



MINISTÈRE
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE

*Liberté
Égalité
Fraternité*



Le programme européen pour la recherche et l'innovation





Appels 2025

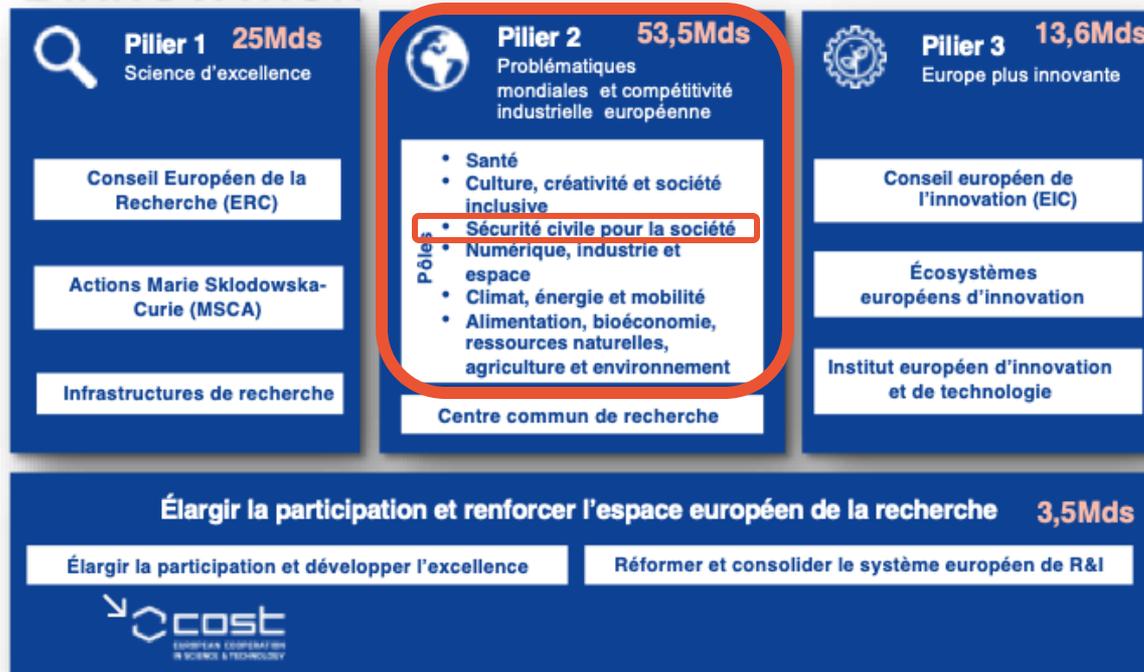
Cluster 3 Sécurité civile pour la société

LE PROGRAMME-CADRE DE L'UNION EUROPÉENNE POUR LA RECHERCHE ET L'INNOVATION

2021 – 2027

95,5 G€

- Renforcer les **bases scientifiques et technologiques** de l'Union ;
- Stimuler sa **capacité d'innovation**, sa **compétitivité** et la création **d'emplois** ;
- Concrétiser les **priorités politiques** stratégiques de l'Union ;
- Contribuer à répondre aux **problématiques mondiales**, dont les objectifs de **développement durable** des Nations Unies.



Critères d'éligibilité – projets collaboratifs

**Au minimum 3 entités légales
Indépendantes, dans 3 Etats membres
ou associés à Horizon Europe*
et -nouveau- dont au moins une établie
dans un des 27 Etats membres.**

**A savoir: dans chaque appel à projets, des
conditions spécifiques peuvent apparaître
(plus de partenaires, autre pays obligatoire et
financé...).**

**La liste des Etats associés sera disponible à l'issue des
négociations sur l'article 16.*

Etats membres de l'UE

Etats associés ou en cours d'association :

Etats tiers :

- à **revenus faibles ou moyens** (consulter la liste) :
automatiquement éligibles au financement
- **autres** : financement à titre très exceptionnel

➤ *Liste complète et actualisation des Etats associés
: [Lien](#)*

27 Etats Membres de l'Union Européenne

- Allemagne
- Autriche
- Belgique
- Bulgarie
- Chypre
- Croatie
- Danemark
- Espagne
- Estonie
- Finlande
- France
- Grèce
- Hongrie
- Irlande
- Italie
- Lettonie
- Lituanie
- Luxembourg
- Malte
- Pays-Bas
- Pologne
- Portugal
- République tchèque
- Roumanie
- Slovaquie
- Slovénie
- Suède

Les états associés au programme Horizon Europe (17.04.2024)

- Albanie
- Arménie
- Bosnie Herzégovine
- Canada
- Egypte
- Iles Féroé
- Géorgie
- Islande
- Israël
- Kosovo
- Moldavie
- Monténégro
- Nouvelle-Zélande
- Macédoine du Nord
- Norvège
- Serbie
- Tunisie
- Turquie
- Ukraine
- UK
- **Maroc**
- **Corée du Sud**
- **Suisse**

Pays tiers (à revenus faibles ou moyens)

- Afghanistan, Algeria, Angola, Argentina, Azerbaijan
- Bangladesh, Belarus, Belize, Benin, Bhutan, Bolivia, Botswana, Burkina Faso, Burundi
- Cabo Verde, Cambodia, Cameroon, Central African Republic, Chad, Colombia, Comoros, Congo (Democratic Republic), Congo (Republic), Costa Rica, Côte d'Ivoire, Cuba
- Djibouti, Dominica, Dominican Republic
- Ecuador, El Salvador, Equatorial Guinea, Eritrea, Eswatini, Ethiopia
- Fiji
- Gabon, Gambia, Ghana, Grenada, Guatemala, Guinea, Guinea-Bissau, Guyana
- Haiti, Honduras
- Indonesia, Iran (Islamic Republic), Iraq
- Jamaica, Jordan
- Kazakhstan, Kenya, Kiribati, Korea (Democratic People's Republic), Kyrgyz Republic

- Lao (People's Democratic Republic), Lebanon, Lesotho, Liberia, Libya
- Madagascar, Malawi, Malaysia, Maldives, Mali, Marshall Islands, Mauritania, Mauritius, Micronesia (Federated States), Mongolia, Morocco, Mozambique, Myanmar
- Namibia, Nepal, Nicaragua, Niger, Nigeria
- Pakistan, Palestine, Papua New Guinea, Paraguay, Peru, Philippines
- Rwanda
- Samoa, São Tomé and Príncipe, Senegal, Sierra Leone, Solomon Islands, Somalia, South Africa, South Sudan, Sri Lanka, St. Lucia, St. Vincent and the Grenadines, Sudan, Suriname, Syrian Arab Republic
- Tajikistan, Tanzania, Thailand, Timor-Leste, Togo, Tonga, Turkmenistan, Tuvalu
- Uganda, Uzbekistan
- Vanuatu, Venezuela (Bolivarian Republic), Vietnam
- Yemen Republic
- Zambia, Zimbabwe



Les pays membres de l'OCDE

- Australie
- Autriche
- Belgique
- Canada
- Chili
- Colombie
- Corée du Sud
- Costa Rica
- Danemark
- Espagne
- Estonie
- États-Unis
- Finlande
- France
- Grèce
- Hongrie
- Irlande
- Islande
- Israël
- Italie
- Japon
- Lettonie
- Lituanie
- Luxembourg
- Mexique
- Norvège
- Nouvelle-Zélande
- Pays-Bas
- Pologne
- Portugal
- Slovaquie
- Royaume-Uni
- Slovénie
- Suède
- Suisse
- République Tchèque
- Turquie



Approche "*top-down*" pour soutenir les **priorités politiques stratégiques** de l'Union Européenne et les **objectifs de développement durable** des Nations Unies.

- Appels à projets **centrés sur des problématiques sociétales**, des **défis globaux** :
 - Répondre aux **impacts attendus**
 - Fournir des **options politiques**, des **solutions (non) technologiques**, des **recommandations...**
- Projets **collaboratifs** **transdisciplinaires**, **transectoriels** et **transnationaux (10-15 partenaires)**
- **3-4 ans** en moyenne
- Minimum **2-3 Millions** d'euros, **4-5 Millions** en moyenne
- 4types de projets : **RIA, IA, CSA, PCP**

Pilier 2
Problématiques mondiales et compétitivité industrielle européenne

Pôles

- Santé
- Culture, créativité et société inclusive
- Sécurité civile pour la société
- Numérique, industrie et espace
- Climat, énergie et mobilité
- Alimentation, bioéconomie, ressources naturelles, agriculture et environnement

Centre commun de recherche

Conseils

- Toujours prendre en compte les facteurs humains, le contexte social (**SSH**)
 - Garantir le respect des droits fondamentaux
 - Lire le **plan stratégique**
 - Lire le **work programme / les appels**
 - Pas d'entités chinoises dans les IA !
 - **Vérifier les accords d'association pour éligibilité des pays (UK, Maroc, etc.)**
 - **Application civile, non militaire**
 - Toujours regarder les appels financés précédemment et démontrer comment votre proposition les prend en compte, notamment dans les "**Open Topics**".
 - Utilisez **Copernicus & Galileo/EGNOS**
 - Soyez en lien avec le **CERIS**
-

