MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATION
Liberté
Égalité
Fraternité

horizon europe

Webinaire Cluster 3

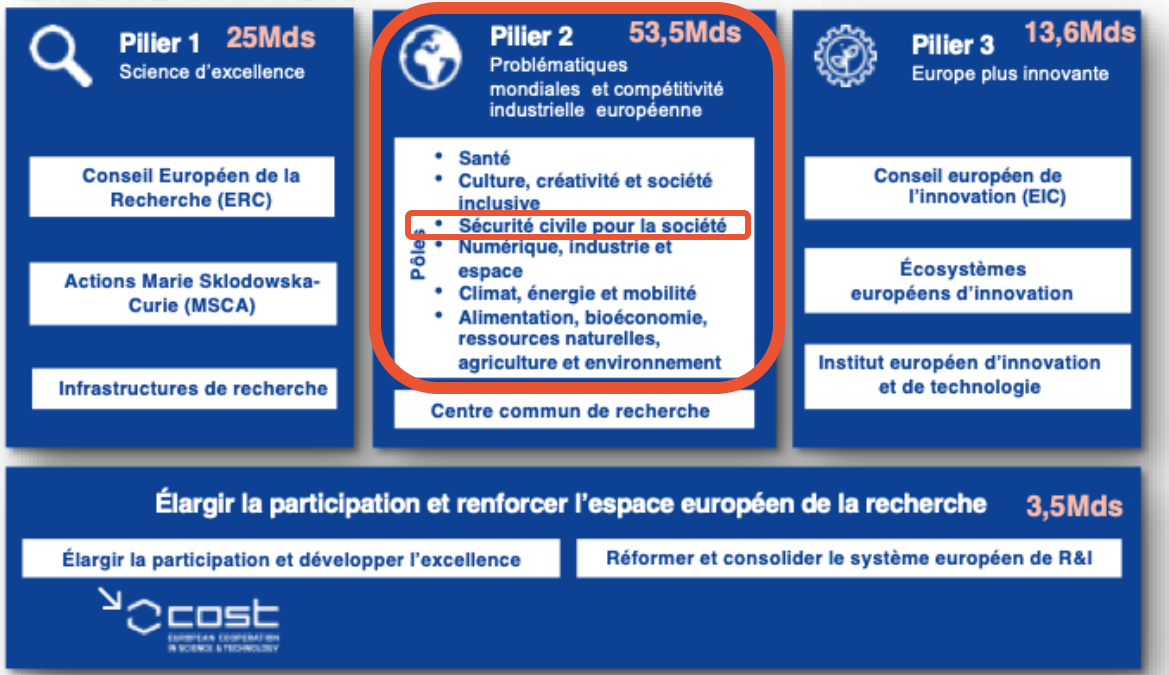
Resilient Infrastructure
Increased Cybersecurity
Strengthening Security Research and Innovation

4 février 2022

Frédéric PERLANT, Membre du PCN Cluster 3

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.*



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** trans**disciplinaires**, trans**sectoriels** et trans**nationaux**
- **3-4 ans** en moyenne
- Minimum **2-3 Millions** d'euros, **4-5 Millions** en moyenne
- **3 types de projets :** RIA, IA, CSA

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 apparaitre (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 :
Albanie, Arménie, Bosnie-Herzégovine, Géorgie, Iles Féroé, Islande, Israël, Kosovo, Maroc, Macédoine du Nord, Moldavie, Monténégro, Norvège, Serbie, Tunisie, Turquie, Ukraine, Royaume-Uni
Ø Attention, la Suisse n'en fait pas partie

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*

L'évaluation des projets Horizon Europe

3 critères principaux d'évaluation:

- **excellence,** (Open Science évaluées comme élément de la méthode scientifique)
- **impact,** (intégrer les Key Impacts Pathways)
- **qualité et efficience de la mise en œuvre,** (partenariat, mais pas la structure de management)

➢ **Attention** aux critères supplémentaires & pondération différente du programme de travail

Evaluation par les pairs: comités d'experts indépendants, les « experts-évaluateurs »

Temps dévolu à l'évaluation: **5 mois maximum** (+ 3 mois de contractualisation)

Nouveautés:

- Réduction de la taille des propositions: **45** pages maximum (**30** pour les CSA) avec moins d'infos demandées (management)
- « Droit de réagir »: permettant des remarques des proposants en cours d'évaluation (pilote)

Les Key Impact Pathways de la partie « Impact ».

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

- 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**
- **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
- 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**

Trois types de projets collaboratifs (instruments de financement)

RIA – Research and Innovation Actions (TRL 4-5)

⇢ Projets visant à **établir de nouvelles connaissances** et/ou à **explorer la faisabilité** d'une technologie, d'un produit, d'un procédé ou d'un service : *recherche fondamentale et appliquée, développement de technologie, essais d'un prototype à petite échelle...*

IA – Innovation Actions (TRL 7-8)

⇢ Projets visant à produire des **plans, arrangements ou concepts pour un produit, procédé ou service** nouveau ou amélioré : *prototypage, essais, démonstration ou pilotes, validation du produit à grande échelle, première commercialisation...*

