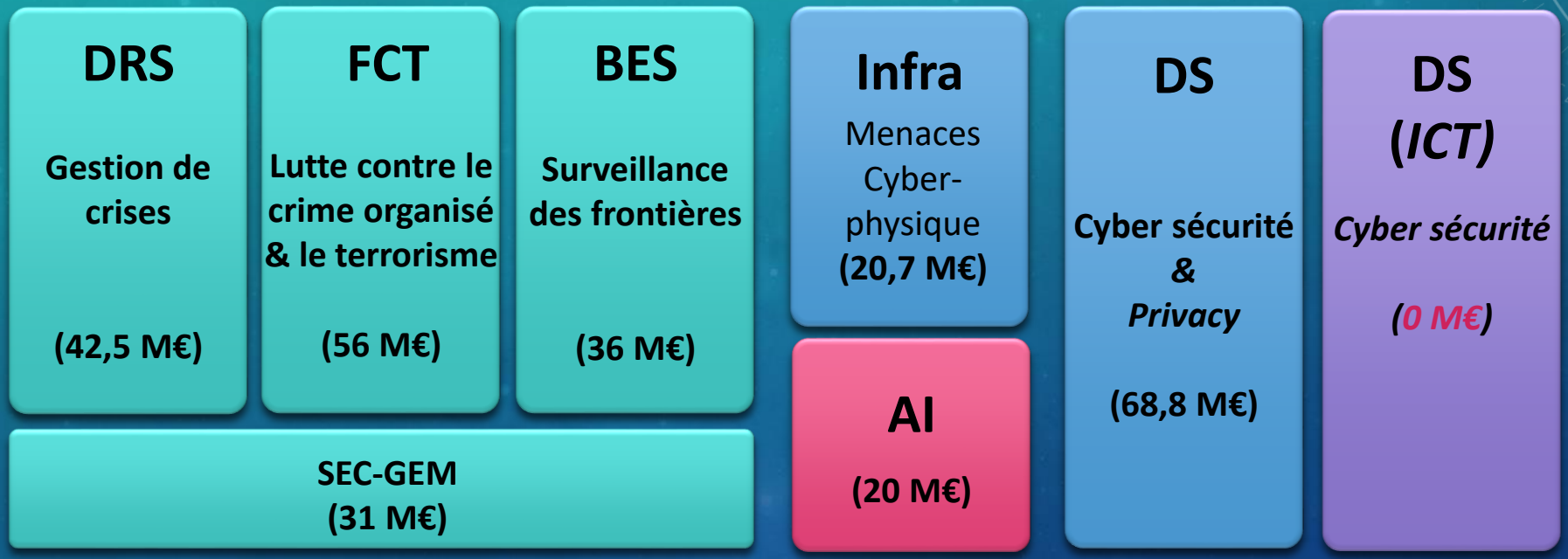
HORIZON2020 - DÉFI SÉCURITÉ
APPELS : 2020

ARMAND NACHEF – PCN SÉCURITÉ – CEA

Sécurité
PCN - Horizon2020

BUDGET DU DÉFI SÉCURITÉ EN 2020



LES TOPICS DES APPELS 2020 DU DÉFI SÉCURITÉ

SU-INFRA

Prévention, détection, réponse et atténuation des menaces physiques et des cyber menaces sur les infrastructures critiques
INFRA01 **(IA)**

SU-AI

Développement d'une feuille de route de R&I en IA pour le maintien de l'ordre
AI01-2020 **(CSA)**

Technologies, outils et solutions d'IA pour les LEA
AI02-2020 **(IA)**

Facteurs humains et aspects éthiques, sociétaux, juridiques et organisationnels de l'utilisation de l'IA en soutien des LEA
AI03-2020 **(CSA)**

SU-FCT

FCT Human factors
- fight human beings trafficking and child sexual exploitation
- counter violent radicalisation
- **NO** open subtopic

FCT01 **(RIA)**

FCT Technologies
- Money flows tracking
- Identify terrorist content online
- Open subtopic

FCT02 **(RIA)**

Information and data stream mgt to secure *soft targets*
FCT03 **(IA)**

Chemicals: intelligence, detection, forensics
explosives, neurotoxins, new drugs, etc.
FCT04 **(IA)**

SU-DRS

DRS Human factors
DRS01**(RIA)**

Technologies for first responders:
- Methods and guidelines for pre-hospital life support and triage
- Open subtopic

DRS02 **(RIA)**

Pre-normative R&Demo for DRS
- First aids vehicles deployment, maintenance, and remote centralized coordination means

DRS03 **(IA)**

CBRN cluster
DRS04 **(RIA)**

SU-BES

BES Human factors
- indicators of threats at the EU external borders
- **NO** open subtopic

BES01 **(RIA)**

Technologies for BES
- Disruptive technologies for non-intrusive identification of hidden goods
- Open subtopic

BES02 **(RIA)**

Demo of applied solutions
- Improved systems for the vessel tracking
- Open subtopic

BES03 **(IA)**

SU-GM

Networks of practitioners:
- intelligence
- fighting cybercrime

GM01 **(CSA)**

PCP of advanced Systems
GM02 **(PCP)**

SU-DS

Intelligent security & privacy mgt
- Dynamic governance, risk mgt & compliance
- Cyber-threat information sharing and analytics
- solutions for users or soft developers
- Distributed trust mgt and digital identity solutions

DS02 **(IA)**

Cyber security & privacy for Micro-SMEs and citizens
DS03 **(IA)**

Cybersecurity in the Electrical Power and Energy System (EPES)
DS04 **(IA)**

http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf

SU-DS

Digital Security

Cybersecurity and Digital Privacy

SU-DS : 2020

Année	Topic (Type d'Action)	Titre	Budget (M€)	Date limite
2020	SU-DS02-2020 (3 IA et 1 RIA)	Gestion intelligente de la sécurité et de la confidentialité	IA : 18,00 RIA : 20,00	27 août 2020
	SU-DS03-2019-2020 (IA)	Sécurité numérique et protection de la vie privée pour les citoyens et les petites et moyennes entreprises et les micro-entreprises	10,80	
	SU-DS04-2018-2020 (IA)	La cybersécurité dans le système d'énergie et d'alimentation électrique (EPES) : une protection contre les cyberattaques et les atteintes à la vie privée et la violation de données	20,00	

SU-DS02-2020

GESTION INTELLIGENTE DE LA SÉCURITÉ ET DE LA CONFIDENTIALITÉ - LE DÉFI

Date limite : le 27 août 2020

Budget total : 38 M€

Présence de PME encouragée

Le défi

- Approches avancées, holistiques et dynamiques de la cyber sécurité et de la confidentialité.