Les références

- [Promoting the European way of life](#)
- [European Green Deal](#)
- [Europe fit for the digital age](#)
- [Security Union Strategy](#)
- [Counter-Terrorism Agenda](#)
- [EU Strategy to tackle Organised Crime](#)
- [EU Strategy on Combatting Trafficking in Human Beings](#)
- [EU strategy for a more effective fight against child sexual abuse](#)
- [EU Action Plan on firearms trafficking](#)
- [Pact on Migration and Asylum, EU Disaster Risk Reduction policies](#)
- [EU Climate Adaptation Strategy](#)
- [EU Maritime Security Strategy](#)
- [EU Cybersecurity Strategy](#)

Permettre à la Commission d'évaluer la valeur ajoutée pendant et après le programme sur 9 enjeux :

<ul style="list-style-type: none">• Créer de nouvelles connaissances de haute qualité• Renforcer le capital humain dans la recherche et l'innovation• Favoriser la diffusion des connaissances et l'open source	Impacts Scientifiques
<ul style="list-style-type: none">• Répondre aux priorités politiques de l'UE et aux défis mondiaux grâce à la recherche et à l'innovation• Produire des bénéfices et des impacts grâce à des missions de recherche et d'innovation• Renforcer l'adoption de la recherche et de l'innovation dans la société	Impacts Sociétaux
<ul style="list-style-type: none">• Générer une croissance basée sur l'innovation• Créer des emplois plus nombreux et de meilleure qualité• Tirer parti des investissements dans la recherche et l'innovation	Impacts Économiques

Objectifs du Cluster 3 Sécurité Civile pour la Société

Priorités

- Soutenir les **priorités politiques de l'UE** en matière de **sécurité civile** et de **cyber sécurité**
- Répondre aux exigences en matière de **capacités**
- Garantir des résultats **éthiques soutenus par la société**
- Créer un marché pour une **industrie de sécurité Européenne compétitive**

Orientations Stratégiques et Impacts attendus

KSO D « Créer une société européenne plus résiliente, inclusive et démocratique » :

- Une UE résiliente préparée aux menaces émergentes
- Une société européenne sûre, ouverte et démocratique
- Améliorer la sécurité aux frontières et maritime

KSO A « Promouvoir une autonomie stratégique ouverte par le dév. de technos numériques »

- Technologies numériques sécurisées et cybersécurisées
-

Introduction – Cross-cutting themes (SHS)

1. Renforcer la résilience des sociétés et la démocratie

- Confiance dans la probité et la compétence de nos représentants
- Confiance dans nos médias
- FIMI: Foreign intervention and manipulation of information

2. La transition digitale

- Vulnérabilités dites imprévues
- OSA : Open Strategic Autonomy

3. Soutenir la transition verte

4. S'assurer que les mesures proposées sont légales, éthiques et acceptées par les citoyens

- 4.1. **Respect des normes** éthiques et légales
- 4.2. **Acceptabilité sociale** : On analyse la « conformité » d'un changement - d'une innovation technologique, de la politique mise en place, d'une façon de faire (gestion de espaces publiques, impôts) ... aux attentes de la population ou aux craintes, appréhension de la population – et de la population dans sa diversité. On analyse des potentiels réactions voire conflits que pourraient susciter cette innovation, cette décision.
- 4.3. Innovation sociale, cocréation (**communities should be engaged**)
= une méthode

5. Vulnérabilité et inclusion

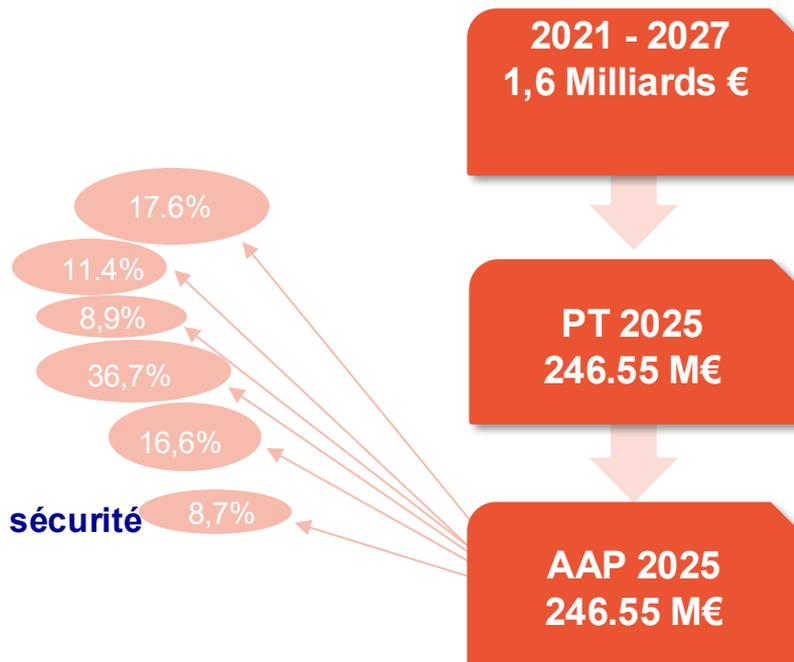
Les destinations du Cluster 3

Six domaines d'intervention « Destinations »

- 1) FCT : la lutte contre le crime et le terrorisme
- 2) BM : la protection des frontières
- 3) RI : la sécurité et la résilience des infrastructures
- 4) IC : la Cybersécurité
- 5) DRS : la résilience de la société face aux catastrophes
- 6) SSRI : le renforcement de la recherche et innovation en sécurité

Calendrier

Appels 2025 : deadline **12 novembre 2025**



Fighting Crime and Terrorism





FCT 2025

- 4 appels / 13 lauréats, 43.5 M€
- 1 IA, 3 RIA
- 2 AAP SHS

HORIZON-CL3-2025-01-FCT-01 : Open topic L'analyse moderne des informations, des preuves et la police de première ligne

HORIZON-CL3-2025-01-FCT-02 : Open topic La prévention, la détection et la dissuasion de diverses formes de criminalité et de terrorisme grâce à une meilleure compréhension des questions sociétales qui y sont liées

HORIZON-CL3-2025-01-FCT-03 : Open topic L'amélioration de l'image du renseignement et le renforcement de la prévention, de la détection et de la dissuasion des différentes formes de criminalité organisée

HORIZON-CL3-2025-01-FCT-04 : Déminage humanitaire / élimination des munitions non explosées (UXO) dans les zones civiles et sensibilisation aux risques liés aux munitions non explosées

HORIZON-CL3-2025-01-FCT-01 : Open topic on modern information and forensic evidence analysis and on frontline policing

L'analyse moderne des informations, des preuves et la police de première ligne

RÉSULTATS ATTENDUS / certain ou tous parmi

- Des outils, des compétences et des méthodologies modernes, uniformes et validés, ainsi que des programmes de formation novateurs pour les praticiens de la sécurité (autorités policières européennes, instituts de police scientifique) afin de prévenir et de détecter les infractions pénales et terroristes et d'enquêter à leur sujet, y compris la collecte légale de preuves judiciaires ;
- Amélioration des mécanismes d'échange transfrontalier d'informations dans le cadre de la lutte contre la criminalité et le terrorisme, en tenant compte de l'ensemble de la législation applicable et des droits fondamentaux ;
- Soutien aux décideurs politiques, sur la base d'éléments concrets, pour l'élaboration et l'adaptation de la réglementation relative à l'analyse moderne de l'information, à l'analyse des preuves ou aux services de police de première ligne.

3 options

- Option a : relever les défis posés par les technologies de pointe ;
- Option b : analyse médico-légale moderne à l'aide de technologies nouvelles et émergentes ;
- Option c : modernisation des services de police de première ligne.

CONSORTIUM

**Au moins 2 autorités de police
d'au moins 2 États membres de
l'UE ou pays associés
différents.**



HORIZON-CL3-2025-01-FCT-02: Open topic on prevention, detection and deterrence of various forms of crime and terrorism through an enhanced understanding of the related societal issues

La prévention, la détection et la dissuasion de diverses formes de criminalité et de terrorisme grâce à une meilleure compréhension des questions sociétales qui y sont liées.

RÉSULTATS ATTENDUS / tous ou certain parmi

- Des outils, compétences ou méthodologies améliorés, modernes, uniformes et validés, ainsi que des programmes de formation innovants pour les praticiens de la sécurité (autorités policières européennes, organisations non gouvernementales, organisations de la société civile) afin de prévenir, détecter et décourager les infractions criminelles ou terroristes, en tenant compte de l'ensemble de la législation applicable et des droits fondamentaux
- Une meilleure compréhension des aspects culturels et sociétaux de la criminalité ou du terrorisme/de la radicalisation, ainsi que des principaux défis liés à la lutte contre ces phénomènes
- Soutien aux décideurs politiques, sur la base d'éléments concrets, pour l'élaboration et l'adaptation de la réglementation relative à la criminalité, au terrorisme et à la radicalisation
- Amélioration de la perception par les citoyens que l'Europe est un espace de liberté, de justice, de sécurité et de respect de la vie privée et des droits de l'homme, grâce, par exemple, à des campagnes de sensibilisation innovantes expliquant aux citoyens les mécanismes clés et évolutifs de la criminalité ou du terrorisme/de la radicalisation, et la manière de s'en prémunir.

2 options

- Option a : questions sociétales liées à la criminalité ;
- Option b : questions sociétales liées au terrorisme et à la radicalisation.

CONSORTIUM

Au moins 1 autorité de police et 1 organisation civile d'au moins 2 États membres de l'UE ou pays associés différents.