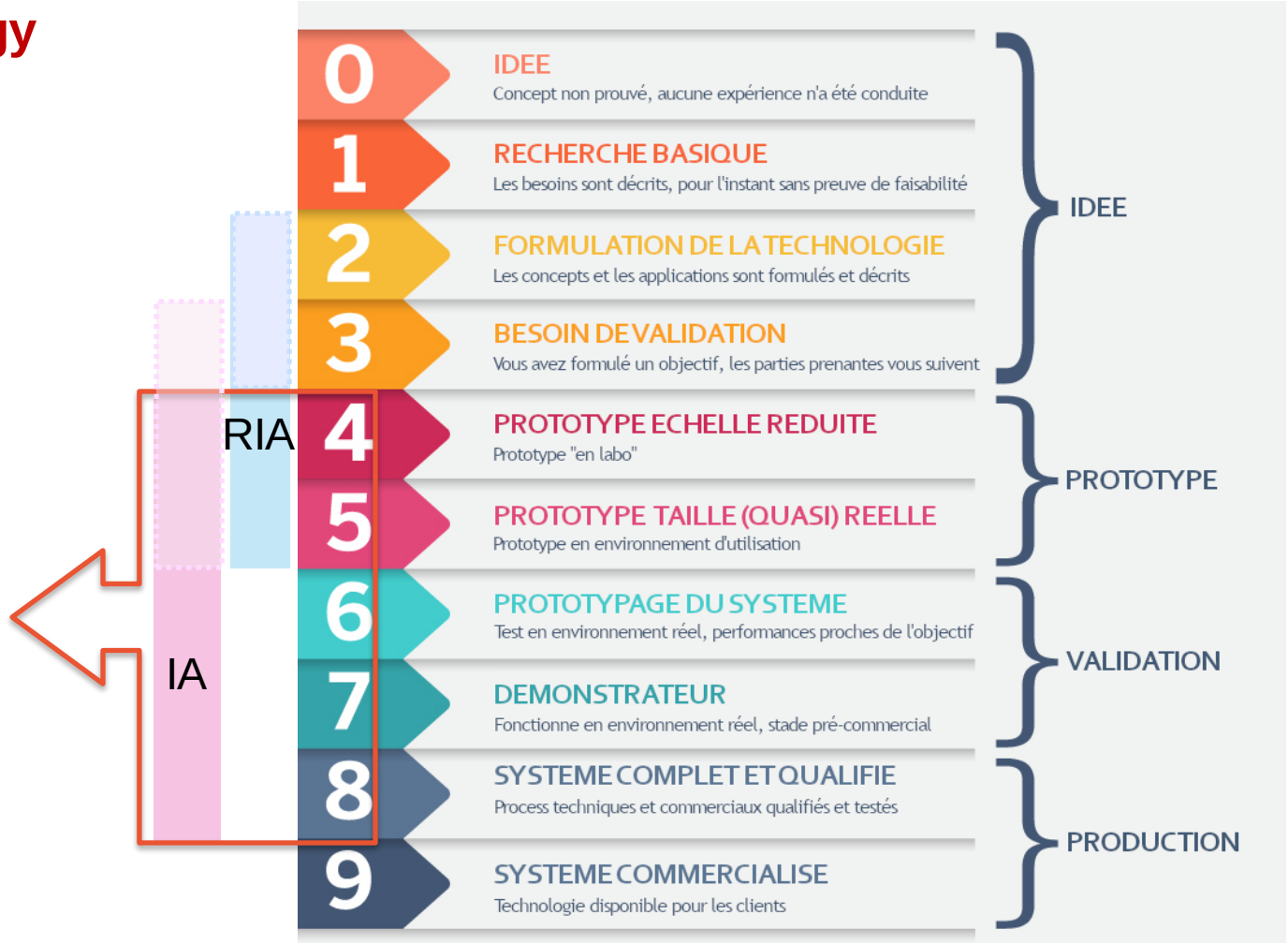
CSA – Coordination and Support Actions

⇢ Projets consistant principalement en des **mesures d'accompagnement** : *mise en réseau des acteurs, actions de communication et sensibilisation, dialogue politique, production d'études/rapports, planification stratégique...*

TRL : Technology Readiness Level

= Niveau de maturité technologique

Calls Cluster 3



D'où vient un appel à projets européen

Programme HORIZON EUROPE

- **7 ans**
- Cadre législatif
- Domaines d'intervention
- Architecture : Piliers/**Clusters**

Planification stratégique HE

- **4 ans**
- Priorités politiques européennes
- Orientations stratégiques clés
- **Impacts attendus**