- Prévoir, surveiller et mettre à jour constamment les systèmes de sécurité :
  - Automatisation, Intelligence artificielle

- Risque d'effets multiformes et en cascade sur les infrastructures TIC interconnectées et complexes -> gestion transparente

SU-DS02-2020

GESTION INTELLIGENTE DE LA SÉCURITÉ ET DE LA CONFIDENTIALITÉ - SCOPE

- Conception, le développement et tests : systèmes IA de gestion de la sécurité et de la protection de la vie privée automatisés, détection d'attaques IA avec auto-réparation, outils de modélisation et de simulation immersifs, gestion de la confiance, identités et accès, sûrs et temps-réel

- Inclure des solutions de formation pratique , interactive et de pointe, comme des exercices de cybersécurité

- Collaboration avec les projets-pilotes et d'autres projets H2020 réalisés

SPARTA

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

ECHO

Cyber Security for Europe

SU-DS02-2020

GESTION INTELLIGENTE DE LA SÉCURITÉ ET DE LA CONFIDENTIALITÉ - LES SOUS TOPICS

4 sous-topics:

1. **Sous-topic a)**
   Gouvernance dynamique, gestion des risques et conformité
   - **Innovation Action (IA) TRL 7 Budget par projet 2 à 5 M€**
2. **Sous-topic b)**
   Partage et analyse des informations sur les cybermenaces
   - **Innovation Action (IA) TRL 7 Budget par projet 2 à 5 M€**
3. **Sous-topic c)**
   Solutions avancées de sécurité et de confidentialité pour les utilisateurs finaux ou les développeurs de logiciels
   - **Research and Innovation Action (RIA) TRL 6 Budget par projet 2 à 5 M€**
4. **Sous-topic d)**
   Solutions distribuées de gestion de confiance et d'identité numérique
   - **Research and Innovation Action (RIA) TRL 5 à 6 Budget par projet 3 à 6 M€**

SU-DS02-2020

GESTION INTELLIGENTE DE LA SÉCURITÉ ET DE LA CONFIDENTIALITÉ

SOUS-TOPIC A) GOUVERNANCE DYNAMIQUE, GESTION DES RISQUES ET CONFORMITÉ (IA)

- nouvelles approches automatisées, dynamiques et adaptatives d'identification des attaques, y compris les " zero-day "

- pilotes à grande échelle -- démontrer la solution sur des applications concrètes
  - prévision,
  - visualisation,
  - surveillance en temps réel et alertes de grande précision,
  - soutien à la prise de décision automatisée
  - adaptation du fonctionnement et récupération autonome après un état défectueux.

- Inclure les aspects techniques, opérationnels, financiers et éthiques de la cybersécurité.

SU-DS02-2020

GESTION INTELLIGENTE DE LA SÉCURITÉ ET DE LA CONFIDENTIALITÉ

SOUS-TOPIC B) PARTAGE ET ANALYSE DES INFORMATIONS SUR LES CYBERMENACES (IA)

- Environnement de de détection des menaces :
  - (i) des dépôts d'informations collaboratifs, ouverts et dynamiques sur les menaces et les vulnérabilités
  - (ii) s'appuyer sur les ontologies, taxonomies et modèles existants et les mettre à jour
  - (iii) des outils dynamiques de détection automatisée dotés de capacités analytiques avancées et, si possible, d'intervention et de récupération
  - (iv) des techniques de responsabilisation et de vérification
  - (v) des systèmes synchronisés en temps réel de décryptage/autodéchange en continu avec capacité de récupération
- proposer de nouvelles technologies permettant de collaborer dans le domaine du renseignement et de l'alerte
- Tenir compte des aspects techniques et humains tels que les comportements, les différences entre les sexes, la vie privée, l'éthique, la souveraineté, la psychologie, les frontières linguistiques et culturelles.
- Les outils et services qui seront mis au point devraient être en mesure d'appuyer les opérations des CERT/CSIRT et des réseaux de CERT/CSIRT.

* CERT : Computer emergency response team ⟺ CSIRT : computer security incident response team

est un groupe d'experts qui traite et centralise les incidents de sécurité informatique. Il joue le rôle de centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations.

En France le CERT affecté au secteur de l'administration française est le CERT-FR qui appartient à l'ANSSI

SU-DS02-2020

GESTION INTELLIGENTE DE LA SÉCURITÉ ET DE LA CONFIDENTIALITÉ

SOUS-TOPIC C) SOLUTIONS AVANCÉES DE SÉCURITÉ ET DE CONFIDENTIALITÉ POUR LES UTILISATEURS FINAUX OU LES DÉVELOPPEURS DE LOGICIELS (RIA)

- développer des outils automatisés pour vérifier la sécurité et la confidentialité des données, des systèmes, des services en ligne et des applications, afin d'aider les utilisateurs finaux ou les développeurs de logiciels (y compris éventuellement les développeurs de solutions d'IA) dans leurs efforts pour sélectionner, utiliser et créer des services numériques dignes de confiance.

- Proposer des cas d'application réels et au moins un des services suivants :
  - génération automatique de code,
  - audit de code et de données,
  - boîtes de données fiables,
  - forenics,
  - certification et assurance,
  - cyberassurance,
  - cyberéthique et IA,
  - tests d’intrusion

SU-DS02-2020

GESTION INTELLIGENTE DE LA SÉCURITÉ ET DE LA CONFIDENTIALITÉ

SOUS-TOPIC D) SOLUTIONS DISTRIBUÉES DE GESTION DE CONFIANCE ET D'IDENTITÉ NUMÉRIQUE

En accordant une attention particulière aux contextes de l'Interner des Objets, proposer et tester/piloter des approches novatrices portant sur les deux points suivants :

i. des solutions distribuées, dynamiques et automatisées de gestion de confiance et de récupération ; et

ii. la mise au point de nouvelles approches de gestion de l'identité des personnes et/ou des objets, y compris des systèmes d'auto-encryptage/décryptage avec possibilité de récupération.

