

#innovacion
#ayudascdti
#asesoramiento
#internacionalizacion

A world map composed of blue dots, with several red dots marking specific locations across the continents.

Opportunities in the call-2024 Cluster 3 - Civil Security Horizon Europe: General Information and call details


**HORIZONTE
EUROPA**
@HorizonteEuropa

PhD Marina Martínez García
NCP and expert in Cluster-3 Horizon Europe
marina.cdti@sost.be

Centro para el Desarrollo Tecnológico y la Innovación



EUROPEAN UNION

© European Union, 2020

HORIZON EUROPE

#HorizonEU

THE EU RESEARCH &
INNOVATION PROGRAMME
2021 - 2027



First-ever revision of the EU's long-term budget Agreement between Parliament and Council

SUMMARY

For the first time ever, the European Parliament and the Council have agreed to revise the ceilings of the EU's multiannual financial framework. The agreement affects the remaining years of the current financial period: 2024 to 2027. The European Parliament had demanded a revision to enable the EU to rise to its challenges effectively. At the special European Council meeting on 1 February 2024, the EU Heads of State or Government reached a highly anticipated decision on the revision following the deadlock of their December meeting. This opened the way for the final negotiations with Parliament and, on 6 February, the negotiators reached a political agreement. Parliament is expected to vote on giving its consent during its 26-29 February plenary session.

The core element of the political agreement is the decision to establish predictable and stable financial support for Ukraine, totalling €50 billion from 2024 to 2027. The funds will be provided through a new framework, the Ukraine Facility, endowed with €33 billion in loans, guaranteed by the EU budget, and €17 billion in grants, financed by the EU budget through a special instrument.

In addition to the financial support for Ukraine, the EU budget will provide €14.6 billion to cope with migration needs, support key technologies and enhance the EU budget's flexibility, of which €10.6 billion originates from a redeployment of funds. The overall reinforcement of the EU budget amounts to €31.6 billion in grants for current priorities, with €21 billion in 'fresh money' from the Member States. This includes the €17 billion that will go to the Ukraine Facility.

As requested by the European Parliament, a mechanism will be introduced over and above the budget's ceilings to cover over-runs in the borrowing costs of the EU's recovery fund, Next Generation EU. In negotiations with the Council, Parliament also secured the smooth implementation of the EU4Health programme.



SCIENCE & BUSINESS[®]

Bringing together industry, research and policy

News Reports Events The Network Communications Services About Us

Horizon Europe budget to be cut by €2.1B, as defence research gets a €1.5B boost

01 Feb 2024 | News

Horizon Europe

R&D Policy

European Defence Fund

Heads of state approved the changes in Brussels today, after Germany rejected a Commission proposal to put an additional €100B into the EU's multiannual budget. The deal frees up a €50B aid package for Ukraine

By Florin Zubaşcu



EU leaders meet with Hungarian Prime Minister Viktor Orbán to discuss an aid package for Ukraine, which Orbán had vetoed in December. Photo: European Union

Horizon Europe will have its €95.5 billion budget cut by €2.1 billion, with €1.5 billion diverted to defence research, following an agreement by EU heads of state at a meeting in Brussels today.

Commission adds extra €1.4B to EU research spending this year

18 Apr 2024 | News

Horizon Europe

R&D Policy

Missions

Changes to Horizon Europe's 2023/24 work programme will see new calls to Pillar 2 and a top-up for Missions, while fresh life is breathed into the New European Bauhaus

By Goda Naujokaityte



Berlaymont building, headquarter of the European Commission, Brussels, Belgium. Photo credits: Bogdan Hoyaux / European Union

The European Commission is adding €1.4 billion to the Horizon Europe research programme this year, in latest amendment to 2023 and 2024 spending plans.

The money will be handed out to researchers through the controversial Horizon Europe Missions, and in four new bottom-up calls in Pillar 2 and a new partnership for pandemic preparedness, among others.

This amendment brings the EU's total Horizon Europe spending in 2024 to €7.3 billion.

But this isn't more money for Horizon Europe as a whole. The amended work programmes mainly roll out the previously planned investment in EU Missions, which was held back because of negotiations between the Commission and member states on their implementation, following an initial assessment in July 2023 of how the Missions were progressing.

As part of the negotiations, EU member states also secured a separate funding mechanism within Horizon Europe for the New European Bauhaus. [Here's](#) how that transpired in November.

The original 2023/24 work programmes were adopted on 3 December 2022 and first amended in March 2023. They outline Horizon Europe's calls for proposals, their budget and scope.