Lien avec les appels Cluster 2 :

HORIZON-CL2-2022-
DEMOCRACY-01-05
HORIZON-CL2-2024-
DEMOCRACY-01-05



HORIZON-CL3-2025-01-FCT-03: Open topic on improved intelligence picture and enhanced prevention, detection and deterrence of various forms of organised crime

L'amélioration de l'image du renseignement et le renforcement de la prévention, de la détection et de la dissuasion des différentes formes de criminalité organisée

RÉSULTATS ATTENDUS / tous parmi

- Des **outils, des compétences et des méthodologies améliorés**, modernes, uniformes et validés, ainsi que des programmes de formation innovants pour les autorités policières européennes afin de prévenir et de détecter les infractions liées à la criminalité organisée et d'enquêter à leur sujet, y compris la détection précoce des réseaux criminels et l'identification des nouvelles tendances et des nouveaux défis ;
- Des **mécanismes améliorés pour l'utilisation d'outils transfrontaliers** afin de faciliter l'échange sécurisé d'informations dans la lutte contre la criminalité organisée, y compris les réseaux criminels, en tenant compte de l'ensemble de la législation applicable et des droits fondamentaux ;
- Une meilleure **compréhension des principaux défis** et des meilleures pratiques en matière de lutte contre la criminalité organisée transfrontalière ;
- Un **soutien factuel aux décideurs politiques** pour l'élaboration et l'adaptation de la réglementation relative à la criminalité organisée transfrontalière, y compris les réseaux criminels.

CONSORTIUM

Au moins 3 autorités de police d'au moins 3 États membres de l'UE ou pays associés différents.

Collaboration avec Europol

HORIZON-CL3-2025-01-FCT-04: Humanitarian demining / Unexploded Ordnance Disposal (UXO) of civil areas and unexploded ordnance risk education

Démunage humanitaire / élimination des munitions non explosées (UXO) dans les zones civiles et sensibilisation aux risques liés aux munitions non explosées

RÉSULTATS ATTENDUS / tous parmi

- Des outils, des compétences et des méthodologies améliorés, modernes et validés, ainsi que des programmes de formation innovants pour les praticiens impliqués dans le déminage humanitaire et la neutralisation des munitions non explosées (UXO) dans les zones civiles, en tenant compte de l'ensemble de la législation applicable et des droits fondamentaux ;
- Amélioration des activités d'éducation visant à réduire les risques de blessures causées par les mines antipersonnel et autres munitions non explosées ;
- une meilleure compréhension des principaux défis et des meilleures pratiques liés au déminage humanitaire et à la sensibilisation aux risques liés aux munitions non explosées, en tenant compte de l'expérience des participants ukrainiens ;
- un soutien factuel aux décideurs politiques pour l'élaboration de l'action de l'UE en matière de lutte contre les mines.

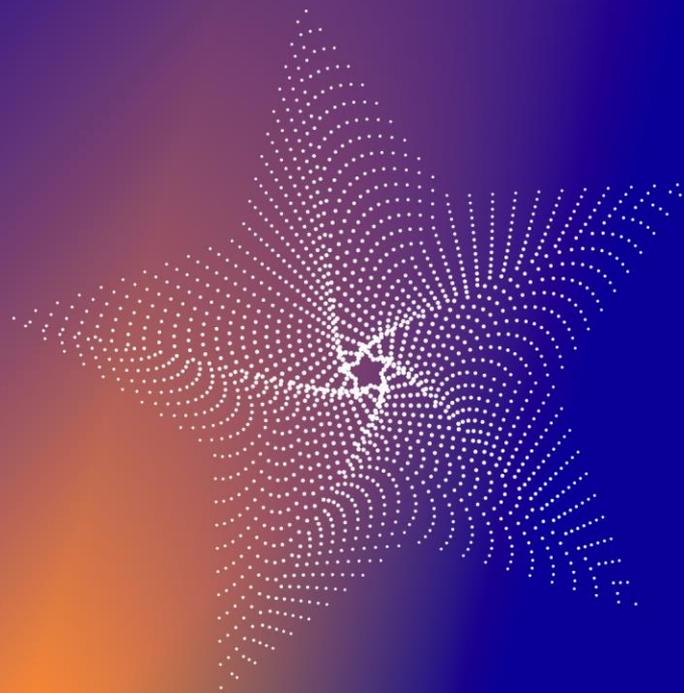
CONSORTIUM

Au moins 1 ONG humanitaire et 2 ONG local ou régional d'au moins 3 États membres de l'UE ou pays associés différents.

Au moins une entité ukrainienne doit obligatoirement faire partie du consortium et posséder des compétences en matière de déminage humanitaire et de neutralisation des munitions non explosées (UXO).



Border Management





BM 2025

- 3 appels / 9 lauréats, 28 M€
- 2 IA, 1 RIA

HORIZON-CL3-2025-01-BM-01 : Open topic Une surveillance efficace des frontières et de la sécurité maritime

HORIZON-CL3-2025-01-BM-02 : Open topic Sécuriser et faciliter le franchissement des frontières extérieures

HORIZON-CL3-2025-01-BM-03 : Open topic Une meilleure sécurité des douanes et de la chaîne d'approvisionnement

HORIZON-CL3-2025-01-BM-01: Open topic on efficient border surveillance and maritime security

une surveillance efficace des frontières et de la sécurité maritime

RÉSULTATS ATTENDUS / tous parmi

- Amélioration de la sécurité des frontières extérieures de l'UE ou de l'environnement, des infrastructures et des activités maritimes contre les catastrophes naturelles, accidentelles ou fortuites ; défis tels que les trafics illégaux (aériens, maritimes, sous-marins, terrestres et de surface), les migrations irrégulières ou les situations exceptionnelles d'arrivées massives aux frontières extérieures, l'exploitation illégale des ressources naturelles, la piraterie et les attaques terroristes potentielles, les cybermenaces et les menaces hybrides ;
- Surveillance soutenue et améliorée, connaissance de la situation en temps réel et capacités de réaction pour faire face à d'éventuelles situations critiques aux frontières extérieures de l'UE ;
- Amélioration des processus décisionnels et des capacités d'évaluation, de confirmation et de réaction aux situations de détresse en mer et sur terre, permettant une réponse meilleure et plus rapide.

CONSORTIUM

Au moins 2 garde-frontières ou garde-côtes d'au moins 2 États membres de l'UE ou pays associés différents.

HORIZON-CL3-2025-01-BM-02: Open topic on secured and facilitated crossing of external borders

Sécuriser et faciliter le franchissement des frontières extérieures

RÉSULTATS ATTENDUS :

- Amélioration de l'expérience de franchissement des frontières pour les voyageurs et le personnel des autorités frontalières (y compris les douanes, les gardes-côtes et les gardes-frontières), tout en maintenant la sécurité et la surveillance des mouvements aux frontières extérieures de l'UE, en soutenant l'espace Schengen, en réduisant les mouvements illégaux de personnes et de marchandises à travers ces frontières et en protégeant les droits fondamentaux des voyageurs, qu'ils soient citoyens de l'UE ou ressortissants d'un pays tiers.

CONSORTIUM

Au moins 2 garde-frontières ou garde-côtes d'au moins 2 États membres de l'UE ou pays associés différents.

HORIZON-CL3-2025-01-BM-03: Open topic on better customs and supply chain security

Une meilleure sécurité des douanes et de la chaîne d'approvisionnement

RÉSULTATS ATTENDUS :

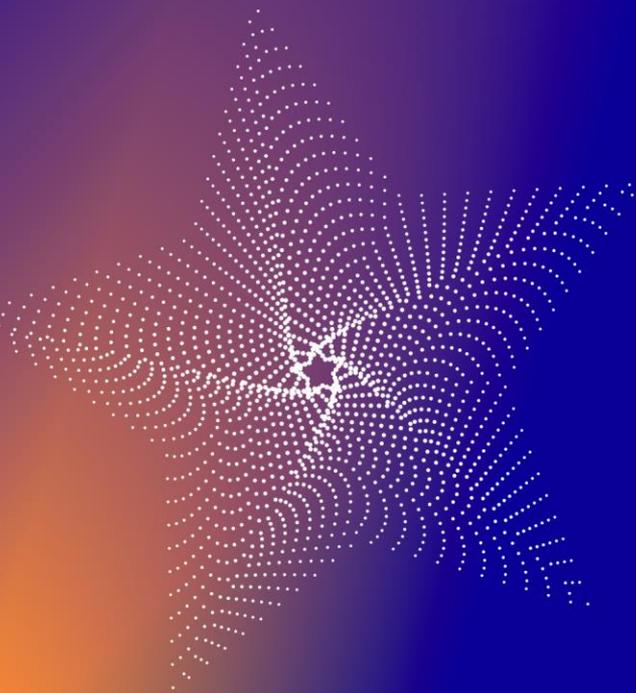
- Amélioration de la sécurité des douanes et de la chaîne d'approvisionnement grâce à une meilleure prévention, détection, dissuasion, lutte contre la falsification et/ou contre les activités illégales impliquant des flux de marchandises à travers les frontières extérieures de l'UE et la chaîne d'approvisionnement, et/ou grâce à une meilleure interopérabilité, minimisant ainsi les perturbations des flux commerciaux.

CONSORTIUM

Au moins 2 douanes d'au moins 2 États membres de l'UE ou pays associés différents.