Les propositions doivent porter sur des cas réels d'application

SU-DS03-2019-2020 (1/2)

SÉCURITÉ NUMÉRIQUE ET PROTECTION DE LA VIE PRIVÉE POUR LES CITOYENS ET LES PETITES ET MOYENNES ENTREPRISES ET LES MICRO-ENTREPRISES

- **Type of Action** Innovation Action
- **Output TRL** 7

- **Budget per project** 4 à 5 M€ pour sub-topic 1

  3 à 4 M€ pour sub-topic 2

- **Budget total** 10,8 M€ en 2020
- **Deadline** 27 août 2020

- **Challenge**
  - ❑ Pour protéger les données à caractère personnel, les citoyens devraient pouvoir évaluer le risque de cybersécurité et configurer leur propre sécurité, leur vie privée et la protection de leurs données personnelles.
  - ❑ La plupart des PME et des MicroE ne sont pas suffisamment sensibilisées et ne peuvent allouer que des ressources limitées - tant techniques qu'humaines - pour lutter contre les cyber-risques, ce qui fait d'elles une cible plus facile.
  - ❑ Compte tenu du rôle économique important des PME et des ME dans l'UE, une recherche adaptée à l'innovation devrait soutenir leur cybersécurité

SU-DS03-2019-2020 - SCOPE (2/2)

SÉCURITÉ NUMÉRIQUE ET PROTECTION DE LA VIE PRIVÉE POUR LES CITOYENS ET LES PETITES ET MOYENNES ENTREPRISES ET LES MICRO-ENTREPRISES

Sub-topic 1: Protecting citizens' security, privacy and personal data protection

- Apporter des solutions innovantes en matière de protection des données personnelles, aider les citoyens à mieux contrôler et auditer la protection de leurs données personnelles.
- Approches, techniques et outils conviviaux pour :
    1. améliorer la résilience face à la protection de la vie privée
    2. l'identification, la suppression et le signalement des contenus potentiellement préjudiciables
    3. l'exercice du droit des citoyens à l'effacement ("droit d'être oublié")
    4. informer les citoyens sur leur niveau de protection de la vie privée et des données personnelles et leur permettre de moduler à tout moment leurs activités numériques...

Sub-topic 2: Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection

- Développer des solutions ciblées, conviviales et rentables permettant aux PME&ME de :
    a) surveiller, prévoir et évaluer dynamiquement leurs risques en matière de sécurité, de protection de la vie privée et de protection des données personnelles ;
    b) prendre davantage conscience des vulnérabilités, des attaques et des risques qui influencent leurs activités;
    c) gérer et prévoir leurs risques en matière de sécurité, de protection de la vie privée et de protection des données personnelles d'une manière simple/abordable;
    d) établir une collaboration en ligne entre les associations de PME et de ME et avec les CERT/CSIRT, permettant ainsi aux PME et aux ME de signaler tout incident.

SU-DS04-2018-2020

LA CYBERSÉCURITÉ DANS LE SYSTÈME D'ÉNERGIE ET D'ALIMENTATION ÉLECTRIQUE (EPES) : UNE PROTECTION CONTRE LES CYBERATTAQUES ET LES ATTEINTES À LA VIE PRIVÉE ET LA VIOLATION DE DONNÉES

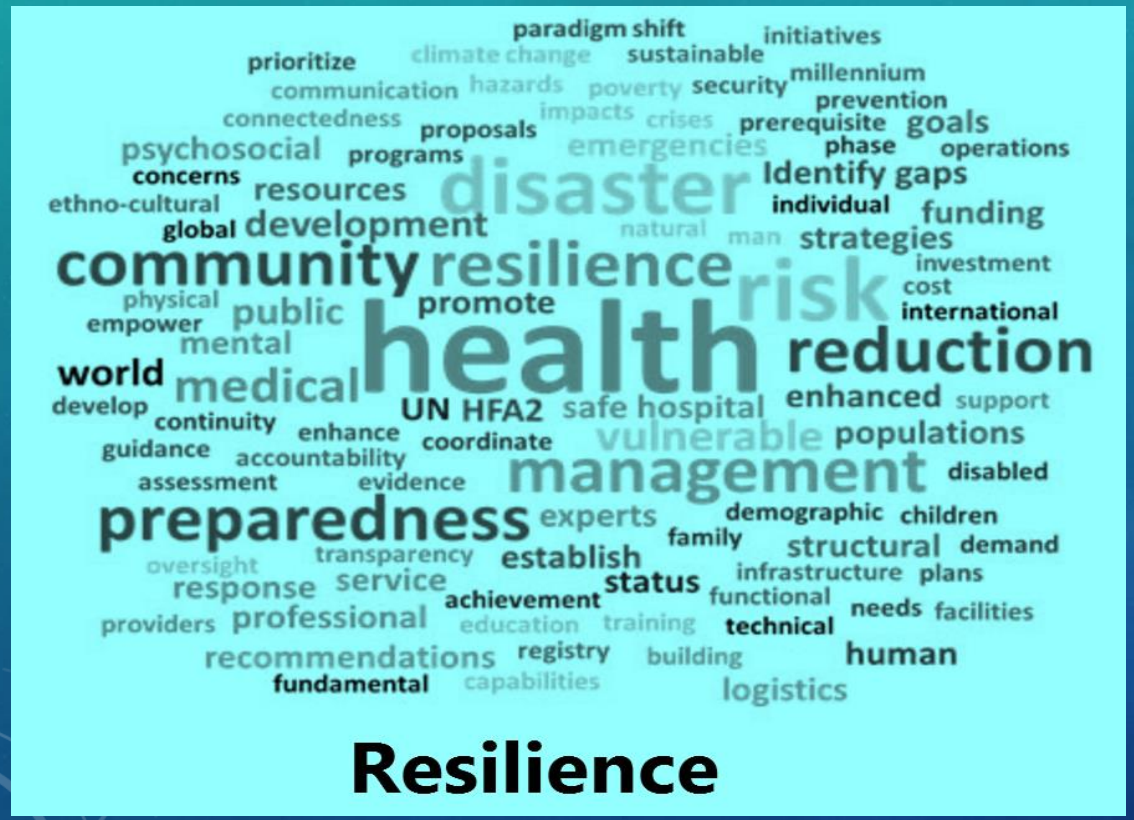
- **Type of Action** Innovation Action
- **Output TRL** 7