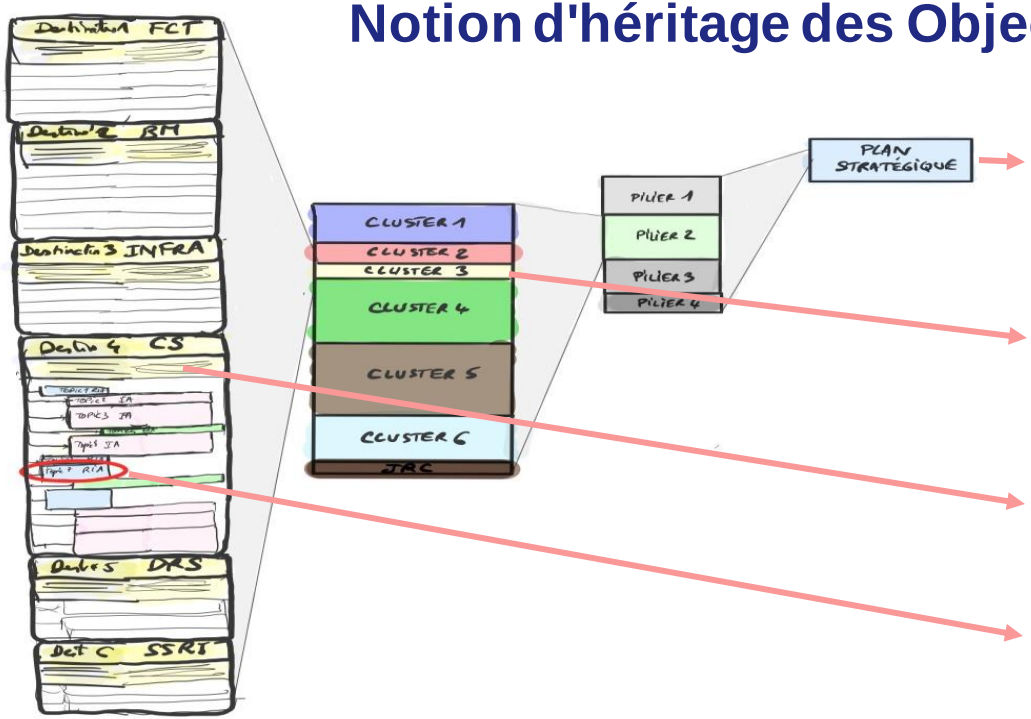
Programme de Travail de chaque Cluster

- **2 ans**
- Des **appels** « *topics* » regroupés en **destinations**

CLUSTER 3 "CIVIL SECURITY FOR SOCIETY

- **Work Programme 2021 – 2022**
  - § **Destination 1 :** Better protect the EU and its citizens against Crime and Terrorism
    - § **Topic :** HORIZON-CL3-2022-FCT-01-01:
      Improved crime scene investigations related to transfer, persistence and background abundance

Notion d'héritage des Objectifs et Impacts attendues



Description des Impacts attendus du Plan stratégique

Description du Programme de Travail du Cluster

Description de sa Destination

Un "Topic" dans une destination hérite

"As those challenges are rapidly evolving and social and technological developments are making a response increasingly complex, security research can serve as a tool to **move from a reactive approach to security to a proactive approach based on foresight, prevention and anticipation**."

Horizon Europe Strategic Plan 2021-2024, p. 57

Cluster 3 will support in particular the following two Horizon Europe key strategic orientations and impact areas associated to them[24]

KEY STRATEGIC ORIENTATIONS FOR R&I	KSO A: Promoting an open strategic autonomy by leading the development of key digital, enabling and emerging technologies, sectors and value chains	KSO D: Creating a more resilient, inclusive and democratic European society
IMPACT AREAS	Competitive and secure data-economy Secure and cybersecure digital technology	A resilient EU prepared for emerging threats A secure, open and democratic EU society
EXPECTED IMPACTS	**14.** Increased cybersecurity and a more secure online environment	**11.** Enhanced disaster risk reduction **12.** Improved air/land/sea border management & maritime security **13.** Tackling crime and terrorism, and threats to infrastructures

Cluster 3 : Civil Security for Society

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**

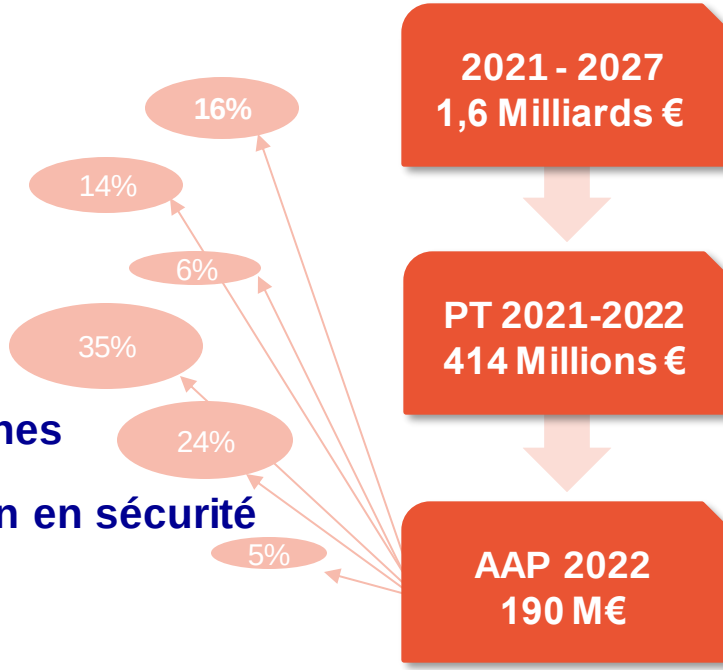
Orientations Stratégiques et Impacts attendus

- ➢ **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 technologies numériques »**
  - ➢ Technologies numériques sécurisées et cybersécurisées

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**
7) **Calendrier**

Appels 2022 : **deadline 16 (IC) ou 23 novembre 2022**



Les destinations et domaines des appels 2021-22 du cluster 3

Destination FCT
56 - 31M€

Domaine FCT01
Analyse de l'information

Domaine FCT02
Collecte de preuves légales

Domaine FCT03
Lutte & dissuasion sur la criminalité

Domaine FCT04
Lutte contre le terrorisme, espaces publics inclus

Domaine FCT05
Lutte contre la criminalité organisée

Domaine FCT06
Lutte contre la cyber criminalité

Destination BM
30,5 - 25M€

Domaine BM01 Surveillance des frontières et sécurité maritime

Domaine BM02 Sécurisation et facilitation du franchissement des frontières extérieures

Domaine BM03
Sécurité des douanes et de la chaîne d'approvisionnement

Destination RI
20 - 11M€

Domaine INFRA01
Préparation et réponse aux perturbations importantes des infrastructures européennes

Domaine INFRA02
Résilience et sécurité des villes

Destination IC
67,5 - 67,5M€

Domaine CS01
Infrastructures numériques et systèmes interconnectés

Domaine CS02
Sécurité du matériel, logiciels et supply chain

Domaine CS03
Technologies de rupture

Domaine CS04
Assurance et certification de sécurité intelligente quantifiable

Domaine CS05
Sécurité centrée sur l'homme, vie privée et éthique

Destination DRS
26 - 46M€

Domaine DRS01
Résilience sociétale : Risques accrus Sensibilisation et préparation des citoyens