Resilient Infrastructure





RI 2025

- **2 appels / 5 lauréats, 22 M€**
- **1 IA, 1 RIA**
- **1 AAP SHS**

HORIZON-CL3-2025-01-INFRA-01 : Open topic Améliorer la préparation, la réaction le rétablissement en cas de perturbations à grande échelle des infrastructures critiques

HORIZON-CL3-2025-01-INFRA-02 : Open topic Comprendre le rôle du facteur humain dans la résilience des infrastructures critiques



HORIZON-CL3-2025-01-INFRA-01: Open topic for improved preparedness for, response to and recovery from large-scale disruptions of critical infrastructures

Améliorer la préparation, la réaction le rétablissement en cas de perturbations à grande échelle des infrastructures critiques

RÉSULTATS ATTENDUS / certain ou tous parmi

- Les infrastructures critiques sont plus résistantes aux risques naturels, aux actions humaines dommageables **intentionnelles et accidentelles**, y compris les **cyberattaques** ;
- Les exploitants d'infrastructures critiques et les autorités disposent d'**une meilleure cartographie** des interdépendances pertinentes pour le(s) secteur(s) concerné(s), également en vue de mieux **gérer les crises potentielles multirisques, intersectorielles et transfrontalières** ;
- Les exploitants d'infrastructures critiques et les autorités ont accès à des **outils améliorés de surveillance, d'évaluation des risques et des menaces, de prévision** et, le cas échéant, de modélisation, ainsi qu'à des solutions en matière de sécurité physique et cybernétique ;
- Les exploitants et les autorités responsables des infrastructures critiques ont accès à des **capacités accrues d'enquête après incident**, ce qui contribue à améliorer la prévention, la préparation, la gestion et la réaction aux crises ;
- Des **outils numériques** efficaces permettant de réaliser des tests de résistance virtuels et physiques sont mis à la disposition des praticiens de la sécurité concernés ;
- Des programmes de **formation** sont élaborés à l'intention des exploitants et des autorités responsables des infrastructures critiques et/ou des intervenants de première ligne.

CONSORTIUM

Au moins 3 praticiens d'au moins 3 États membres de l'UE ou pays associés différents.

Le montant maximum à accorder à chaque tiers est de 200 000 euros.

HORIZON-CL3-2025-01-INFRA-02: Open topic for role of the human factor for the resilience of critical infrastructures

Comprendre le rôle du facteur humain dans la résilience des infrastructures critiques

RÉSULTATS ATTENDUS / certain ou tous parmi

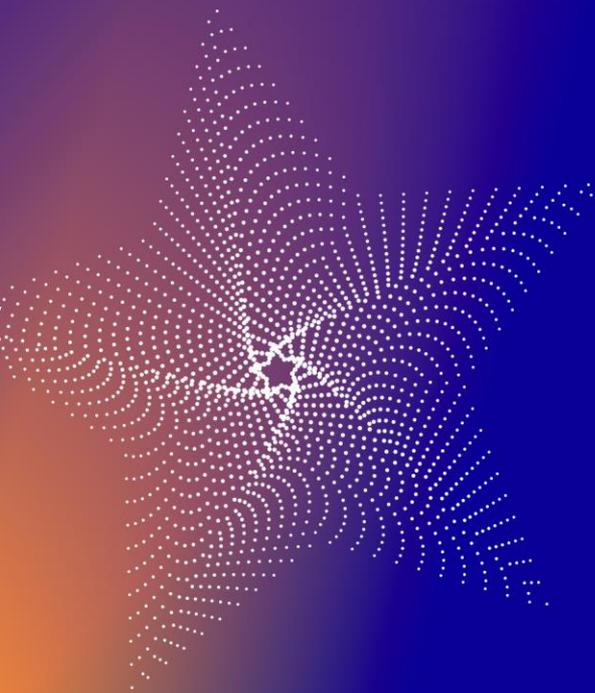
- Les infrastructures critiques sont plus résistantes aux risques naturels, aux actions humaines dommageables **intentionnelles et accidentelles**, y compris les **cyberattaques** ;
- Les exploitants d'infrastructures critiques et les autorités disposent d'**une meilleure cartographie** des interdépendances pertinentes pour le(s) secteur(s) concerné(s), également en vue de mieux **gérer les crises potentielles multirisques, intersectorielles et transfrontalières** ;
- Les exploitants d'infrastructures critiques et les autorités ont accès à des **outils améliorés de surveillance, d'évaluation des risques et des menaces, de prévision** et, le cas échéant, de modélisation, ainsi qu'à des solutions en matière de sécurité physique et cybernétique ;
- Les exploitants et les autorités responsables des infrastructures critiques ont accès à des **capacités accrues d'enquête après incident**, ce qui contribue à améliorer la prévention, la préparation, la gestion et la réaction aux crises ;
- Des **outils numériques** efficaces permettant de réaliser des tests de résistance virtuels et physiques sont mis à la disposition des praticiens de la sécurité concernés ;
- Des programmes de **formation** sont élaborés à l'intention des exploitants et des autorités responsables des infrastructures critiques et/ou des intervenants de première ligne.

CONSORTIUM

Au moins 3 praticiens d'au moins 3 États membres de l'UE ou pays associés différents.



Increased Cybersecurity





CS-ECCC 2025

6 appels / 16 lauréats 90,55 M€
1 IA, 5 RIA

HORIZON-CL3-2025-02-CS-ECCC-01 : IA générative pour des applications en cybersécurité

HORIZON-CL3-2025-02-CS-ECCC-02 : Nouveaux outils et processus avancés pour la cybersécurité opérationnelle

HORIZON-CL3-2025-02-CS-ECCC-03 : Technologies d'amélioration pour la protection de la vie privée

HORIZON-CL3-2025-02-CS-ECCC-04 : Évaluation de la sécurité des primitives de cryptographie post-quantique (PQC)

HORIZON-CL3-2025-02-CS-ECCC-05 : Sécurité des implémentations des algorithmes de cryptographie post-quantique

HORIZON-CL3-2025-02-CS-ECCC-06 : Intégration d'algorithmes de cryptographie post-quantique (PQC) dans des protocoles de haut niveau

HORIZON-CL3-2025-02-CS-ECCC-01: Generative AI for Cybersecurity applications

IA générative pour des applications en cybersécurité

RÉSULTATS ATTENDUS / certains ou tous parmi

Développer des technologies, outils et processus basés sur l'IA générative pour améliorer la cybersécurité, en conformité avec les politiques, lois et exigences éthiques de l'UE.

Les propositions doivent porter sur au moins l'un des résultats suivants :

1. Développement et test de modèles d'IA générative pour la surveillance, la détection, la réponse et l'auto-réparation face aux cyberattaques.
2. Création d'outils d'IA générative pour la conformité continue et la remédiation automatisée, en tenant compte des aspects juridiques et éthiques.

POINTS IMPORTANTS

- Limité aux états membres et états associés
- Interdits aux entités détenues par des pays ou des entités de pays non éligibles
- Restreint aux réseaux de communication européens.

HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for Operational Cybersecurity

Nouveaux outils et processus avancés pour la cybersécurité opérationnelle

RÉSULTATS ATTENDUS / minimum 2 parmi

- Amélioration de la connaissance de la situation grâce à des cadres, des outils et des services avancés de renseignement sur les cybermenaces, ainsi qu'à des évaluations des risques de cybersécurité pour les chaînes d'approvisionnement critiques réalisées dans l'UE,
- Cadres, outils et services de préparation aux cybermenaces et aux menaces hybrides dans le domaine des technologies de l'information et de la communication (TIC) et des technologies opérationnelles (OT), y compris des exercices de cybersécurité,
- Extension des fonctionnalités des centres d'opérations de sécurité/équipes de réaction aux incidents de sécurité informatique (SOC/CSIRT) grâce à des outils et services avancés pour la détection, l'analyse, le traitement des incidents, y compris la réaction et l'établissement de rapports, ainsi que la remédiation,
- Développement d'installations d'essai et d'expérimentation pour les outils et processus avancés de cybersécurité opérationnelle, y compris la création de jumeaux numériques pour les infrastructures critiques et les entités essentielles et importantes telles que définies dans la NIS2,
- L'élaboration et la mise en œuvre pilote de cadres, de services et d'outils intersectoriels et/ou transfrontaliers de gestion des cybercrises,
- Cadres, services et outils visant à mettre en place des mécanismes et des processus de coopération opérationnelle renforcée entre les entités du secteur public (réseau CSIRT, EU-CyCLONe). L'extension de ce qui précède aux entités essentielles et importantes telles que définies dans NIS2 serait un avantage.

POINTS IMPORTANTS

- Lump sum
- Limité aux états membres et états associés
- Interdits aux entités détenues par des pays ou des entités de pays non éligibles
- Restreint aux réseaux de communication européens.

HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing Technologies

Technologies d'amélioration pour la protection de la vie privée

RÉSULTATS ATTENDUS / certains ou tous parmi

- Développement de technologies robustes, évolutives et fiables pour préserver la vie privée dans des cadres de partage de données fédérés et sécurisés, ainsi que dans le traitement de données personnelles et industrielles, intégrées dans des systèmes du monde réel.
- Développement d'approches préservant la vie privée pour les solutions de partage de données, y compris le partage d'informations sur les cybermenaces préservant la vie privée, et dans les calculs collaboratifs impliquant des données sensibles.
- Intégration de la protection de la vie privée dès la conception au cœur des processus de développement de logiciels et de protocoles, en veillant à ce que les blocs de construction cryptographiques et les implémentations de signatures numériques et de systèmes d'authentification de l'utilisateur respectueux de la vie privée soient cryptographiques et modulaires, afin de faciliter la transition vers des algorithmes cryptographiques post-quantiques.
- Contribution à l'avancement des espaces de données européens conformes au GDPR pour les services numériques et la recherche, tels que ceux sur les données de santé, en accord avec les thèmes DATA du cluster 4 d'Horizon Europe.
- Développement de technologies et de solutions renforçant la protection de la vie privée, pour répondre aux besoins des citoyens et des entreprises, y compris les petites et moyennes entreprises (PME).
- Développement de technologies de protection de la vie privée basées sur la blockchain et décentralisées, afin de préserver la confidentialité et l'intégrité des données, ainsi que l'authenticité des transactions et des actifs numériques. Combinaison possible de la blockchain avec d'autres technologies, telles que les systèmes d'information fédérés.