Horizon Europe's total budget for seven years currently amounts to €93.5 billion. It was originally €95.5 billion, but back in January EU member states [diverted](#) €2.1 billion to more pressing issues, such as aid to Ukraine. Since then, €100 million has been clawed back from unspent Horizon Europe funds, the so-called [decommitments](#).

This latest amendment is, most likely, the last one to the current set of work programmes before a new set of documents that cover spending from next year is adopted by the new European Commission in early 2025.

What's new?

EU Missions. A €648 million top-up for the five research Missions in 2024. The Missions funnel research funding into demonstrator projects and actions enhancing dialogue, which in turn are intended to promote innovation and leverage external funding in the five areas of cancer, climate adaptation, oceans and rivers, soil and climate-neutral cities.

The first 2024 calls will open between 18 and 24 April. The deadlines for most calls are in September. The exceptions are the Cities Mission, with some of the calls open from 17 September 2024 to 16 January 2025, and the Soils Mission with calls open from 8 May to 8 October. [Here's](#) the work programme.

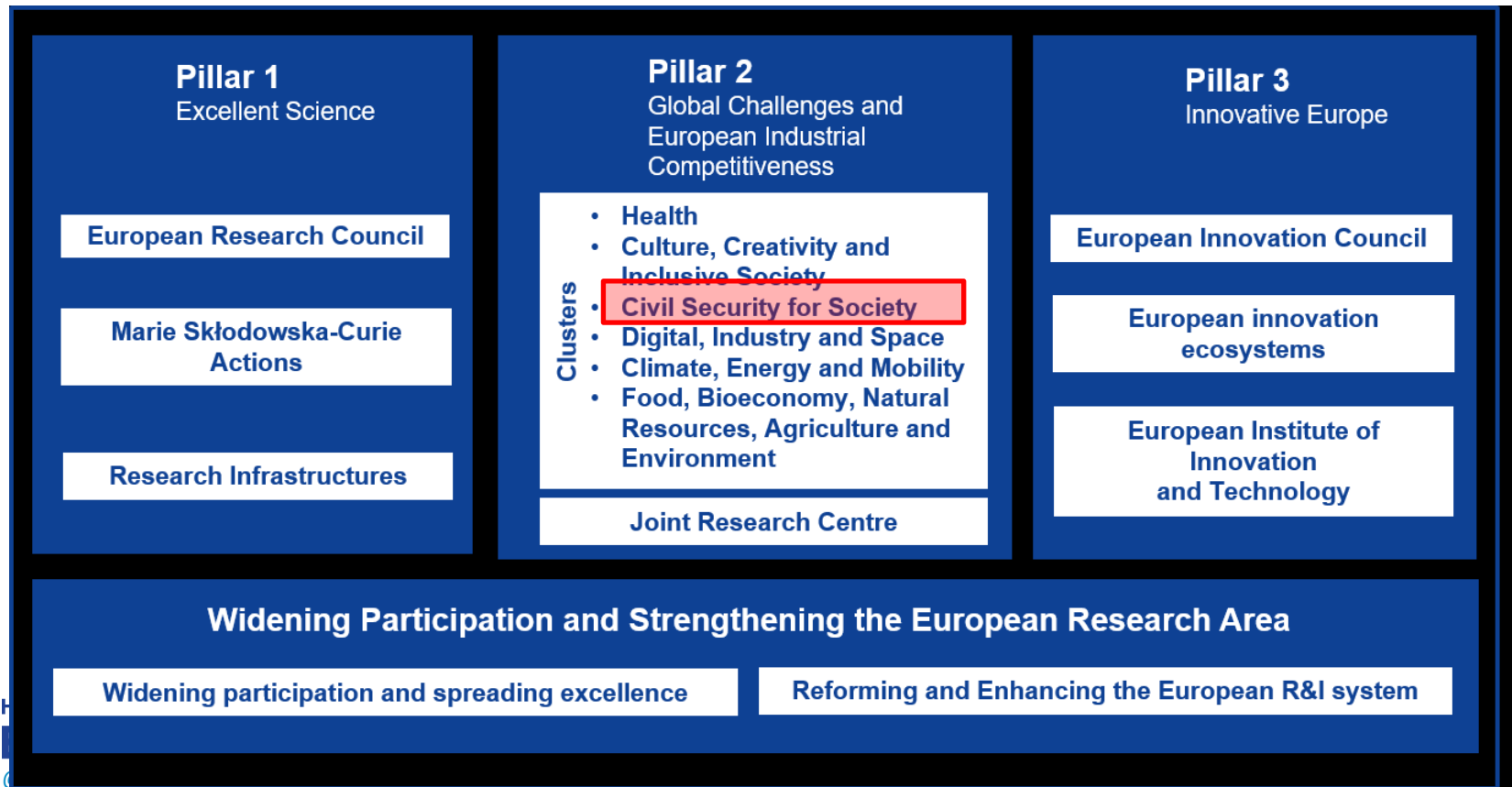
New European Bauhaus. The new work programme sets aside €20 million to lay the groundwork for the New European Bauhaus (NEB) facility, a dedicated funding mechanism under Horizon Europe that the Commission hopes to formally launch next year. The NEB facility will have a separate work programme from 2025 to fund the green culture initiative.