Domaine DRS02
Gestion des risques de catastrophes et gouvernance

Domaine DRS03
Renforcement des capacités des premiers intervenants

Destination SSRI
16 - 9,5M€

Domaine SSRI01
Renforcer les piliers de Recherche et innovation en matière de sécurité

Domaine SSRI02
Accroître l'adoption de l'innovation

Domaine SSRI03
Connaissances transversales et valeurs pour les solutions de sécurité communes

Destination INFRA – Resilient infrastructure

RIA	INFRA02 - Resilient and secure smart cities	HORIZON-CL3-2022-INFRA-01-01: Nature-based Solutions integrated to protect local infrastructure
IA		HORIZON-CL3-2022-INFRA-01-02: Autonomous systems used for infrastructure protection

Destination CS – Increased Cybersecurity

IA	CS01 - Secure and resilient digital infrastructures and interconnected systems	HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures
RIA	CS02 - Hardware, software and supply chain security	HORIZON-CL3-2022-CS-01-02: Trustworthy methodologies, tools and data security "by design" for dynamic testing of potentially vulnerable, insecure hardware and software components
IA	CS03 - Cybersecurity and disruptive technologies	HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography
IA	CS04 - Smart and quantifiable security assurance and certification shared across Europe	HORIZON-CL3-2022-CS-01-04: Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes

Destination SSRI - Strengthened Security Research and Innovation

CSA	SSRI 01 - Stronger pillars of security Research and Innovation	HORIZON-CL3-2022-SSRI-01-01: Increased foresight capacity for securit
CSA		HORIZON-CL3-2022-SSRI-01-02: Knowledge Networks for security Research & Innovation
CSA	SSRI 02 - Increased Innovation uptake	HORIZON-CL3-2022-SSRI-01-03: Stronger grounds for pre-commercial procurement of innovative security technologies
RIA	SSRI 03 - Cross-cutting knowledge and value for common security solutions	HORIZON-CL3-2022-SSRI-01-04: Social innovations as enablers of security solutions and increased security perception

Mode d'emploi de lecture de notre guide

Synergies avec les autres Clusters

Synergies – CL2

1 projet 5 M€ | RIA | TRL 4-5 ?

Code de l'appel et **titre** (avec lien hypertexte vers sa page officielle de publication sur le portail "Funding & tenders")

L3-2022-INFRA-01-01 : Nature-Based pr

Nombre de projet financés sur ce Sujet,
Budget par projet
Instrument de financement
TRL attendus en fin de projet

THÉMATIQUES
Ville intelligente résiliente et sûres

CONSORTIUM

A minima, 2 autorités publics régionales ou locales de 2 Etats membres de l'UE ou pays associés différents.

La coopération internationale avec des pays pionniers dans le développement de NBS est conseillée.

AUTRES DISCIPLINES
Impact climatique

TOPICS

SU-INFRA02-2019; CIP-2017; DRS-13-2015

Synthèse des **Thématiques et disciplines, Structure de Consortium** et **Référence de projets passés**

Etendre la connaissance sur les « Solutions basées nature » (NBS) et leur capacité à améliorer la résilience des infrastructures dans les villes contre les risques divers

RÉSULTATS ATTENDUS / certains ou tous parmi

- Apport des Solutions « Biomimétiques » en complément des méthodes existantes pour la protection et résilience des infrastructures
- Stratégies d'**adaptation de la protection des infrastru**
  systèmes naturels
- Résilience basée sur les **connaissances locales, histo**
  naturels.
- **Nouveaux matériaux de construction** plus durables e

Synthèse du sujet
Synthèse des "expected outcome"
Synthèse des Points Importants

POINTS IMPORTANTS

Forte implication des Citoyens/ Société civile avec les autorités publiques, les PMEs et les Académiques.

éveloppées en situation réelles par les autorités locales

e Galileo/EGNOS et Copernicus et de données sensible / classifiées

MINISTÈRE
DE L'ENSEIGNEMENT
SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Liberté
Égalité
Fraternité

horizon europe

Resilient Infrastructure

RI 2022

- 2 appels / 2 lauréats, 11 M€
- 1 RIA, 1 IA
- 1 AAP Coopération internationale

Cluster 3 will support in particular the following two Horizon Europe key strategic orientations and impact areas associated to them[24]

KEY STRATEGIC ORIENTATIONS FOR R&I	KSO A: Promoting an open strategic autonomy by leading the development of key digital, enabling and emerging technologies, sectors and value chains	KSO D: Creating a more resilient, inclusive and democratic European society
IMPACT AREAS	Competitive and secure data-economy Secure and cybersecure digital technology	A resilient EU prepared for emerging threats A secure, open and democratic EU society
EXPECTED IMPACTS	**14.** Increased cybersecurity and a more secure online environment	**11.** Enhanced disaster risk reduction **12.** Improved air/land/sea border management & maritime security **13.** Tackling crime and terrorism, and threats to infrastructures

Les défis

- Assurer la **résilience des grandes infrastructures interconnectées et assurer les fonctions sociétales vitales face** à tous types d'attaques complexes, pandémies…
- **Meilleurs systèmes de protection** pour des infrastructures Européennes résilientes et autonomes
- **Transférer les savoirs acquis dans la protection des infrastructures complexes** pour des villes intelligentes plus sûres et **résilientes**

Impacts attendus de la Destination INFRA

- une **prévention**, une **préparation** et une **réponse** plus puissantes,
- une meilleure compréhension des **aspects humains, sociétaux** et **technologiques connexes**,
- le développement de **capacités de pointe** pour les opérateurs d'infrastructures

HORIZON-CL3-2022-INFRA-01-01 : Nature-Based Solutions integrated to protect local infrastructure

THÉMATIQUES
Ville intelligente résiliente et sûres

CONSORTIUM
A minima, 2 autorités publics régionales ou locales de 2 Etats membres de l'UE ou pays associés différents.