- **Budget per project** 6 to 8 M€
- **Total budget** 20 M€ in 2018 ------ 20 M€ in 2020 (Half of the budget is originated from Societal Challenge 3)
- **Deadline** 23 Aug 2018 ------ 27 Aug 2020

- **Challenge**
  - ❑ The Electrical Power and Energy System (EPES) is of key importance to the economy, as all other domains rely on the availability of electricity,
  - ❑ EPES will face an increasing range of threats requiring an attentive evaluation of the cyber security risk
  - ❑ Without appropriate cyber-defence measures, systems access could be violated and may cause power outages, damages and cascading effects to interconnected systems
  - ❑ To pursue the integration of the renewables within the existing EPES and to ensure that it benefits from the advantages brought by a modern digitalised electricity grid, there is a need for new security approaches.

SU-DRS

Disaster-Resilient Societies



SU-DRS : 2020

Année	Topic (Type d'Action)	Titre	Budget (M€)	Date limite
2020	SU-DRS01-2018-2019-2020 (RIA)	Facteurs humains et aspects sociaux, sociétaux et organisationnels des sociétés résilientes aux catastrophes	5,0	27 août 2020
	SU-DRS02-2018-2019-2020 (RIA)	Technologies pour les premiers intervenants	21,0	
	SU-DRS03-2018-2019-2020 (IA)	Recherche et démonstration prénormatives pour des sociétés résilientes aux catastrophes	6,0	
	SU-DRS04-2019-2020 (RIA)	Cluster NRBC	10,5	

SU-DRS01-2018-2019-2020

FACTEURS HUMAINS ET ASPECTS SOCIAUX, SOCIÉTAUX ET ORGANISATIONNELS DES SOCIÉTÉS RÉSILIENTES AUX CATASTROPHES

- **Type of Action** Action de Recherche et d'Innovation (RIA)
- **TRL de sortie** non spécifié
- **Durée du projet** non spécifié
- **Budget par projet** 5 M€
- **Budget total** 5 M€ in 2019
- **Conditions d'éligibilité** Participation d'au moins 3 premiers intervenants de 3 États membres ou pays associés
  La coopération internationale est encouragée (*mais pas obligatoire*)

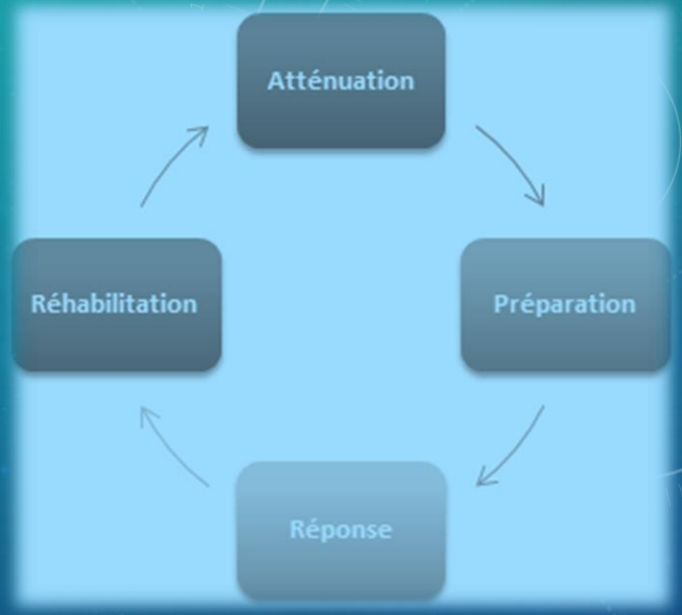
- **Date limite** 27 août 2020

- **Challenge**
  - ❑ La résilience des sociétés dépend fortement de la façon dont leurs citoyens se comportent individuellement ou collectivement.
  - ❑ La diffusion des nouvelles technologies et des nouveaux médias induit des changements spectaculaires dans le comportement des individus et des communautés.
  - ❑ Pour renforcer la résilience, il faut mieux comprendre et mettre en œuvre ces nouvelles technologies afin de sensibiliser davantage les citoyens aux risques de catastrophe, d'améliorer leur compréhension des risques et d'améliorer la gouvernance.

SU-DRS01-2018-2019-2020 - SCOPE

- Etudier tout le cycle de la gestion des catastrophes :
  - la prévention : éducation, sensibilisation aux risques
  - la préparation : savoir comment réagir
  - la gestion des situations d'urgence : communication avant et pendant un événement
  - La réponse : donner aux citoyens les moyens d'agir par eux-mêmes selon des pratiques plus efficaces et en suivant les lignes directrices établies
  - La reprise rapide d'activité

  en tenant compte des changements culturels et de la diversité géographique qui engendrent une diversité dans la perception des risques et dans la compréhension des réponses aux crises



- Tenir compte des médias sociaux et des données provenant de la foule :
  analyser leurs rôles positifs et négatifs
- Évaluer ces pratiques pour différents scénarios de catastrophes :
  risques naturels, catastrophes industrielles, menaces terroristes
- Faire participer les citoyens au test et à la validation du processus de gestion de catastrophes
- Améliorer le processus de reconstruction en tenant compte
  du patrimoine culturel matériel et immatériel, et du savoir-faire traditionnel
- Apprendre des pays qui sont constamment menacés par les catastrophes naturels et où le risque est perçu différemment