The €20 million will be spent on transforming neighbourhoods, regeneration, leveraging new bio-based materials, assessing the impact of the built environment of social relations, and governance models for the co-design of neighbourhoods.

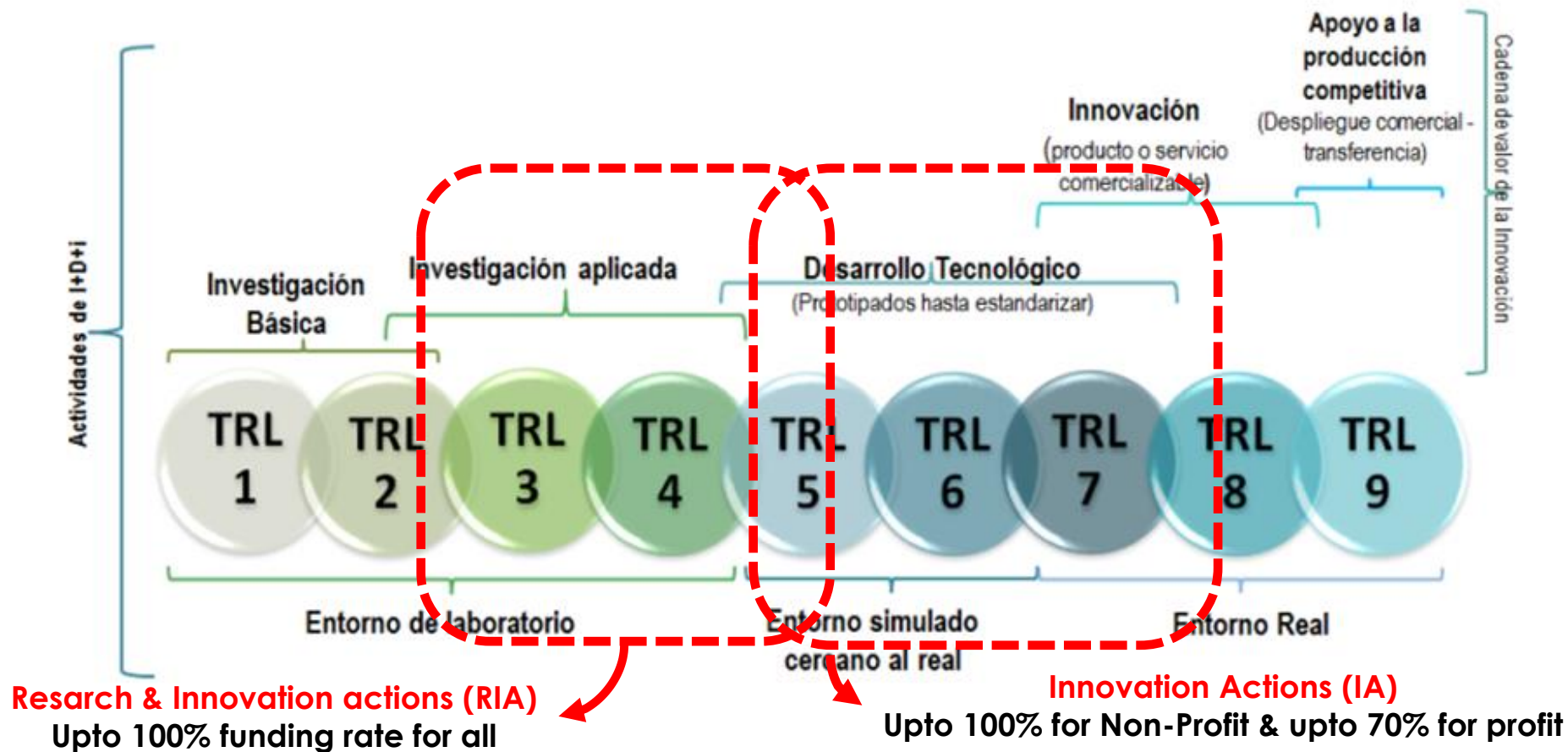
Open calls in Pillar 2. The Commission has set aside money for four bottom-up, open call topics that allow researchers to choose what they investigate. The total budget is €76 million in three Horizon Europe clusters: health; climate, energy and mobility; and food, bioeconomy, natural resources, agriculture and environment.