La **coopération internationale avec des pays pionniers dans le développement de NBS** est conseillée.

AUTRES DISCIPLINES
Impact climatique

TOPICS
SU-INFRA02-2019; CIP-01-2016-2017; DRS-13-2015 ;H2020-SC5-2019-2

Etendre la connaissance sur les « Solutions Basées Nature » (NBS) et leur capacité à améliorer la résilience des infrastructures dans les villes contre les risques divers

RÉSULTATS ATTENDUS / certains ou tous parmi

- Apport des Solutions « Biomimétiques » en complément des méthodes existantes pour la protection et résilience des infrastructures
- Stratégies d'**adaptation de la protection des infrastructures** basée sur l'exemple des **éco-systèmes naturels**
- Résilience basée sur les **connaissances locales, historiques** et supportées par des moyens naturels.
- **Nouveaux matériaux de construction** plus durables et résistants

POINTS IMPORTANTS

Forte implication des Citoyens/Société civile avec les autorités publiques, les PMEs et les Académiques.
Test des solutions développées en situation réelles par les autorités locales

Utilisation possible de Galileo/EGNOS et Copernicus et de données sensible / classifiées

HORIZON-CL3-2022-INFRA-01-02 : Autonomous systems used for infrastructure protection

THÉMATIQUES
Villes intelligentes Sûres et Résilientes

CONSORTIUM
A minima, 2 opérateurs d'infrastructure critique de 2 Etats membres de l'UE ou pays associés différents.

AUTRES DISCIPLINES
Robotique avancée et AI, réparation autonome

TOPICS
ICT-25-2016-2017; DS-3-2015; DS-7-2015; SU-INFRA01-2018-2019-2020; DRS-15-2015

Utilisation de systèmes autonomes pour la protection des infrastructures

RÉSULTATS ATTENDUS / certains ou tous parmi

- Surveillance, detection et réponse rapide et coordonnées autonomes basée sur des plans de continuité intégrés à jour, face aux menaces pour différentes infrastructures en **situation dégradées.**
- **Solutions autonomes déployées dans la durée / permanentes** pour la **détection** et la **décontamination CBRN** ou la réponse aux **pandémies** pour les grandes infrastructures.
- **Analyse systémique** et Concepts pour **réduire les destructions potentielles** des infrastructures
- Protection et réponses contre les **attaques d'objets volants rapides**
- Impact légal et éthique de l'utilisation de robots pour assurer les fonctions vitales de la société

POINTS IMPORTANTS

Solutions autonomes, sécurisés et **éthiques et respectueuses de la vie privée**, **zones contaminées** NRBC, **zones inaccessibles**

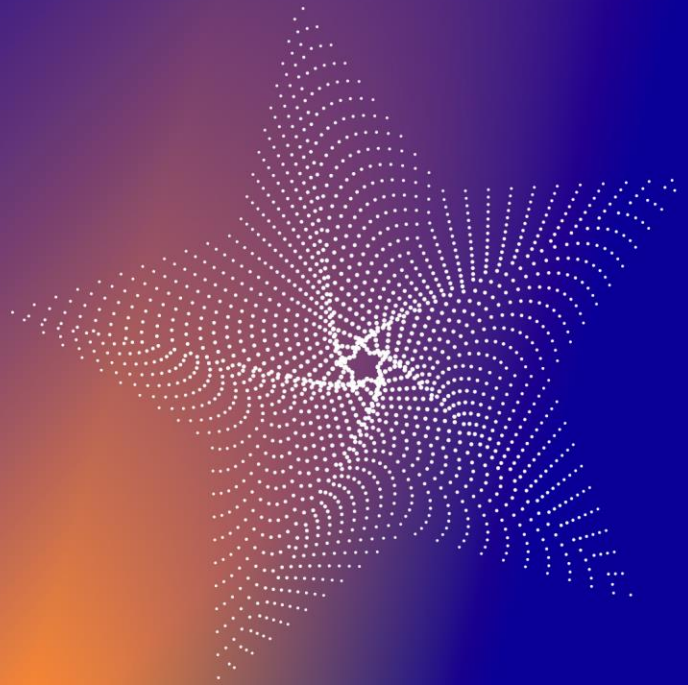
Prendre en compte les **attaques intentionnelles** plutôt que les accidents et défaillances.

Utilisation possible de Galileo/EGNOS et Copernicus et de données sensible / classifiées

MINISTÈRE
DE L'ENSEIGNEMENT
SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

horizon europe

Increased Cybersecurity



IC 2022

- 4 appels / 14 lauréats, 67,3 M€
- 1 RIA, 3 IA
- 0 AAP Coopération internationale

Cluster 3 will support in particular the following two Horizon Europe key strategic orientations and impact areas associated to them[24]

KEY STRATEGIC ORIENTATIONS FOR R&I	KSO A: Promoting an open strategic autonomy by leading the development of key digital, enabling and emerging technologies, sectors and value chains	KSO D: Creating a more resilient, inclusive and democratic European society
IMPACT AREAS	Competitive and secure data-economy Secure and cybersecure digital technology	A resilient EU prepared for emerging threats A secure, open and democratic EU society
EXPECTED IMPACTS	**14.** Increased cybersecurity and a more secure online environment	**11.** Enhanced disaster risk reduction **12.** Improved air/land/sea border management & maritime security **13.** Tackling crime and terrorism, and threats to infrastructures

Les défis

- L'Europe doit **renforcer sa résilience aux cyberattaques** et créer une **"cyber dissuasion" efficace,** tout en veillant à ce que
- la **protection des données** et **la liberté des citoyens soient renforcées** (préservation de la **vie privée,** de la **sécurité,** de la **sûreté** et des **normes éthiques)**

Impact attendu de la Destination CS

- Cybersécurité accrue et environnement en ligne plus sûr soutenant la **protection des données et des réseaux**, **dans le respect de la vie privée** et des autres droits fondamentaux ;
- **Sécurisation** des **services**, des **processus** et des **produits**,
- **Infrastructures numériques robustes** capables de résister et de contrer les cyberattaques et les menaces hybrides.