POINTS IMPORTANTS

- Lump sum
- Restreint aux réseaux de communication européens.

HORIZON-CL3-2025-02-CS-ECCC-04: Security evaluations of Post-Quantum Cryptography (PQC) primitives

Évaluation de la sécurité des primitives de cryptographie post-quantique (PQC)

RÉSULTATS ATTENDUS / certains ou tous parmi

- La compréhension du durcissement quantique de diverses classes de problèmes mathématiques qui sous-tendent la sécurité des cryptosystèmes post-quantiques actuels et futurs ;
- De nouveaux algorithmes quantiques avec une accélération significative pour des classes de problèmes mathématiques basés sur les réseaux (Lattice-based), basés sur du code (code-based) et potentiellement d'autres classes de problèmes mathématiques ;
- Amélioration de la mise en œuvre des algorithmes quantiques à l'aide de langages de programmation quantique de haut niveau pour résoudre les problèmes mathématiques constituant le cœur des cryptosystèmes ;
- La mise en place d'environnements permettant de tester la robustesse des cryptosystèmes face aux attaquants quantiques ;
- Approches basées sur l'IA pour aider à découvrir les vulnérabilités des classes de problèmes mathématiques basées sur les treillis ou autres ;
- Résultats de la cryptanalyse ;
- Suggestions de paramètres pour créer un ensemble robuste de blocs de construction cryptographiques pour la cybersécurité post-quantique et la conception de cryptosystèmes post-quantiques avec une sécurité améliorée contre les attaques quantiques ou basées sur l'IA.

POINTS IMPORTANTS

- Lump sum
- Limité aux états membres, états associés et états de l'OCDE
- Interdits aux entités détenues par des pays ou des entités de pays non éligibles
- Restreint aux réseaux de communication européens.

HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of Post-Quantum Cryptography algorithms

Sécurité des implémentations des algorithmes de cryptographie post-quantique

RÉSULTATS ATTENDUS / certains ou tous parmi

- Conception et mise en œuvre d'algorithmes de cryptographie post-quantique (PQC) résistants aux attaques par canaux latéraux et aux failles ;
- Des contre-mesures optimisées tenant compte d'un compromis équilibré entre la sécurité, les performances et les coûts ;
- Des recommandations sur la mise en œuvre de contre-mesures pour une large gamme d'attaques, en identifiant également le matériel disponible et nécessaire ;
- Analyse de nouvelles attaques ou combinaisons d'attaques, éventuellement améliorées par l'IA, applicables aux conditions du monde réel.
- Conception d'évaluations de sécurité automatisées pour les implémentations PQC.

POINTS IMPORTANTS

- Lump sum
- Limité aux états membres, états associés et états de l'OCDE
- Interdits aux entités détenues par des pays ou des entités de pays non éligibles
- Restreint aux réseaux de communication européens.

HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols

Intégration d'algorithmes de cryptographie post-quantique (PQC) dans des protocoles de haut niveau

RÉSULTATS ATTENDUS / certains ou tous parmi

- Conception et mise en œuvre d'au moins un protocole de cryptographie post-quantique de haut niveau, accompagné d'une analyse de sécurité démontrant qu'il n'y a pas de perte de sécurité par rapport aux blocs de construction/protocoles de niveau inférieur utilisés (KEM, signatures, AEAD,...) ;
- Soumission de ces protocoles de haut niveau intégrant la PQC à des organismes de normalisation et/ou soumission de la spécification et de la mise en œuvre aux projets open source respectifs ;
- Analyse des besoins mettant en évidence les obstacles et les besoins en matière de développement de solutions PQC pour les éléments de base manquants en vue de la migration des protocoles de haut niveau vers PQC.

POINTS IMPORTANTS

- Lump sum
- Limité aux états membres, états associés et états de l'OCDE
- Interdits aux entités détenues par des pays ou des entités de pays non éligibles
- Restreint aux réseaux de communication européens.

Disaster-Resilient Society For Europe



DRS 2025

- 4 appels / 10 lauréats, 41 M€
- 2 RIA, 2 IA
- 1 AAP SHS

HORIZON-CL3-2025-01-DRS-01 : Open topic L'engagement des citoyens et des autorités régionales et/ou locales dans une meilleure sensibilisation aux risques de catastrophes, y compris l'éducation, et la préparation

HORIZON-CL3-2025-01-DRS-02 : Open topic L'amélioration de la gestion des risques de catastrophes et de la gouvernance pour assurer l'autosuffisance et la durabilité des opérations en faveur d'une résilience accrue

HORIZON-CL3-2025-01-DRS-03 : Open topic L'essai et la validation d'outils, de technologies et de données utilisés dans la prévention, la préparation et les réponses transfrontalières aux événements climatiques extrêmes et géologiques et aux menaces d'urgence chimiques, biologiques ou radiologiques

HORIZON-CL3-2025-01-DRS-04 : Faire progresser les systèmes autonomes et la robotique pour les interventions en cas de catastrophe à haut risque, renforcer la résilience aux catastrophes dans les zones de crise touchées par des conflits



HORIZON-CL3-2025-01-DRS-01: Open topic on citizen and regional and/or local authorities' engagement in enhanced disaster risk awareness, including education, and preparedness

L'engagement des citoyens et des autorités régionales et/ou locales dans une meilleure sensibilisation aux risques de catastrophes, y compris l'éducation, et la préparation.

RÉSULTATS ATTENDUS / certains ou tous parmi

1. Amélioration de la préparation aux catastrophes, en tirant les leçons des catastrophes ou crises passées, et meilleur partage des connaissances sur les enseignements tirés et la sensibilisation aux risques des citoyens et des autorités régionales et/ou locales, en comprenant quelles contre-mesures ont été prises lors d'incidents antérieurs et en explorant les produits actuellement disponibles pour améliorer les résultats à l'avenir ;
2. Renforcer le dialogue et la coopération entre les communautés scientifiques et techniques, les parties prenantes, les décideurs politiques et les communautés régionales et/ou locales dans le domaine de la réduction des risques de catastrophes afin d'améliorer l'utilisation des résultats de la recherche.

POINTS IMPORTANTS

Option a : Outils et solutions pour améliorer la préparation

Option b : mécanisme visant à renforcer le dialogue entre les communautés

CONSORTIUM

- au moins 2 autorités régionales et/ou locales
- au moins 2 organisations représentant les citoyens ou les communautés régionales et/ou locales
- au moins 2 primo-intervenants ou autorités de gestion des catastrophes
- d'au moins 3 États membres différents de l'UE ou pays associés

HORIZON-CL3-2025-01-DRS-02: Open topic on Improving disaster risk management and governance to ensure self-sufficiency and sustainability of operations in support of enhanced resilience

L'amélioration de la gestion des risques de catastrophes et de la gouvernance pour assurer l'autosuffisance et la durabilité des opérations en faveur d'une résilience accrue

RÉSULTATS ATTENDUS

- Meilleure compréhension de l'impact des catastrophes et des crises, et amélioration des alertes précoces et de la planification à long terme liées à des causes naturelles ou à des menaces d'origine humaine (y compris CBRN) sur la gouvernance des risques, y compris les services d'urgence, les autorités régionales et/ou locales et les citoyens volontaires, et amélioration de l'adaptation et de la résilience des systèmes d'urgence pour la prévention des catastrophes et la préparation aux catastrophes - en particulier dans un environnement à risques multiples où les catastrophes se succèdent en cascade.

POINTS IMPORTANTS

Entités juridiques établies dans les pays d'Amérique latine/Afrique/Caraïbes/Asie centrale sont éligibles

CONSORTIUM

- au moins 2 autorités régionales et/ou locales
- au moins 1 autorité de gestion des catastrophes
- au moins 1 organisation de volontaires
- d'au moins 3 États membres différents de l'UE ou de pays associés

HORIZON-CL3-2025-01-DRS-03: Open topic on testing / validating tools, technologies and data used in cross-border prevention, preparedness and responses to climate extreme and geological events and chemical, biological or radiological emergency threats

L'essai et la validation d'outils, de technologies et de données utilisés dans la prévention, la préparation et les réponses transfrontalières aux événements climatiques extrêmes et géologiques et aux menaces d'urgence chimiques, biologiques ou radiologiques.

RÉSULTATS ATTENDUS

- Renforcement de l'interopérabilité européenne et mondiale des outils et technologies existants et amélioration des capacités de prévention, de préparation et de réaction à différents types de catastrophes (naturelles ou causées par l'homme) par divers praticiens (par exemple, les pompiers, les intervenants médicaux, la protection civile).