New partnership for pandemic preparedness. There's €50 million to set up a European partnership for pandemic preparedness. The call will open on 25 April and close on 26 November. The details are on pages 118-126 of the [updated health work programme](#).

**Cluster-3 of Horizon Europe → 1.600 M€, out of 95.500 M€ total
(final budget for the period 2025-2027 TBC in the coming weeks)**



Opportunities in the call-2024



Main features of the programme...

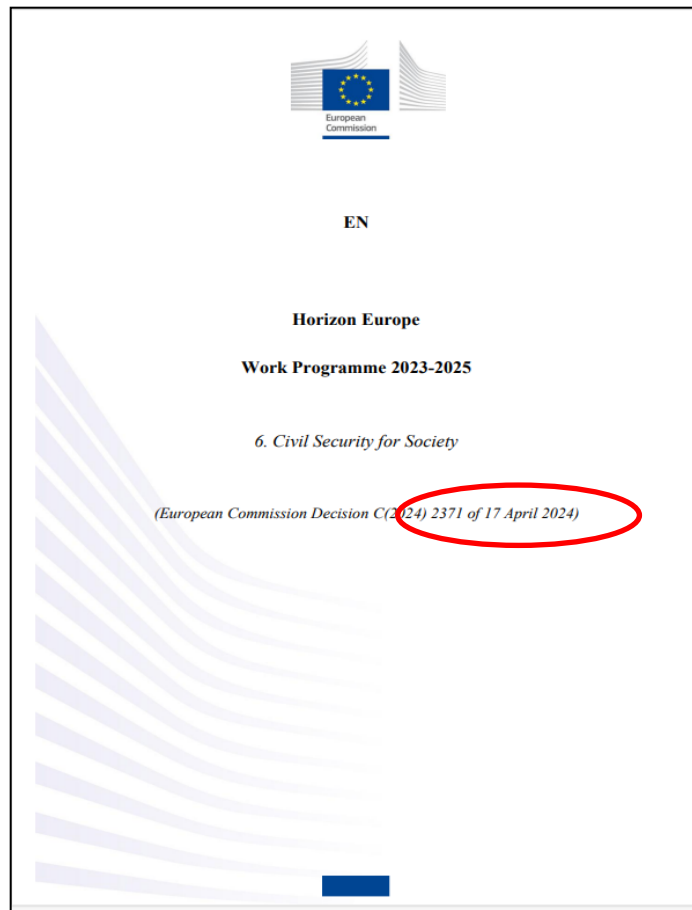


- ✓ **“Challenge-driven”** → Focus on testing, validating and developing capacities based on R&I of technologies, new methodologies and services for identified end-users & practitioners. → **Most of the topics in this call are “top-down”** focussed on **disaster risk management, pandemic preparedness, protection of critical infrastructures, maritime security, customs, civil protection,...**
- ✓ The **end-users in security** are **COMPULSORY PARTNERS in the consortia of your proposals** (check eligibility, which are reason for exclusion if they are not reached). → Police forces, forensic institutes, border and coast guards, customs authorities, **civil protection, firefighters, emergency units...**
- ✓ Stronger involvement of **Civil Society Entities** → **Associations, NGOs, Volunteers,...**
- ✓ **Some projects may be Security Classified** as they may contain, generate or use (background/foreground) secure sensitive Information.
- ✓ Those projects proposed for funding should pass the **ETHICAL SCRUTINY** in order to sign the GA and to start... → Thus, ethical aspects matter!

Other interesting features of the programme ...

- ✓ **close-to-market projects / almost operational** (TRL 5 → 8)
- ✓ **Exclusive civil application**, even that some technologies could be further developed for dual use... outside of Horizon Europe!
- ✓ International collaboration, specially in **DRS topics, is welcome/encouraged!**
- ✓ **Pilots, demos, “test-beds”** in real or semi-real environment → Strong **collaboration among “end-users”** and industry (including **SMEs**), **academia & civil society**.