HORIZON-CL3-2022-CS-01-01 : Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures

THÉMATIQUES
Infrastructures digitales – systèmes interconnectés

CONSORTIUM
A minima, 3 organisations ou agences de premiers secours d'au moins 3 États membres de l'UE ou pays associés différents. Peut impliquer des Informations sensibles et classifiées. Encourager la participation des PME

AUTRES DISCIPLINES
Digital infrastructures

TOPICS
H2020_SU-DS01-2018; SU-DS04-2018-2020; SU-DS05-2018-2019 et SU-TDS-02-2018

La disponibilité des infrastructures IT, leurs performances contrôlées et leurs fiabilités doivent être garanties à tout moment pour répondre aux besoins, parfois critiques et liés à la sécurité.

RÉSULTATS ATTENDUS / au moins 3 ou tous parmi
- **Meilleure préparation et resilience** face à l'arrêt des infrastructure numérique en Europe
- **Meilleures capacités organisationnelles et opérationnelles** pour la sécurité des infrastructures digitales
- **Preuves solides utilisées dans les décisions** et les outils de cybersécurité
- **Meilleure prévision des menaces** de cybersécurité et des risques associés
- Capacités de réponse améliorées sur la base d'une **collaboration et/ou d'une coordination efficaces avec d'autres organismes nationaux ou européens** en charge de la cybersécurité, y compris la notification globale des incidents et la **possibilité d'une réponse coordonnée** aux cyberincidents

POINTS IMPORTANTS

Support financier à des tierces parties jusqu'à 20% du financement EU de l'action.

Démontrer la reproductibilité des solutions.

Synergie avec le Framework de certification de la cybersécurité de l'UE, tel qu'établi par EU Cybersecurity Act

HORIZON-CL3-2022-CS-01-02 : Trustworthy methodologies, tools and data security "by design" for dynamic testing of potentially vulnerable, insecure hardware and software components

THÉMATIQUES
Sécurité logicielle, matérielle et de la logistique

CONSORTIUM
Non défini

AUTRES DISCIPLINES
Peut impliquer l'utilisation d'informations classifiées et/ou la production de résultats sensibles en matière de sécurité.
Participation des PME encouragée.

TOPICS
DS-06-2017

Définir les méthodes et tester la sécurité des systèmes logiciels, matériels et logistiques

RÉSULTATS ATTENDUS / certains ou tous parmi
- Framework Logiciel et Matériel sécurisé global incluant méthodes, procédures d'audit, environnement de codage, données, l'intégration, les tests et vérifications, la certification, les contrôles d'accès, la mise à jour …
- Développer des outils hybrides, agiles et à haute assurance

POINTS IMPORTANTS
Synergie avec le Framework de certification de la cybersécurité de l'UE, tel qu'établi par EU Cybersecurity Act.

HORIZON-CL3-2022-CS-01-03 : Transition towards Quantum-Resistant Cryptography

THÉMATIQUES
Cryptographie, Ordinateurs quantiques, technologies de rupture

CONSORTIUM Proposition incluant **seulement des entités des Etats membres et Pays associés**. Peut impliquer l'utilisation d'informations classifiées et la production de résultats sensibles en matière de sécurité. Participation des PME encouragée.

AUTRES DISCIPLINES
Mathematics, Physics, electrical engineering

TOPICS
H2020 SU-ICT-03-2018; ICT-32-2014 PQCRYPTO

Garantir une Cybersécurité Post Quantique (Cybersecurity and disruptive technologies) par une cryptographie résistante aux quantums

RÉSULTATS ATTENDUS / au moins 3 parmi

- Mesurer, évaluer et standardiser/certifier une **cryptographie à l'épreuve du temps**
- Combler les écarts entre les possibilités théoriques offertes par la cryptographie résistante quantique et ses i**mplémentations pratiques**
- Solutions et méthodes qui pourraient être utilisées pour **migrer de la cryptographie actuelle vers une cryptographie évolutive**
- Préparation à l'échange et au traitement sécurisés des informations en **cas d'attaques quantiques à grande échelle**

POINTS IMPORTANTS

Démonstrateurs pilotes dans des cas d'utilisation pertinents (migrations…)

Support financier à des tierces parties jusqu'à 20% du financement EU de l'action: 300 k€ par partie.

S'appuyer sur projets H2020 projects, NIST Post-Quantum Cryptography competition, ETSI, projet H2020 OpenQKD, EuroQCI.

HORIZON-CL3-2022-CS-01-04 : Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes

THÉMATIQUES
CyberSécurité, certification

CONSORTIUM
Peut impliquer l'utilisation d'informations classifiées et/ou la production de résultats sensibles en matière de sécurité.

AUTRES DISCIPLINES
Partage de données sécurisé, infrastructures de test

TOPICS
H2020-EU.1.3.3

Assurance et certification de sécurité intelligentes et quantifiables partagées dans toute l'Europe

RÉSULTATS ATTENDUS / au moins 3 parmi

- Disponibilité des outils et procédures applicables pour l'**évaluation partielle et continue et la re-certification Lean** des produits, services et processus TIC
- **Réduction du temps et des efforts pour la (re-)certification** des produits, services et processus TIC
- Amélioration de la **collaboration** (fabricants, utilisateurs finaux, Etats membres...) **sur les informations de certification** de cybersécurité
- **(ré)utilisation efficace des informations** et des preuves pertinentes pour la certification et la (ré)utilisation multi-programmes
- **Intégration de la certification** sur l'ensemble du processus de modélisation, test et vérification du système
- **Comparabilité accrue des déclarations d'assurance** des programmes de certification et des normes
- **Faire progresser les installations de test et de simulation**, l'analyse des incidents et des menaces ;
- Augmentation des capacités de **Digital Twin pour l'évaluation continue et l'intégration de nouvelles solutions**.