SU-DRS02-2018-2019-2020

TECHNOLOGIES POUR LES PREMIERS INTERVENANTS

- **Type d'action** — Action de Rechercher et d'Innovation (RIA)
- **TRL de sortie** — 4 à 6 pour sous-topic open et de 6 à 7 pour sous-topic 3
  Technologies testées et validées, non seulement en laboratoire, mais dans des installations de formation et dans des déploiements expérimentaux in-situ
- **Durée du projet** — non spécifiée
- **Budget par projet** — ~7 M€
- **Budget total** — 21 M€ in 2019

- **Conditions d'éligibilité** — Participation d'au moins 3 premiers intervenants de 3 États membres ou pays associés (ou au moins 5 premiers intervenants pour le sous-topic ouvert)
  Des équipes interdisciplinaires doivent être impliquées
  services d'urgence médicale, autorités de santé publique, forces de l'ordre, ou professionnels de la protection civile
  La coopération internationale est encouragée (ex. Japon ou Corée du Sud) mais pas obligatoire
- **Date limite** — 27 août 2020
- **Challenge** — Besoin de technologies nouvelles pour des sociétés à plus résilientes aux catastrophes

SU-DRS02-2018-2019-2020

SOUS-TOPIC 3 (TRL 6 À 7)

Sous-topic 3: [**2020**] Méthodes et recommandations pour le soin pré-hospitalier des victimes, leur maintien en vie et le triage

- ❑ Assurer une évaluation et un contrôle plus rapides et plus efficaces des blessés graves en cas de grande catastrophe
  - ➢ un triage pré-hospitalier plus efficace des victimes
  - ➢ une traçabilité numérique appropriée des actions
  - ➢ un transfert de données de l'événement aux hôpitaux, y compris au-delà des frontières
- ❑ Développer des outils, des méthodologies et des guides européens innovants pour les premiers intervenants : services médicaux, services d'incendie, équipes de police et équipes de traumatologie hospitalière
- ❑ Apprendre des techniques militaires de médecine de guerre, comme la chirurgie « damage control » qui est mise en œuvre dans un contexte dégradé
  - à l'occasion d'une catastrophe (naturelle, industrielle, ferroviaire, aérienne, carambolage, une tuerie de masse ou un attentat)
  - afflux massif de victimes
  - moyens insuffisants pour prendre en charge le patient de manière complète

SU-DRS02-2018-2019-2020

SOUS-TOPIC OPEN

Améliorer la protection des premiers intervenants contre des dangers multiples et inattendus
ou
Renforcer leurs capacités en abordant les questions de recherche et d'innovation connexes :

- Sous-topic : [2018-2019-**2020**] Open - **Toute technologie à l'usage des premiers intervenants comme** :
  - des vêtements communicants et intelligents pour les premiers intervenants et les unités canines et des sources d'énergie légères
  - des systèmes de connaissance de la situation et d'atténuation des risques utilisant
    - des drones et des robots, connectés et en essaim
    - des systèmes basés sur l'Internet des objets
    - des solutions basées sur la réalité virtuelle ou augmentée
    - des systèmes de communication entre premiers intervenants et victimes
    - des technologies pour l'anticipation des risques et l'alerte précoce
    - des technologies pour atténuer les dégâts, pour combattre physiquement ou pour neutraliser les attaquants etc.

SU-DRS03-2018-2019-2020

RECHERCHE ET DÉMONSTRATION PRÉNORMATIVES POUR DES SOCIÉTÉS RÉSILIENTES AUX CATASTROPHES

- **Type d'action** Action d'Innovation (IA)
- **TRL de sortie** 6 à 7
- **Durée du projet** non spécifié

- **Budget par projet** 6M€
- **Budget total** 6 M€ in 2019

- **Conditions** d'éligibilité Participation d'au moins 3 premiers intervenants de 3 États membres ou pays associés
- **Date limite** 27 août 2020
- **Challenge**
  - ❑ L'interaction difficile entre les praticiens et le faible niveau d'interopérabilité des équipements et des procédures mis en œuvre par les premiers intervenants s'expliquent en partie par le manque d'harmonisation et de normalisation, que la recherche et les démonstrations prénormatives peuvent traiter efficacement

SU-DRS03-2018-2019-2020

SOUS-TOPIC 3: [2020] ***VÉHICULES DE PREMIERS SECOURS*** *: MOYENS DE DÉPLOIEMENT, DE FORMATION, DE MAINTENANCE, DE LOGISTIQUE ET DE COORDINATION CENTRALISÉE À DISTANCE*

- Des normes et des mécanismes communs d'échange de données de communication pour un déploiement efficace des ressources
  - pendant la période précédant une catastrophe majeure (d'origine naturelle ou humaine)
  - ou immédiatement après l'événement

  par exemple pour une évacuation massive d'une zone urbaine

- Les propositions devraient cibler en particulier les événements pour lesquelles
  - de fortes activités de coordination intersectorielle, transfrontalière et interhiérarchique sont nécessaires
  - le besoin de l'interopérabilité est fort

- L'objectif est d'ouvrir la voie à l'amélioration des normes, y compris
  - des normes ISO ou EN
  - et/ou des Procédures Opératoires Normalisées (PON ou SOP) qui décrivent comment affronter une menace et comment agir pour en diminuer le risque.
    - Pour un garde forestier, par exemple, le PON lui indique le nombre de rondes à effectuer, ce qu'il doit emmener avec lui à chaque ronde, et les règles à appliquer en cas d'incident ou incendie détecté(e) au cours de l'une d'entre elles.

SU-DRS04-2019-2020

CLUSTER NRBC (LUTTE CONTRE LES ATTAQUES NUCLÉAIRES, RADIOLOGIQUES, BIOLOGIQUES ET CHIMIQUES

- **Type d'action** Action de Rechercher et d'Innovation (RIA)
- **TRL de sortie** 4 to 6
- **Durée du projet** non spécifiée
- **Budget par projet** ~3,5 M€
- **Budget total** 10,5 M€ (pour 3 projets)
- **Conditions d'éligibilité**
  - Participation d'au moins 3 premiers intervenants de 3 États membres ou pays associés
  - Chaque proposition doit être coordonnée par une PME
  - **Une convention avec le projet ENCIRCLE doit définir comment les résultats seront intégrés dans les plateformes gérées par ENCIRCLE**.
- **Date limite** 27 août 2020
- **Challenge**

  Les entreprises développant des technologies NRBC éprouvent des difficultés à les mettre sur le marché.
  Au moins trois raisons sont identifiées : Ces entreprises

  - s'adressent à de petits marchés de niche locaux ;
  - n'ont ni les capacités ni l'objectif stratégique d'aller sur les marchés étrangers
  - ont besoin d'intégrer leurs avec des offres d'outils d'autres entreprises qui ont les capacités et la stratégie nécessaires pour commercialiser des produits en Europe et à l'International.