- **Call 2024 logistics:**

- Opening: 27-June-2024
- **Deadline: 20-November-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

MODIFIED VERSION ONWARDS 17/04/2024

View available work programmes

2023 - 24

9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - General introduction English (1.48 MB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - EU Missions English (1.59 MB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - Cluster 1 English (1.97 MB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - Cluster 2 English (1.53 MB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - Cluster 3 English (1.53 MB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - Cluster 4 English (3.73 MB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - Cluster 5 English (4.14 MB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - Cluster 6 English (4.03 MB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - European Innovation Ecosystems English (801.58 KB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - MSCA English (1.79 MB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - Infrastructures English (1.38 MB - PDF)	Download ↓
9 DECEMBER 2022 Horizon Europe Work programme (2023-24) - WIDERA English (1.51 MB - PDF)	Download ↓
9 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



Main modificacions in the WP-2024: No participation of the so called “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 in the call-2024 excluding the participation of « high-risk supplier entities » within 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



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

Where to find info about the “high risk suppliers”? See the General Annexes ...

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 2019¹¹ 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 2023¹⁷ and the related Communication on the implementation of the 5G cybersecurity toolbox of 2023¹⁸.

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 part¹⁹ 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



... And who are those “high risk suppliers”?

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

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

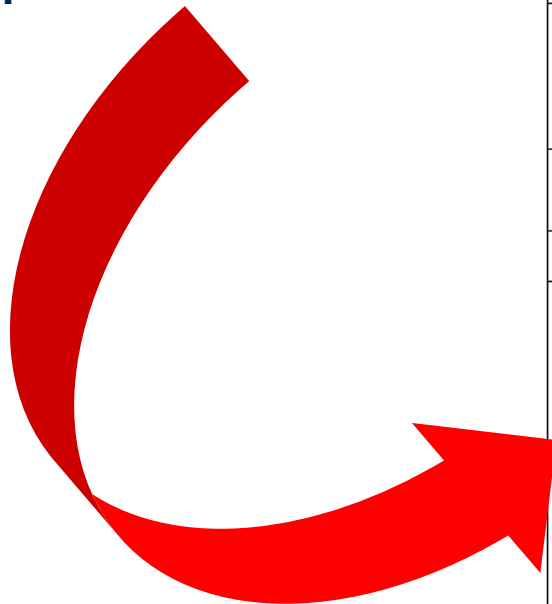
Cybersecurity



Topics in **CLUSTER-4 call-2024** excluding the participation of « high-risk supplier entities »

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

Where are those modifications within the topics concerned?



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

Specific conditions	
<i>Expected EU contribution per project</i>	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.
<i>Indicative budget</i>	The total indicative budget for the topic is EUR 3.70 million.
<i>Type of Action</i>	Research and Innovation Actions
<i>Eligibility conditions</i>	<p>The conditions are described in General Annex B. The following exceptions apply:</p> <p>The following additional eligibility conditions apply:</p> <p>This topic requires the active involvement, as beneficiaries, of at least 2 Police Authorities²² 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.</p> <p>The following exceptions apply: subject to restrictions for the protection of European communication networks.</p>
<i>Technology Readiness Level</i>	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.
<i>Security Sensitive Topics</i>	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.

6“Destinations” / All calls running in parallel, with the same opening and deadline!



- **Destination 1** – Better protect the EU and its citizens against Crime and Terrorism (FCT)
- **Destination 2** – Effective Management of EU external Borders (BM)
- **Destination 3** – Resilient INFRAstructure (INFRA)
- **Destination 4** – Increased CYBersecurity (CS)
- **Destination 5** – A Disaster-Resilient Society for Europe (DRS)
- **Destination 6** – Strengthened security research and innovation (SSRI)



- ✓ All topics are **1-stage evaluation**
- ✓ **FOR ALL TOPICS**, *“beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).”*

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

Destination Fighting Crime and Terrorism (FCT)

- ✓ **Prevention, investigation and mitigation** of the impact of criminal acts (including cyber) and terrorism
- ✓ Security in **urban public spaces**
- ✓ End-users: **Mainly LEAs...**



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.



