953

PRESENTACIONES DISPONIBLES A FINALES DE ESTA SEMANA!

22 **SMI2G - Security Mission Information & Innovation Group...**

Date: 22 May 2024 09:00 - 23 May 2024 17:00 CEST

Venue: Campus Cyber, Paris

Location: 5 Rue Bellini, 92800 Puteaux, France

Register for this event

How to contact the organiser

SMI2G Organisers
enquiries@smi2g.eu

Categories

Networking event

Share event

Share event

SMI2G_pitch_presentation-template_2024...

Instructions_for_presentations_2024.pdf

SMI2G_end-user_pitch-template_2024.pptx

Every year, SMI2G hosts top-level keynote speakers, expert panel discussions as well as ground-breaking pitch sessions related to the respective calls. As a result, the event offers participants significant networking opportunities, supporting consortium building efforts and the sharing of valuable information concerning the Horizon Europe Security Calls.

To attend in person

Simply register through this page and your request will be acknowledged.

If you'd like to present a pitch at the event...

- Given the limitations in the number of participants, the Organising Committee may have to select presenters based on the quality of their submitted pitch proposals.
- Please find the instructions for sending your pitches and the presentation template available as a download attached to this notice.
- The facility for submitting pitch presentations is limited to those we have time for so the faster you submit, the more chance there is of yours being included.
- The deadline for submitting pitch presentations is **29 March 2024**.
- You'll be notified if your request has been accepted **ultimately 26 April 2024**.

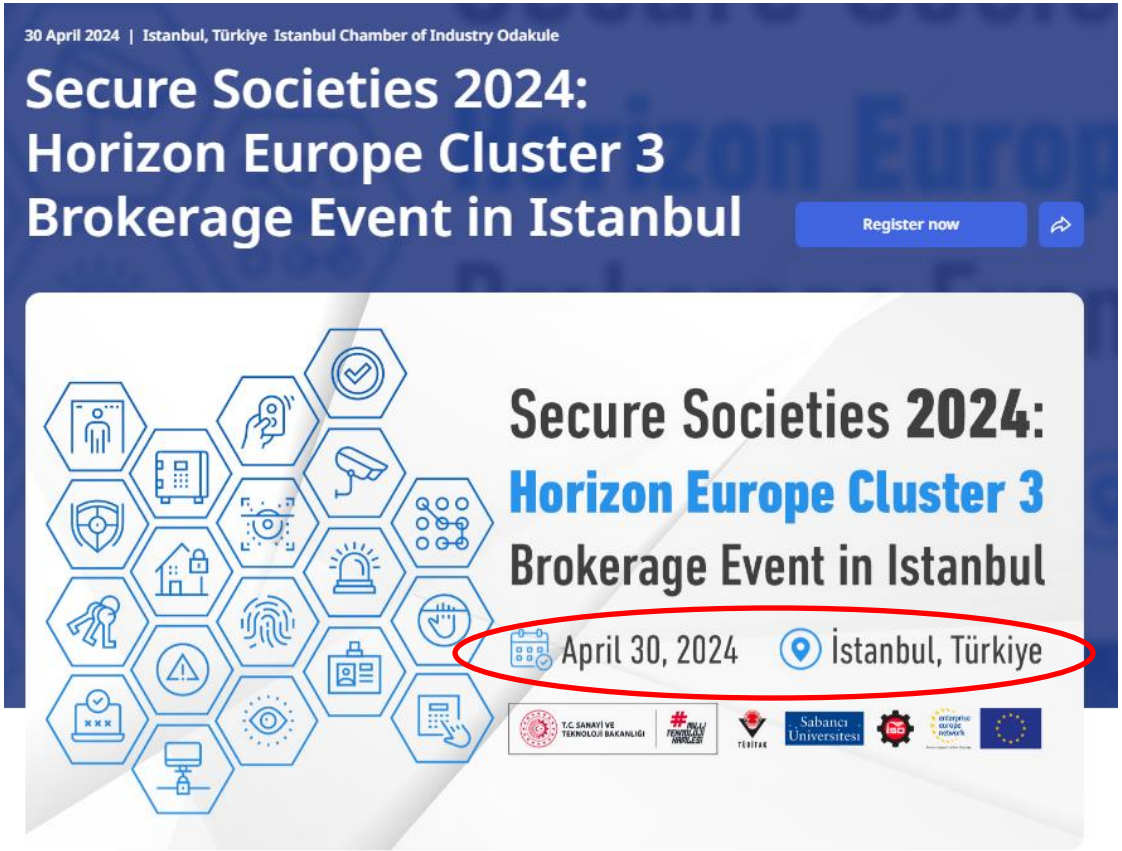
Presentations by potential coordinators will be preferred. Presentations by different organisations (rather than multiple presentations by a single organisation) will also be preferred.

Specifically for practitioner organisations:

- Practitioner organisations may have a broader interest in a particular destiination, covering multiple topics within one single destination. **Only for end-user organisations** we offer the possibility to have a more generic pitch presentation covering the interests they have in a specific destination.

Registration is now open till the maximum capacity per day of the event is reached.

https://www.b2match.com/e/horizon-europe-2024-secure-societies/components/38215/info



Herramienta B2Match todavía abierta para búsqueda de socios!!!!

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
CDTI INNOVACIÓN

Community for Research and Innovation for Security (CERIS)

European Commission

EN English

Search

Migration and Home Affairs

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

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.

The objectives of CERIS are to

- analyse identified **capability needs and gaps** in the corresponding areas
- identify **solutions** available to address the gaps
- translate capability gaps and potential solutions into **research needs**
- identify **funding opportunities and synergies** between different funding instruments
- identify **standardisation** research-related needs
- integrate the **views of citizens**

Subscribe to our mailing list

Thematic areas

Projects and Results

EU security market study

News

Events

About CERIS

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

CDTI INNOVACIÓN

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

CERIS events

ATENCIÓN: Próximos eventos antes de verano…

Filter by

Status

Select

Event date

Select

Subject

Select

Search | Clear filters

CERIS events (30) RSS

Showing results 1 to 10

25-26 JUN 2024

Training and workshops

The Projects to Policy Seminar (PPS)

External event

05-07 JUN 2024

Training and workshops

CERIS Annual Event 2024: Disaster-Resilient Societies – From Local to International Cooperation

SEREMAP: Herramienta de búsqueda de socios

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

HORIZONTE EUROPA
@HorizonteEuropa

CDTI INNOVACIÓN

Enlaces de interés

- Innovation and Security
- EU Security Market Study
- Study on the Factors Influencing the Uptake of EU-Funded Security Research Outcomes
- SEREN5 PROJECT (Red de NCPs Cluster 3)
- Proyectos financiados y otra información (REA)

maite.boyero@cdti.es

marina.cdti@sost.be

ripaca@inta.es

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

www.horizonteeuropa.es

Canal de Telegram “Horizonte Europa”

HORIZONTE EUROPA
@HorizonteEuropa

División de Programas de la UE

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

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, INNOVACIÓN Y UNIVERSIDADES

CDTI INNOVACIÓN