POINTS IMPORTANTS

Entités juridiques établies dans les pays d'Amérique latine/Afrique/Caraïbes/Asie centrale sont éligibles

CONSORTIUM

- au moins 2 primo-intervenants
- au moins 2 PME
- d'au moins 3 états membres différents de l'UE ou de pays associés

HORIZON-CL3-2025-01-DRS-04: Advancing autonomous systems and robotics for high-risk disaster response, strengthening disaster resilience in conflict-afflicted crisis zones

Faire progresser les systèmes autonomes et la robotique pour les interventions en cas de catastrophe à haut risque, renforcer la résilience aux catastrophes dans les zones de crise touchées par des conflits

RÉSULTATS ATTENDUS / certains ou tous parmi

- Développer et/ou adapter un système autonome multifonctionnel pour les scénarios à haut risque, capable de relever les défis uniques posés par les catastrophes provoquées par les conflits, tels que les structures instables et les environnements urbains fortement obstrués. Ce système exécutera ou soutiendra des tâches civiles telles que la recherche et le sauvetage, l'évaluation des risques et le transport de fournitures dans des zones trop dangereuses pour les intervenants humains ;
- Amélioration de la télédétection et de la connaissance de la situation : création de technologies basées sur des capteurs qui améliorent la connaissance de la situation pour les premiers intervenants et les décideurs, leur permettant d'évaluer les zones sinistrées à distance et en toute sécurité ;
- Capacités de navigation et de recherche autonomes dans des environnements dangereux, en mettant l'accent sur les technologies qui améliorent la capacité des systèmes autonomes à effectuer des opérations de recherche dans des conditions de faible visibilité ou de fumée, typiques des zones touchées par des attentats à la bombe, des incendies ou d'autres incidents liés à des conflits ;
- des essais centrés sur l'utilisateur et en conditions réelles dans des environnements qui reproduisent les conditions des zones de conflit et des catastrophes urbaines ;
- Le renforcement des capacités et la formation pour le déploiement de systèmes autonomes, en fournissant des directives de formation spécialisées pour les premiers intervenants et les agences de protection civile afin d'exploiter et d'entretenir les systèmes autonomes de manière efficace dans des scénarios de conflit.

CONSORTIUM

- Au moins 3 organisations ou agences de primo intervenants d'au moins 3 États membres de l'UE ou pays associés, y compris l'Ukraine.

Strengthening Security Research Innovation





SSRI 2025

- 6 appels / 7 lauréats, 21.5 M€
- 2 IA, 3 CSA, 1PCP

HORIZON-CL3-2025-01-SSRI-01 : Points de contact nationaux (PCN) dans le domaine de la sécurité et de la cybersécurité, favorisant les liens avec la construction de communautés nationales pour des sociétés sûres, sécurisées et résilientes.

HORIZON-CL3-2025-01-SSRI-02 : Services d'accélération de la mise en œuvre

HORIZON-CL3-2025-01-SSRI-03 : Permettre les achats publics avant commercialisation de technologies de sécurité innovantes

HORIZON-CL3-2025-01-SSRI-04 : Accélérer l'adoption de propositions ouvertes pour l'innovation avancée des PME

HORIZON-CL3-2025-01-SSRI-05 : Référentiel de données pour la recherche et l'innovation en matière de sécurité

HORIZON-CL3-2025-01-SSRI-06 : Innovation axée sur la demande en matière de sécurité civile grâce aux achats publics avant commercialisation (PCP)

Les défis

- **Eviter les préjugés sectoriels et briser les silos et la fragmentation du marché** qui entravent la prolifération de solutions de sécurité communes
- **R&I plus performante** pour le développement de **capacités de sécurité utilisables et utilisées par des praticiens de la sécurité et utilisateurs finaux**
- **Compétitivité de l'industrie de la sécurité de l'UE et sécurité des approvisionnements** en produits de l'UE dans des domaines de sécurité clés.

Impact attendu de la Destination SSRI

- Générer des **connaissances** et de la **valeur** dans des **domaines transversaux**
- Renforcer les principaux piliers du cycle de recherche et d'innovation
- **Soutenir l'adoption de l'innovation et les stratégies de mise sur le marché** pour Industrialisation, commercialisation, et déploiement accrus des résultats
- Développement de technologies de sécurité **socialement acceptables**



HORIZON-CL3-2025-01-SSRI-01: National Contact Points (NCPs) in the field of security and cybersecurity fostering the links with National Community building for Safe, Secure and Resilient Societies

Points de contact nationaux (PCN) dans le domaine de la sécurité et de la cybersécurité, favorisant les liens avec la construction de communautés nationales pour des sociétés sûres, sécurisées et résilientes.

RÉSULTATS ATTENDUS / certains ou tous parmi

•Un service amélioré et professionnalisé de connaissances, d'expériences et de compétences des PCN, cohérent dans toute l'Europe, contribuant ainsi à simplifier l'accès aux appels d'Horizon Europe, à abaisser les barrières à l'entrée pour les nouveaux arrivants et à augmenter la qualité moyenne des propositions soumises ;

CONSORTIUM

Les candidats doivent être des structures nationales de soutien Horizon Europe (Points de contact nationaux - PCN),s de travail antérieurs



HORIZON-CL3-2025-01-SSRI-02: Uptake Acceleration Services

Services d'accélération de la mise en œuvre

RÉSULTATS ATTENDUS / certains ou tous parmi

- Offrir des services avancés sur l'adoption de l'innovation à la communauté de la sécurité ;
- Fournir un mécanisme autonome pour des services avancés de conseil et de soutien, agir en tant que catalyseur du marché et accélérer l'adoption de l'innovation pour la sécurité ;
- Renforcer la coopération entre les institutions de recherche, les petites agences de recherche privées, les praticiens de la sécurité, les start-ups et les PME pour soutenir l'adoption de l'innovation ;
- Renforcer le transfert de technologie de la recherche vers le marché et renforcer l'écosystème de la sécurité. Soutenir les start-ups et les PME pour qu'elles atteignent le marché de la sécurité et renforcer la capacité des praticiens de la sécurité à adopter les outils innovants du marché de la sécurité.

POINT IMPORTANT

Les bénéficiaires peuvent apporter un soutien financier à des tiers. Le montant maximum est de 60 000 EUR.

CONSORTIUM

au moins 2 organismes de recherche et de technologie.

HORIZON-CL3-2025-01-SSRI-03: Open grounds for pre-commercial procurement of innovative security technologies

Permettre les achats publics avant commercialisation de technologies de sécurité innovantes

RÉSULTATS ATTENDUS / certains ou tous parmi

- Une demande consolidée de technologies de sécurité innovantes fondée sur l'agrégation d'acheteurs publics ayant un besoin commun exprimé en termes fonctionnels et/ou opérationnels, sans prescrire de solutions techniques ;
- une prise de décision mieux informée concernant l'investissement dans les technologies de sécurité innovantes, fondée sur une meilleure compréhension de l'offre potentielle, au niveau de l'UE, d'alternatives techniques susceptibles de répondre aux besoins communs des acheteurs publics de l'UE ;
- une prise de décision mieux informée en ce qui concerne les investissements dans les technologies de sécurité innovantes, grâce à une meilleure visibilité de la demande potentielle sur le marché de l'UE pour des technologies de sécurité communes ;
- Capacité accrue des acheteurs publics de l'UE à aligner leurs exigences sur celles de l'industrie et des produits futurs et à attirer l'innovation et les innovateurs du secteur de la sécurité et d'autres secteurs grâce à des stratégies de validation communes, à l'innovation rapide, à l'expérimentation et aux achats publics avant commercialisation ;
- Renforcement de la capacité d'innovation des acheteurs publics de l'UE grâce à la disponibilité d'orientations novatrices en matière d'appels d'offres, de stratégies de validation adoptées d'un commun accord et de perspectives fondées sur des données probantes en ce qui concerne la passation de nouveaux marchés conjoints pour des solutions de sécurité communes.

CONSORTIUM

- au moins 6 end-users
- au moins 3 acheteurs publics.
- d'au moins 3 États membres de l'UE ou pays associés différents.

HORIZON-CL3-2025-01-SSRI-04: Accelerating uptake through open proposals for advanced SME innovation

Accélérer l'adoption de propositions ouvertes pour l'innovation avancée des PME

RÉSULTATS ATTENDUS / certains ou tous parmi

- Développement d'une solution technologique mature répondant aux priorités de la politique de sécurité de l'UE dans les domaines abordés par le programme de travail du groupe 3 et en particulier la destination de la lutte contre la criminalité et le terrorisme, les sociétés résilientes aux catastrophes, la gestion des frontières et les infrastructures résilientes.
- Accès facilité au marché de la sécurité civile pour les petits innovateurs ;
- Amélioration de la coopération entre les acheteurs publics et les petits acteurs du marché de l'approvisionnement pour une adoption plus rapide de l'innovation en réponse aux besoins à court et à moyen terme ;
- des partenariats plus solides entre les petites et moyennes entreprises de sécurité de l'UE et les acteurs technologiques pour assurer la durabilité de la capacité d'innovation de l'UE dans le domaine de la sécurité civile et réduire les dépendances technologiques à l'égard des fournisseurs non européens dans les domaines critiques de la sécurité.

CONSORTIUM

Minimum 3 et maximum 7 partenaires et

Au moins 2 PME de 2 États membres différents.

Au moins une organisation d'utilisateurs finaux

Au moins 3 États membres ou pays associés doivent être représentés dans le consortium.

La participation d'industries non-PME et de RTO n'est pas exclue, mais elle doit être limitée à 15% du budget.

Au moins 50% du budget doit être alloué aux PME.