**Destination BM:
Effective management of EU
external borders**

Destination BM/BS

- ✓ **Traffic of passengers** (*flow of people*) **and traffic of goods** (*flow of goods*) in the EU
- ✓ Prevention and counter-measures against illegal traffic, piracy and other criminality (including terrorism)
- ✓ **Aerial borders, maritime and terrestrial** → End-users: **Mainly coast guards and customs,...**



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.**



Destination INFRA: Protected infrastructure

Destination Infrastructures

- ✓ **Resilience and autonomy** → Both physical and cyber as well interconnected systems!
- ✓ Security in **big events, smart cities and urban infrastructures**
- ✓ End-users: **Mainly CIOs, municipalities,...**

**INFRASTR.
PROTECTION**



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 <u>at national level</u>

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



Destination DRS: A Disaster-resilient society for Europe

Destination DRS

- ✓ Prevention, mitigation, response and recovering from **crisis & disasters (natural, CBRN-E, pandemics, climate change,...)**
- ✓ **Trans-border coordination** (including neighbouring countries of the EU)
- ✓ End-users: **Mainly emergency services & civil protection** (CBRN-E, extrem events, pandemics, etc...), **municipalities, volunteers and NGOs,...**

**DISASTER
RISK
REDUCTION**



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACIÓN
Y UNIVERSIDADES



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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.**




Destination SSRI: Strengthened Security Research and Innovation

Destination Strengthening Security R&I

- ✓ Improving **market uptake** of the R&I results
- ✓ Improving the **impact of projects**
- ✓ **Planning and medium-long term vision** of research needs



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: <ul style="list-style-type: none"> • From 3 to 7 partners 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 budget 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

- Capacities for **Europe's strategic autonomy**
- Strengthening **digital infrastructures** from cyber and hybrid attacks
- **data protection, privacy & ethics**

CYBERSECURITY



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...

Calendar of next events / infodays

- ✓ **Spanish national infoday** →
Madrid, **30-May 2024**
- ✓ **Regional Spanish infodays** →
Galicia, Catalonia, Basque
Country, Valencia, Andalucía and
Murcia!
- ✓ **European Infoday + brokerage
event** → Brussels, **12-13 June 2024**



SMI2G

Security Mission Information & Innovation Group

2024 Brokerage Event

22 & 23 May

Campus Cyber,
La Défense, Paris

SMI2G Brokerage 2024 Event - Please register!

Following the success of past years...

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 [Horizon Europe's Civil Security for Society 2023-2024 Work Programme](#)

The SMI2G brokerage event is organised 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 Cyber and ENLETS



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

REGISTRATION CLOSED

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 destination, 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.

Community for Research and Innovation for Security (CERIS)



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

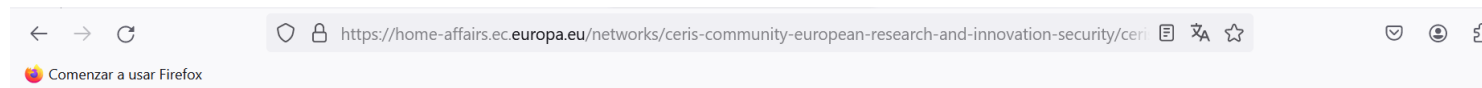


GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACIÓN
Y UNIVERSIDADES



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



Filter by

Status

Event date

Subject

Search

Clear filters

CERIS events (50)




Showing results 1 to 10

11
APR
2024

Training and workshops
CERIS workshop on 'Innovating Smart Cities Resilience through Research and Best Practices'

21
MAR
2024

Training and workshops
Chemical, biological, radiological, nuclear, explosive (CBRNE) Research & Innovation Day
 France

05
MAR
2024

Training and workshops
Community for European Research and Innovation for Security (CERIS) workshop on Foresight and Key Enabling Technologies
 Brussels, Belgium

SEREMAP tool for partner search...

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

Security Research Map

Home Participants Marketplace Login Register

SeReMa Security Research Map

Info First steps! How it works FAQ Contact

NEW Security Research Database

The purpose of the Security Research Map (SeReMa) is to increase the visibility of civil security related research in Europe and to optimize the networking between various actors in that field: research facilities, universities, public authorities, end-users/practitioners users, suppliers of security solutions and operators of critical infrastructures. SeReMa aims to be a focal point for all stakeholders who aim to be involved in projects submitted for calls of Horizon Europe's Cluster 3.

Register now
Open until 30 June 2024

ORGANISED BY

SeReMa

Interesting links!

- [Innovation and Security](#)
- [EU Security Market Study](#)
- [Study on the Factors Influencing the Uptake of EU-Funded Security Research Outcomes](#)
- [SEREN5 PROJECT \(Cluster-3 NCPs\)](#)
- [Already funded projects and additional info from REA](#)



Many thanks... see you in Brussels!