SU-FCT

Fight Against Crime and Terrorism

SU-FCT : 2020

Année	Topic (Type d'Action)	Titre	Budget (M€)	Date limite
2020	SU-FCT01-2018-2019-2020 (RIA)	Facteurs humains et aspects sociaux, sociétaux et organisationnels pour résoudre les problèmes liés à la lutte contre la criminalité et le terrorisme	10,00	27 août 2020
	SU-FCT02-2018-2019-2020 (RIA)	Technologies pour renforcer la lutte contre la criminalité et le terrorisme	28,00	
	SU-FCT03-2018-2019-2020 (IA)	Gestion de l'information et des flux de données pour lutter contre la (cyber)criminalité et le terrorisme	8,00	
	SU-FCT04-2020 (IA)	Chimie : renseignement, détection, expertise judiciaire	10,00	

SU-FCT01-2018-2019-2020

FACTEURS HUMAINS ET ASPECTS SOCIAUX, SOCIÉTAUX ET ORGANISATIONNELS POUR RÉSOUDRE LES PROBLÈMES LIÉS À LA LUTTE CONTRE LA CRIMINALITÉ ET LE TERRORISME

Plus de sous-sujets ouverts en 2020

- **Type d'action** Action de Rechercher et d'Innovation (RIA)
- **TRL de sortie** non spécifié
- **Durée du projet** non spécifiée
- **Budget par projet** ~5 M€
- **Budget total** 10 M€
- **Conditions d'éligibilité** Participation d'au moins 3 premiers intervenants de 3 États membres ou pays associés
- **Date limite** 27 août 2020

- **Challenge**
  - ❑ Risques liés à la criminalité et au terrorisme, avec des répercussions transfrontalières au sein de l'UE.
  - ❑ Activités des groupes criminels s'étendant au-delà des frontières nationales

SU-FCT01-2018-2019-2020

SOUS-TOPIC 1 *:[2018, 2020] NOUVELLES MÉTHODES POUR PRÉVENIR, ENQUÊTER ET ATTÉNUER LA TRAITE DES ÊTRES HUMAINS ET L'EXPLOITATION SEXUELLE DES ENFANTS - ET SUR LA PROTECTION DES VICTIMES (1/3)*

Challenge

- La traite des êtres humains et l'exploitation sexuelle des enfants sont facilitées par la mondialisation et les progrès technologiques.
- Des mesures préventives, s'appuyant sur les SHS, et des mesures visant à assurer une protection et une assistance aux victimes sont nécessaires.

Propositions

- Doivent couvrir tout domaine concernant la **prévention**, les **enquêtes** et/ou l'**assistance aux victimes** à la fois pour
  1. La traite des êtres humains
  2. L'exploitation sexuelle des enfants
- Doivent aborder ces deux phénomènes 1) et 2) de manière équilibrée dans les projets.

SU-FCT01-2018-2019-2020

SOUS-TOPIC 1 :[2018, 2020] NOUVELLES MÉTHODES POUR PRÉVENIR, ENQUÊTER ET ATTÉNUER LA TRAITE DES ÊTRES HUMAINS ET L'EXPLOITATION SEXUELLE DES ENFANTS - ET SUR LA PROTECTION DES VICTIMES (2/3)

En ce qui concerne la traite des êtres humains :

- ❑ Prévenir le phénomène
- ❑ Réduire la demande de toutes les formes d'exploitation dans la chaîne de la traite et ses secteurs légaux et illégaux.
- ❑ Analyser l'implication possible de groupes du crimes organisés dans la traite des êtres humains et également dans d'autres crimes (comme les crimes financiers) ;
- ❑ Proposer de nouvelles approches pour enquêter sur les affaires de traite des êtres humains
- ❑ Proposer de nouvelles approches pour atténuer l'impact sur les victimes à court et à long terme.

SU-FCT01-2018-2019-2020

SOUS-TOPIC 1 :[2018, 2020] NOUVELLES MÉTHODES POUR PRÉVENIR, ENQUÊTER ET ATTÉNUER LA TRAITE DES ÊTRES HUMAINS ET L'EXPLOITATION SEXUELLE DES ENFANTS - ET SUR LA PROTECTION DES VICTIMES (3/3)

En ce qui concerne l'exploitation sexuelle des enfants, analyser comment :

- ❑ Faire face à la diffusion vidéo en direct/streaming de la violence à l'égard des enfants, ainsi qu' à la pression, le chantage et le racket sur les victimes
- ❑ Fournir aux « LEA » des moyens efficaces pour détecter, enquêter et faire tomber les nombreux réseaux peer-to-peer et forums sur le darknet qui supportent les criminels
- ❑ Aider les victimes d'abus pendant les enquêtes criminelles, les procédures judiciaires et à long terme pour faire face aux effets
- ❑ Réduire les risques de récidive et de passer à l'acte en comprenant mieux le comportement des agresseurs et des agresseurs potentiels.