Coordination de PME encouragé

Durée maximum de 2 ans

POINT IMPORTANT

Lump Sum



HORIZON-CL3-2025-01-SSRI-05: Data repository for security research and innovation

Référentiel de données pour la recherche et l'innovation en matière de sécurité

RÉSULTATS ATTENDUS / certains ou tous parmi

- Des données de formation et d'expérimentation de la recherche collectées, stockées, gérées et préservées avec précision, ventilées par sexe le cas échéant, qui sont vérifiées et sélectionnées afin d'être réalistes, actualisées et suffisantes, et de rendre la recherche plus digne de confiance et reproductible ;
- Les chercheurs et les projets peuvent encore accroître l'impact et la visibilité de leur travail en ne se contentant pas d'archiver les documents de recherche, mais en les ouvrant à la réutilisation et à la citation par d'autres acteurs et parties prenantes concernés ;
- Des données de recherche pertinentes correctement partagées et réutilisées peuvent sauver des vies, aider à développer des solutions et maximiser les connaissances ;
- Amélioration de la collaboration au sein de la communauté des chercheurs concernés, amélioration de la confiance entre les chercheurs et les praticiens/utilisateurs finaux, facilitation de la coopération entre les différents projets de recherche et réduction de la charge de la recherche gaspillée ou des résultats perdus.

CONSORTIUM

HORIZON-CL3-2025-01-SSRI-06: Open grounds for pre-commercial procurement of innovative security technologies

Innovation axée sur la demande en matière de sécurité civile grâce aux achats publics avant commercialisation (PCP)

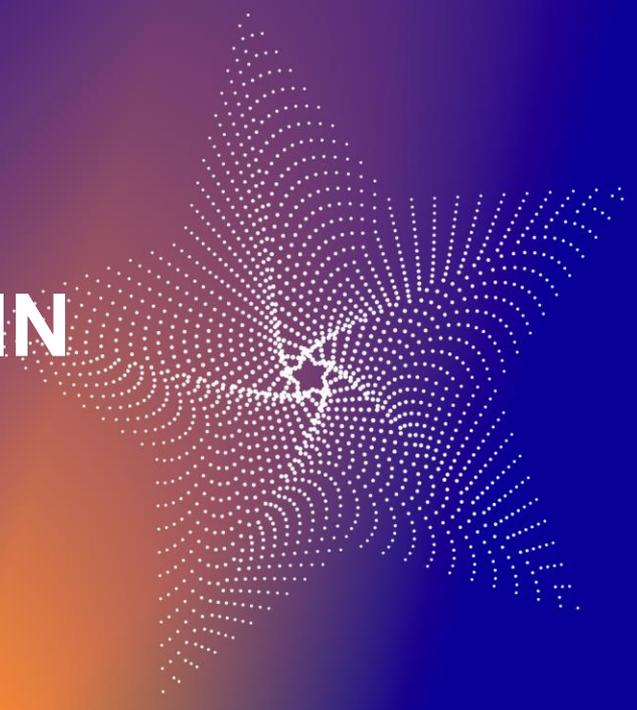
RÉSULTATS ATTENDUS / tous parmi

- Une communauté de praticiens de la sécurité civile de l'UE ayant des besoins communs en matière de solutions technologiques innovantes, soutenus par une base industrielle, en particulier des PME et des start-ups, pour accéder au marché des marchés publics et développer leurs activités ;
- Les acheteurs facilitent la commercialisation de solutions innovantes par leurs fournisseurs retenus en leur fournissant les premières références de clients pour la validation et le premier déploiement pilote ;
- Augmentation des possibilités d'adoption par le marché et d'économies d'échelle pour l'offre grâce à une demande accrue de solutions innovantes, à une large publication des résultats et, le cas échéant, à une contribution à la normalisation, à la réglementation ou à la certification ;
- Soutenir les acheteurs publics pour qu'ils mettent en œuvre collectivement des PCP afin de stimuler l'innovation du côté de la demande et d'ouvrir des opportunités de commercialisation plus larges pour les entreprises européennes afin qu'elles prennent ou conservent une position de leader international sur de nouveaux marchés susceptibles d'offrir des solutions innovantes.

CONSORTIUM

- au moins 3 end-users
- au moins 3 acheteurs publics.
- d'au moins 3 États membres de l'UE ou pays associés différents.

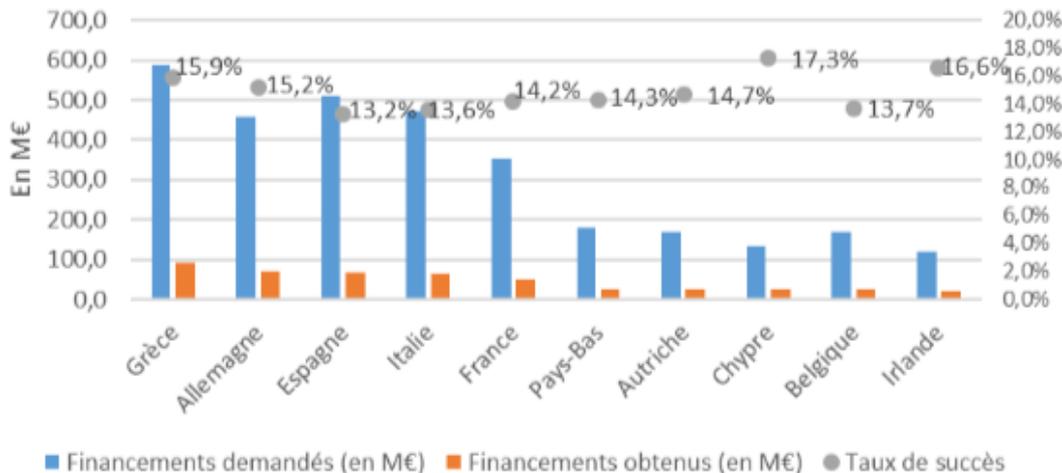
POUR ALLER PLUS LOIN



Positionnement de la France à mi-parcours Financements

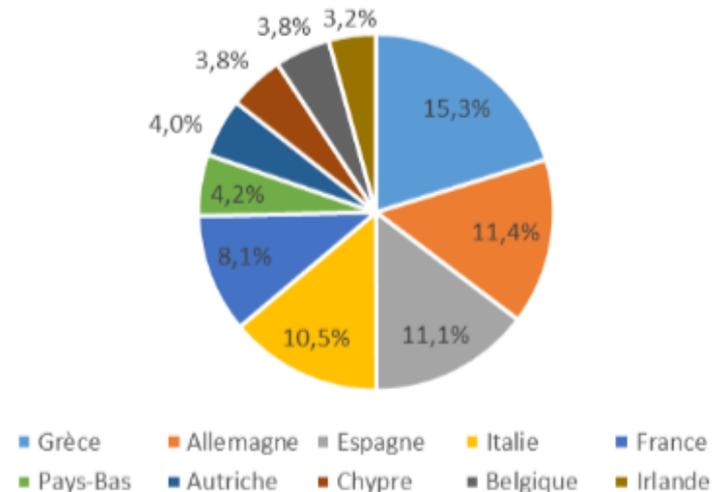
Cluster 3 - Top 10 UE

Financements demandés et obtenus & taux de succès



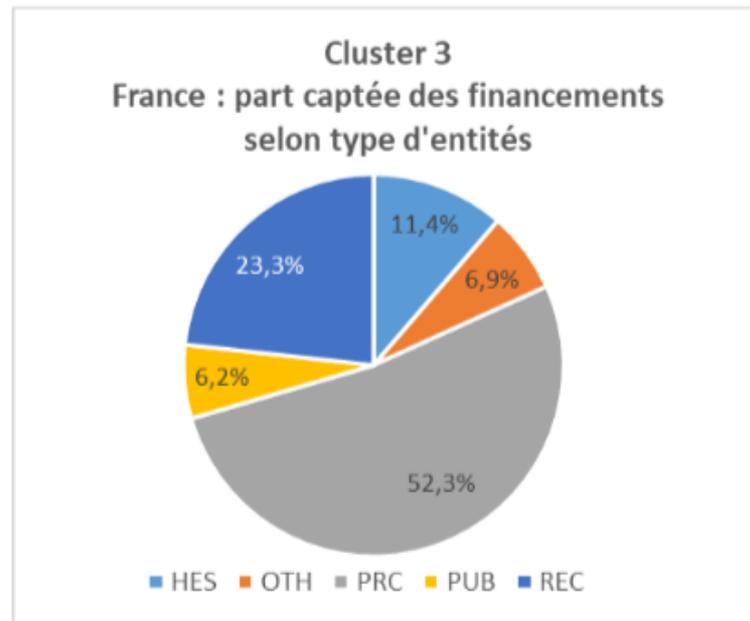
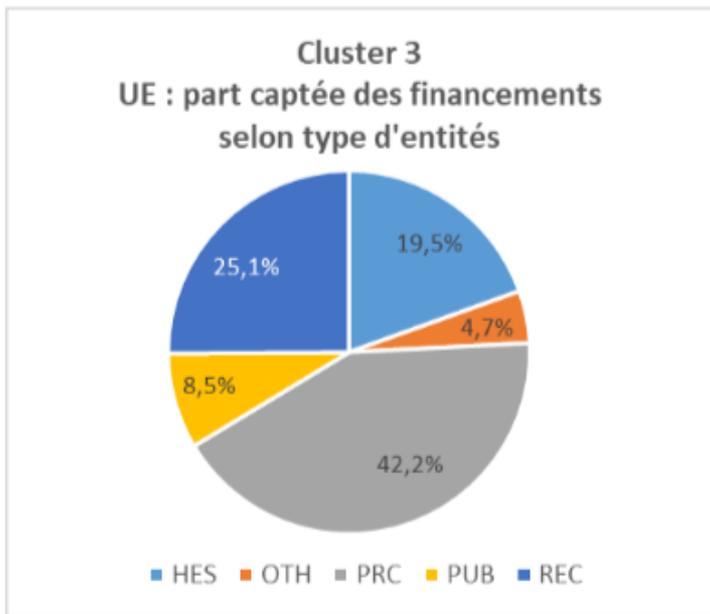
Cluster 3