POINTS IMPORTANTS

Synergie avec le Framework de certification de la cybersécurité de l'UE, tel qu'établi par EU Cybersecurity Act.

Aligné sur les objectifs du Centre de compétences en cybersécurité et du Réseau des centres nationaux de coordination

Les résultats peuvent alimenter le travail opérationnel sur la préparation et la réponse au sein de l'unité conjointe Cyber

MINISTÈRE
DE L'ENSEIGNEMENT
SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Liberté
Égalité
Fraternité

horizon
europe

SSRI : Strengthened Security Research and Innovation

SSRI 2022

- 4 appels / 6 lauréats, 9,5 M€
- 1 RIA, 3 CSA
- 0 AAP Coopération internationale
- 4 AAP SHS attendu

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-CL3-2022-SSRI-01-01 : Increased foresight capacity for security

THÉMATIQUES
Prospective

CONSORTIUM Peut impliquer l'utilisation d'informations classifiées et la production de résultats sensibles en matière de sécurité.

AUTRES DISCIPLINES
SSH

TOPICS

SU-INFRA02-2019, SU-FCT03-2018-2019-2020

Des piliers renforcés de Recherche et Innovation en Sécurité - Anticiper le Futur

RÉSULTATS ATTENDUS / tous

- **Pilotage anticipé de l'évolution prévisible des technologies liées à la sécurité** et des défis et opportunités apportés par une telle évolution sur l'industrialisation et l'utilisation des futures technologies de sécurité
- Un **cadre de prospective commun pour la sécurité civile de l'UE** avec un modèle scientifique solide qui relie les technologies futures à leur utilisation future. Approche qualitative et quantitative plus accessible aux acteurs de la sécurité
- **Approche de Research-as-a-Service** pour le programme de prospective stratégique de la Commission européenne

POINTS IMPORTANTS

Se coordonner avec le CERIS, Frontex. **Approches prospectives existantes** du JRC, EDA, INTERPOL, UNIDO, etc… Réseaux de praticiens financés dans le cadre de H2020 Secure Societies et Knowledge Networks for Security Research & Innovation financés dans le cadre d'Horizon Europe Cluster 3.

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATION
Liberté
Égalité
Fraternité

horizon europe

Synergies – CL2

2 projets 2 M€ | CSA | TRL -

HORIZON-CL3-2022-SSRI-01-02 : Knowledge Networks for security Research & Innovation

THÉMATIQUES Réseaux de connaissances

CONSORTIUM A minima autorités d'au moins 3 États membres de l'UE ou pays associés différents. Résultats Sensibles. Obligation de dissémination et participation à des WG EU. Soit Option A **(DRS)** soit Option B (**FCT**)

AUTRES DISCIPLINES
Effective contribution of SSH

TOPICS
Tous les projets Sécurité passés

Réseaux de connaissances qui collectent, agrègent, traitent, disséminent et exploitent les connaissances existantes pour mieux programmer la Recherche & Innovation en Sécurité

RÉSULTATS ATTENDUS / tous

- **Soutenir la programmation de la recherche sur la sécurité financée par l'UE** et des fonds de renforcement des capacités grâce à un retour d'information périodique et opportun sur les politiques fondées sur des preuves ;
- **Vue périodiquement agrégée et consolidée** des besoins et des lacunes en matière de capacités dans les domaines thématiques considérés, des technologies, techniques, méthodes et outils de pointe qui peuvent contribuer à combler les lacunes identifiées en matière de capacités, des résultats, les tendances futures, les leçons apprises et les meilleures pratiques dérivées des efforts de recherche passés et actuels en matière de sécurité engagés dans les domaines thématiques considérés.
- Évaluation et validation plus systématiques des résultats des projets de recherche sur la sécurité financés par l'UE en ce qui concerne les lacunes identifiées en matière de capacités grâce à des mécanismes de soutien harmonisés ;
- Carte commune et mise à jour des **opportunités et des contraintes pour l'exploitation des projets** de R&I en matière de sécurité de l'UE,
- Carte commune et mise à jour des domaines nécessitant des **solutions standardisées** et/ou des **programmes de certification** pour favoriser l'adoption de l'innovation et la création de marchés, ainsi que des formations et des options pour la mise en œuvre de tels programmes.
- **Coopération renforcée entre les différents acteurs** pour soutenir une participation intégrée dans la détermination et l'analyse des exigences, la recherche et la validation et l'évaluation des résultats.