SU-FCT01-2018-2019-2020

SOUS-TOPIC 3 *:[2020] ÉLABORER DES APPROCHES FONDÉES SUR DES DONNÉES PROBANTES POUR ÉVALUER ET DÉVELOPPER LES INITIATIVES VISANT À PRÉVENIR ET À CONTRER LA RADICALISATION VIOLENTE (1/2)*

Challenges

- les facteurs et les voies menant à la radicalisation
- les facteurs influençant la résilience à la radicalisation
  - l'accent étant mis sur les groupes nécessitant une attention particulière (comme les enfants)
- le lien entre extrémisme violent et autres formes de criminalité
- l'extrémisme violent en ligne (comme les médias sociaux) et la propagande terroriste
- l’évaluation et impact des contre-récits et des récits alternatifs
- la question des rapatriés, en particulier les enfants et les femmes
- La gestion des extrémistes après leur libération de prison (en impliquant les services pénitentiaires et les autorités judiciaires)
- les aspects socio-économiques et de genre de la radicalisation
- les défis liés au phénomène des acteurs isolés et évaluation des stratégies locales et nationales de prévention

SU-FCT01-2018-2019-2020

SOUS-TOPIC 3 :[2020] ÉLABORER DES APPROCHES FONDÉES SUR DES DONNÉES PROBANTES POUR ÉVALUER ET DÉVELOPPER LES INITIATIVES VISANT À PRÉVENIR ET À CONTRER LA RADICALISATION VIOLENTE (2/2)

L'objectif n'est pas de soutenir des projets qui couvrent toutes ces challenges. Les propositions doivent :

- aborder une ou plusieurs de ces challenges
- tenir compte de l'importance d'une approche multidisciplinaire, multi-institutionnelle et multipartite
- faire référence à des recherches fondées sur des données probantes qui comparent et distillent diverses approches, fournissant des résultats qui sont directement utiles aux décideurs et aux praticiens.
- fournir des indicateurs quantitatifs et/ou qualitatifs permettant d'évaluer les initiatives de prévention, de lutte et de dé radicalisation.
- éventuellement analyser et évaluer différentes méthodologies de recherche dans ce domaine
- s'appuyer sur l'expertise des différentes disciplines et parties prenantes, y compris les praticiens, afin de refléter le défi horizontal de la radicalisation.

L'objectif n'est pas nécessairement d'élaborer de nouvelles réponses, mais de se concentrer sur des analyses comparatives et des évaluations des réponses existantes afin d‘

- identifier des approches transférables et efficaces basées sur ce qui a été fait jusqu'ici, et/ou d'élaborer des indicateurs de performance et/ou des méthodes d'évaluation

La coopération internationale est encouragée.

Le cas échéant, les propositions pourraient s'appuyer sur des projets de radicalisation antérieurs et en cours financés par l'UE

SU-FCT02-2018-2019-2020

TECHNOLOGIES POUR RENFORCER LA LUTTE CONTRE LA CRIMINALITÉ ET LE TERRORISME

- **Type d'action** — Action de Rechercher et d'Innovation (RIA)
- **TRL de sortie** — 4 to 6
- **Durée du projet** — non spécifiée
- **Budget par projet** — ~7 M€
- **Budget total** — 28,00 M€

- **Conditions d'éligibilité** — Participation d'au moins 3 premiers intervenants de 3 États membres ou pays associés (ou au moins 5 premiers intervenants pour le sous-topic ouvert)
- **Date limite** — 27 août 2020

- **Challenge**
  - ❑ Le crime organisé et les organisations terroristes sont souvent à l'avant-garde de l'innovation technologique dans la planification, l'exécution et la dissimulation de leurs activités criminelles et des revenus qui en découlent.
  - ❑ Les LEA sont souvent à la traîne dans la lutte contre les activités criminelles soutenues par les technologies de pointe.

SU-FCT02-2018-2019-2020

SOUS-TOPIC 3 : [2020] SUIVI DES FLUX MONÉTAIRES (1/2)

Challenges

Les nouvelles méthodes ou technologies comme

- ❑ les ventes pseudo-légales
- ❑ l'économie parallèle
- ❑ le darknet
- ❑ les crypto monnaies

sont de plus en plus utilisées pour faciliter diverses activités criminelles

- physiques/traditionnelles comme les
  - abus sexuel d'enfants
  - trafic d'organes ou d'embryons humains
  - traite des êtres humains
  - trafic des armes à feu
  - trafic des drogues
  - blanchiment de capitaux
  - terrorisme
- et/ou en ligne comme les
  - rançon
  - piratage des noms de domaine
  - phishing

Nécessité de

- gouverner et détecter les flux monétaires transfrontaliers susceptibles de soutenir le terrorisme,
- renforcer la coopération entre les secteurs public et privé pour le partage des données financières
- renforcer l'efficacité des méthodes de lutte contre le financement du terrorisme et de modélisation des transactions anormales

SU-FCT02-2018-2019-2020
SOUS-TOPIC 3 : [2020] SUIVI DES FLUX MONÉTAIRES (2/2)

Les propositions devraient porter sur R&D d'approches et d'outils pour :

- identifier des nouveaux développements
  - des nouveaux marchés et réseaux
  - des nouvelles manières de procéder
- retracer les flux d'argent ainsi que les personnes impliquées dans des activités criminelles en ligne
- analyser les marchés sur le Darknet
- localiser et cartographier les répertoires de services cachés
- analyser les supports numériques afin d'identifier des jeux de données monétaires numériques
- établir des modèles de provenance des données (apportant la preuve admissible en justice), incluant la relation entre les artefacts de preuves algorithmiques et la preuve légale.

SU-FCT02-2018-2019-2020

SOUS-THÈME 4 : [2020] DÉVELOPPEMENT ET DÉPLOIEMENT DE TECHNOLOGIES, D'OUTILS ET D'INFRASTRUCTURES PERTINENTES POUR IDENTIFIER RAPIDEMENT LES CONTENUS TERRORISTES EN LIGNE ET EMPÊCHER LEUR RECHARGEMENT. (1/2)

Contexte

Pour faire face à la menace de contenus terroristes en ligne, la Commission a adopté une proposition de règlement le 12/09/2018

- Les fournisseurs de services d'hébergement du monde entier (groupes, PMEs ou microentreprises)
  - couvrant les médias sociaux, les services cloud, le partage de fichiers, etc.
  - offrant leurs services aux citoyens de l'UE

  seraient tenus de mettre en place un certain nombre de mesures
  - réactives rapides, comme par exemple un délai d'une heure pour retirer ou désactiver les contenus terroristes suite à la demande d'une autorité d'un État membre
  - proactives, notamment une détection automatisée, pour retirer ou désactiver efficacement et rapidement les contenus terroristes et empêcher leur réapparition et leur diffusion après leur retrait