Top 10 UE : part captée des financements



Positionnement de la France à mi-parcours

Typologie des lauréats



Positionnement de la France à mi-parcours

Position	Top 20 Entités européennes	Financements obtenus (en M€)	Top 20 Entités françaises	Financements obtenus (en M€)
1	EL-Centre for Research and Technology Hellas	12,2	CEA	6,8
2	IT-Engineering (Italy)	8,8	Thales	4,7
3	DE-Fraunhofer Society	8,7	CS group	2,1
4	EL-Center for Security Studies	8,7	Ministère de l'Intérieur et des Outre-mer	1,7
5	FR-CEA	6,8	Montimage	1,6
6	AT-Austrian Institute of Technology	6,7	Institut Mines-Télécom (IMT)	1,4
7	EL/CY-Ubitech	5,5	Idemia	1,3
8	EL-Institute of Communication and Computer Systems	5,3	Red alert labs	1,2
9	LU-INTRASOFT International	5,1	Airbus Defense and Space	1,2
10	FR-Thales	4,7	Privanova	1,1
11	DE-Aegis it research gmbh	4,4	Civipol	0,9
12	PT-Institute for Systems Engineering and Computers	4,4	SAFE Cluster	0,8
13	NL-Delft University of Technology	3,9	Sopra Steria	0,8
14	NL-Netherlands Organisation for Applied Scientific Research	3,9	Synnav	0,8
15	IT-National Research Council	3,8	CNRS	0,7
16	EL-Athena R&I Center In Info. Comm. & Knowledge Technologies	3,6	Pompiers de l'urgence internationale	0,7
17	EL-National Centre of Scientific Research "Demokritos"	3,5	Institut Pasteur	0,7
18	ES-Universitat Politècnica de Catalunya	3,4	BRGM	0,6
19	ES-Atos	3,2	Nokia	0,6
20	ES-Tecnalia	3,2	Vinci	0,6

Positionnement de la France à mi-parcours

France : destinations du Cluster 3		Financements demandés (M€)	Financements obtenus (M€)	Taux de succès	Part captée des financements européens par la France	Place de la France au regard des financements obtenus
Destination 1	Lutte contre la criminalité et le terrorisme	44,7	7,7	17,2 %	6,5 %	5
Destination 2	Gestion des frontières	33,7	7,4	21,8 %	7,8 %	4
Destination 3	Infrastructure résiliente	18,6	3,0	16,2 %	6,8 %	6
Destination 4	Renforcement de la cybersécurité	162,5	16,2	10,0 %	8,1 %	5
Destination 5	Société résiliente aux catastrophes pour l'Europe	84,0	11,8	14,1 %	9,4 %	4
Destination 6	Renforcement de la recherche et de l'innovation en matière de sécurité	6,8	3,0	43,3 %	12,6 %	1
Cluster 3 other	Cluster 3 autre	0,61	0,63	N/P	N/P	N/P
Total général		350,9	49,7	14,2 %	8,1 %	5



6 CLUSTERS - 34 destinations	
<u>Calls Cluster 1 - Health</u>	<u>Calls destinations Digital Cluster 4</u>
<ul style="list-style-type: none"> Destination 1 : Staying Healthy in a rapidly changing society Destination 2 : Living and working in a health promoting environment Destination 3 : Tackling diseases and reducing disease burden Destination 4 : Ensuring access to innovative, sustainable and high-quality health-care Destination 5 : Unlocking the full potential of new tools, technologies and digital solutions for a healthy society Destination 6 : Maintaining an innovative, sustainable and globally competitive health industry 	<ul style="list-style-type: none"> Destination 3 – World leading data and computing technologies Destination 5 – A human-centred and ethical development of digital and industrial technologies Destination 6 – Climate neutral, circular and digitised production
	<u>Calls destination Space and Earth Observation Cluster 4</u>
	<ul style="list-style-type: none"> Strategic Autonomy in developing, deploying and using Global Space-based Infrastructures, Services, Applications and Data
	<u>Calls Cluster 5 - Climate, Energie and Mobility.</u>
<u>Calls Cluster 2 - Culture, Creativity and inclusive Society</u>	<u>Calls destinations Climate - Energie Cluster 5</u>
<ul style="list-style-type: none"> Destination 1 – Innovative Research on Democracy and Governance Destination 2 – Innovative Research on the European Cultural Heritage and the Cultural and Creative Industries Destination 3 – Innovative Research on Social and Economic Transformations 	<ul style="list-style-type: none"> Destination 1 – Climate sciences and responses for the transformation towards climate neutrality Destination 2 – Cross-sectoral solutions for the climate transition Destination 3 – Sustainable, secure and competitive energy supply Destination 4 – Efficient, sustainable and inclusive energy use
<u>Calls Cluster 3 - Civil Security for Society</u>	
<ul style="list-style-type: none"> Destination 1 - Fighting Crime and Terrorism Destination 2 - Border Management Destination 3 - Resilient Infrastructure Destination 4 - Increased Cybersecurity Destination 5 - Disaster-Resilient Society for Europe Destination 6 - Strengthened Security Research and Innovation 	<u>Calls destinations Transport Cluster 5</u>
	<ul style="list-style-type: none"> Destination 2 – Cross-sectoral solutions for the climate transition Destination 5 – Clean and competitive solutions for all transport modes Destination 6 – Safe, Resilient Transport and Smart Mobility services for passengers and goods
<u>Calls Cluster 4 - Digital, industry and space</u>	<u>Calls Cluster 6 - Food, Bioeconomie, Natural Resources, Agriculture and Environment.</u>
<u>Calls destinations Industry Cluster 4</u>	<ul style="list-style-type: none"> Destination 1 : Biodiversity and Ecosystem Services Destination 2 : Fair, healthy and environmentally friendly food systems from primary production to consumption Destination 3 : Circular economy and bioeconomy sectors Destination 4 : Clean Environment and zero pollution Destination 5 : Land, ocean and water for climate action Destination 6 : Resilient, inclusive, healthy and green rural, coastal and urban communities Destination 7 : Innovative governance, environmental observations and digital solutions in support of the Green Deal
<ul style="list-style-type: none"> Destination 1 : Climate neutral, circular and digitised production Destination 2 : Increased autonomy in key strategic value chains for resilient industry 	

Roadmap PCN Cluster 3 2025

26-27
mars 2025

WISG

Se faire connaître et identifier des partenaires académiques

- Identifier des partenaires académiques, notamment SHS
- Rencontrer des partenaires aguerris

17
avril 2025

Webinaires

Identifier les appels

- Comprendre le programme
- Qui peut participer ?
- Trouver un sujet adapté
- Attendus, vision
- Evaluation sujet, adéquation stratégie

6-7
mai 2025

SMI2G

Brokerage event européen

- Se faire connaître, identifier des partenaires européens
- Identifier et /ou construire un consortium européen
- Trouver de nouveaux acteurs et des partenaires de confiance

12/
11/
25

deadline des candidatures

EN CONTINU : tournée du PCN en Régions, réunions bilatérales... tenez-vous au courant : je reste informé

Contactez-nous : pcn-securite@recherche.gouv.fr

Liens et outils

- Le site de la CE **Funding and Tenders** : tous les programmes UE, candidature aux AAP, devenir expert évaluateur...
outil Partner search
- Le **portail français pour Horizon Europe** : actualités, évènements, documentation en français, statistiques, contacts des PCN...

Financer une aide au montage

- Académique / Entité publique : **ANR – MRSEI**
 - 35 000 euros pour aider le coordinateur/trice à monter son consortium
 - 4 vagues par an
- PME : **Diagnostic Europe BPI**
 - Prestation d'accompagnement de conseil réalisée par un expert dans les financements européens
 - Dont accompagnement à la rédaction du dossier de candidature

Contactez votre région pour identifier les aides que certaines proposent pour les projets européens, ou **cliquez ici** pour consulter les aides que nous avons identifiées

Devenez expert-évaluateur pour HORIZON EUROPE

Pourquoi

- ✓ Comprendre l'**évaluation** des projets, les attendus
- ✓ Être en **contact direct avec les responsables** des Directions thématiques de la CE
- ✓ Bénéficier d'un **environnement de travail international** - réseautage
- ✓ Bénéficier d'**un état de l'art** à l'instant T dans votre domaine

Comment

- **Inscription une seule fois** pour 7 ans → **Mise à jour régulière de votre profil**
- La CE interroge la base de données à travers des **mots clés** pour solliciter les experts et constituer ses panels d'évaluation

Liens

- [Guide pour devenir expert](#)
- [S'enregistrer comme expert](#)

PCN Sécurité



Frédéric Perlant
Coordinateur & RCP



Jean-Florian Bacquey-Roullet
Membre



pcn-securite@recherche.gouv.fr

<https://www.horizon-europe.gouv.fr/cluster-3-securite>