POINTS IMPORTANTS

Support financier à des tierces parties (prix jusqu'à 60 k€ par partie) pour un total d'au moins 25% du budget du projet.
Accès à toutes les informations générées dans le cadre des programmes de R&I sur la sécurité financés par l'UE et au-delà.
Assure la diffusion et exploitation des résultats et contribution aux **Union Civil Protection Knowledge Network**, **CERIS**, **EUROPOL**

HORIZON-CL3-2022-SSRI-01-03 : Stronger grounds for pre-commercial procurement of innovative security technologies

THÉMATIQUES PCP

CONSORTIUM A minima, 6 utilisateurs et 3 autorités de procurement public d'au moins 3 États membres de l'UE ou pays associés différents. Résultats sensibles. Max 1 year

AUTRES DISCIPLINES
SSH

TOPICS

Augmentation de l'adoption de l'innovation via une action préparatoire pour l'action d'approvisionnement pré-commerciale par des utilisateurs et acheteurs publics de plusieurs pays

RÉSULTATS ATTENDUS / tous

- Une demande consolidée de technologies de sécurité innovantes construites 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 en matière d'investissement dans des technologies de sécurité innovantes basée sur une **meilleure compréhension de l'offre potentielle d'alternatives techniques basées dans l'UE** qui pourraient répondre aux besoins communs des acheteurs publics de l'UE ;
- Une prise de décision mieux informée en matière d'investissement dans des technologies de sécurité innovantes basée sur 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 les exigences sur l'industrie et les produits futurs** et à attirer l'innovation et les innovateurs des secteurs de la sécurité et d'autres par le biais de stratégies de validation communes, d'innovation rapide, d'expérimentation et d'achats avant commercialisation.
- Capacité d'innovation accrue des acheteurs publics de l'UE grâce à la **disponibilité d'orientations innovantes pour les appels d'offres**, de **stratégies de validation convenues d'un commun accord** et de perspectives fondées sur des preuves de **nouveaux achats conjoints de solutions de sécurité communes**.

POINTS IMPORTANTS

Soumettre une proposition à un appel ouvert pour une action PCP de suivi dans le cluster 3 2023-24
Consultations d'open market durant le projet dans au moins 3 États membres ou pays associés différents
Mesures visant à réduire les obstacles aux start-ups de haute technologie et aux PME innovantes

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE ET DE L'INNOVATION
Liberté
Égalité
Fraternité

horizon europe

Synergies – CL2

1 projet 2 M€ | RIA | TRL 4

HORIZON-CL3-2022-SSRI-01-04 : Social innovations as enablers of security solutions and increased security perception

THÉMATIQUES
Sécurité et Société

CONSORTIUM
Peut impliquer l'utilisation d'informations classifiées et/ou la production de résultats sensibles en matière de sécurité. Max 4 ans

AUTRES DISCIPLINES
SHS effectif, Multidisciplinaire

TOPICS
H2020-Adhoc-2014-20

Connaissances transversales et valeurs pour des solutions de sécurité communes avec l'implication et la co-création des citoyens et des communautés locales

RÉSULTATS ATTENDUS / certains ou tous parmi

- Les décideurs politiques, les praticiens de la sécurité et les chercheurs ont une **meilleure compréhension des capacités des communautés locales et des citoyens** à contribuer au développement de solutions de sécurité ;
- Les décideurs politiques, les chercheurs et les développeurs de systèmes orientent davantage le développement de solutions de sécurité vers des **approches de R&I socialement innovantes et responsables** ;
- Les notions de « **citoyens intelligents** » et de « **communautés locales intelligentes** » portées par la Recherche et l'Innovation responsables et l'innovation sociale, où le grand public co-contrôle la sûreté et la sécurité de son environnement, sont plus largement adoptées par les décideurs ;
- De **nouvelles références, normes ou autres critères de qualité** sont établis pour développer des solutions de sécurité grâce à la **recherche et l'innovation responsables**
- Une **collaboration accrue entre toutes les parties** (universités/recherche, pouvoirs publics, industrie/PME, société civile/citoyens/communautés locales) pour développer des **innovations conformes aux besoins, valeurs et attentes de la société** ;
- Des solutions technologiques innovantes, transférables et potentiellement évolutives **co-créées avec les citoyens et les communautés locales** dans les laboratoires sociaux et les centres de vie de l'innovation, et les citoyens habilités à agir en tant que générateurs, validateurs et utilisateurs finaux des nouvelles technologies horizontales ;
- **Confiance de la société dans les produits de recherche en sécurité**, leur utilité souhaitée et leur acceptabilité sociale

POINTS IMPORTANTS
Soutien financier à des tierces parties sous forme de prix (max 60 k€).
Synergies avec d'autres programmes comme : le **Civil Society Empowerment Program** (CSEP-ISF), **Science with and for Society** (SwafS), le **Digital Europe Program**

MINISTÈRE
DE L'ENSEIGNEMENT
SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Liberté
Égalité
Fraternité

horizon europe

Témoignage de Noémi THOMAZO ARIADNEXT

Webinaires 2022 du Cluster 3

- 27 janvier 10h-11h30 : Disaster-Resilient Society (DRS)
- 2 février 10h-11h30 : Fighting Crime and Terrorism (FCT) et Border Management (BM)
- 4 février 10h-11h30 : Increased Cybersecurity (IC), Resilient Infrastructure (RI) et Support Security and Research Innovation (SSRI)

https://www.horizon-europe.gouv.fr/webinaires-securite-pour-la-societe-civile-29098

Pitch sessions 2022 du Cluster 3

- 10 mars 14h-15h30 : DRS
- 17 mars 10h-11h30 : FCT et BM
- 23 mars : 10h-11h30 : IC, RI et SSRI

Présidence française du conseil de l'Union européenne – Premier semestre 2022:

- ✓ Security research event : les 1er et 2 mars 2022
  - ✓ Cité des Sciences et de l'industrie
  - ✓ Conférence de haut niveau (ministres, commissaires, PDG)
  - ✓ Stands de projets, démonstrations
  - ✓ Capacité 900 personnes : un lieu pour rencontrer des partenaires

Conférence et panels

- ✓ L'impact de la numérisation de la société sur la sécurité Cité des Sciences et de l'industrie
- ✓ Aspects sociétaux d'une situation de crise
- ✓ Capacités de sécurité critiques et technologies critiques pour l'UE
- ✓ La résilience des infrastructures européennes

https://www.sre2022.eu/