Défi

- La mise en place de tels moyens proactifs/automatisés est susceptible de créer une charge sur les ressources
- Nécessité d'envisager des mesures d'atténuation au profit des petites entreprises

SU-FCT02-2018-2019-2020

SOUS-THÈME 4 : [2020] DÉVELOPPEMENT ET DÉPLOIEMENT DE TECHNOLOGIES, D'OUTILS ET D'INFRASTRUCTURES PERTINENTES POUR IDENTIFIER RAPIDEMENT LES CONTENUS TERRORISTES EN LIGNE ET EMPÊCHER LEUR RECHARGEMENT. (2/2)

Les propositions devraient

- soutenir la R&D et le déploiement de technologies, d'outils et d'infrastructures pour
  - identifier rapidement les contenus terroristes en ligne
  - empêcher leur re-téléchargement
- analyser le contenu des médias pour développer des outils de détection des comportements préjudiciables en ligne comme
  - le traitement du langage naturel
  - l'analyse du contenu image
  - l'analyse du contenu vidéo

- La participation des PMEs est nécessaire pour s'assurer que la technologie mise au point soit directement adaptée à leurs plates-formes
- La dissémination et le déploiement des résultats à l'échelle mondiale sont encouragés

SU-FCT02-2018-2019-2020
*SOUS TOPIC : [2018-2019-2020] OUVERT **

Les propositions doivent être soutenues par un grand nombre de praticiens et doivent porter sur des sujets qui

- ne peuvent pas être traités dans les sous-topics prédéfinis dans SU-FCT02

- sont en rapport avec le défi de lutte contre la criminalité et le terrorisme comme des
  - technologies visant à améliorer les capacités des LEA (y compris la réalité augmentée)
  - systèmes autonomes visant à améliorer la lutte contre la criminalité et le terrorisme
  - technologies visant à mieux protéger des personnalités publiques
  - technologies de suivi et de surveillance, notamment la prévention automatique du téléchargement de contenus liés au terrorisme
  - capacités à détecter le plus large éventail possible de menaces et de dissimulations (notamment les armes complexes)

SU-FCT03-2018-2019-2020

*GESTION DE L'INFORMATION ET DES FLUX DE DONNÉES POUR LUTTER CONTRE LA (CYBER)CRIMINALITÉ ET LE TERRORISME **

- **Type d'action** Action d'Innovation (IA)
- **TRL de sortie** 5 à 7
- **Project duration** maximum **24 mois**
- **Durée du projet** 8M€
- **Budget total** 8 M€
- **Conditions d'éligibilité** Participation d'au moins 3 LEAs de 3 États membres ou pays associés
- **Date limite** 27 août 2020
- **Challenge**
  - ❑ Le monde cyber est plus vulnérable avec
    - L'Internet des objets qui peut tout connecter
    - Les appareils portables qui nous permettent d'être traçables
    - les imprimantes 3D qui peuvent produire des armes,
    - les voitures autonomes offrent des opportunités aux kidnappeurs
    - le télétravail qui ouvre des portes pour le cyber-espionnage
  - ❑ De grandes quantités de données et d'informations d'origines diverses sont devenues accessibles aux praticiens impliqués dans la lutte contre la criminalité et le terrorisme.
  - ❑ Les techniques les plus avancées en matière d'analyse de grandes données et d'intelligence artificielle ne sont pas encore pleinement exploitées.

SU-FCT03-2018-2019-2020 - SCOPE

*GESTION DE L'INFORMATION ET DES FLUX DE DONNÉES POUR LUTTER CONTRE LA (CYBER)CRIMINALITÉ ET LE TERRORISME **

- Les propositions devraient *exclusivement porter point b du sous-topic :*
  - Fournir une solution pour exploiter les big data et pour faire des analyses prédictives afin d'améliorer **la sécurité des citoyens vis-à-vis des attaques terroristes dans les lieux considérés comme cibles faciles**, notamment les zones denses (stations, centres commerciaux, salles de spectacles, etc.)

  en mettant l'**accent sur les opérateurs privés**
  les premières personnes sur les lieux d'un attentat terroriste sont souvent des agents de sécurité privés de magasins locaux ou d'opérateurs de transport
- Mette en place des systèmes de détection comportementale/anomalie fonctionnant en temps quasi réel et à des distances (utilisant une grande variété de capteurs) pour permettre l'identification des événements suspects ou des criminels.
- Améliorer l'efficacité des enquêteurs en utilisant des outils d'analyse big data (prétraitement, traitement et analyse, visualisation, etc.)
- Améliorer la qualité des données et à convertir des ensembles de big data hétérogènes
  images, vidéos, renseignements géospatiaux, données de communication, données relatives au trafic, données relatives aux transactions financières, date, etc.
- Collecter des renseignements de source ouverte, des réseaux sociaux et de l'analyse de données darknet
- Les consortia doivent associer des opérationnels de la sécurité, des organisations de la société civile et un équilibre approprié de spécialistes des technologies de l'information, de psychologues, de sociologues, de linguistes, etc.
- Les aspects sociétaux (par exemple, la perception de la sécurité, les effets secondaires possibles des solutions technologiques, la résilience de la société) doivent être abordés de manière globale et approfondie

SU-FCT04-2020

CHIMIE : RENSEIGNEMENT, DÉTECTION, EXPERTISE JUDICIAIRE

- **Type d'action** Action d'Innovation (IA)
- **TRL de sortie** 6 à 7
- **Project duration** maximum **24 months**

- **Durée du projet** 5 M€
- **Budget total** 10 M€

- **Conditions d'éligibilité** Participation d'au moins 3 LEAs de 3 États membres ou pays associés
- **Date limite** 27 août 2020
- **Challenge**
  - ❑ Les criminels, y compris les terroristes, cherchent constamment de nouvelles façons de développer, de déployer et d'activer des produits chimiques dangereux (explosifs, neurotoxines, nouvelles drogues, etc.).
  - ❑ La façon dont ces produits chimiques sont fabriqués et combinés évolue en permanence

SU-FCT04-2020 - SCOPE

CHIMIE : RENSEIGNEMENT, DÉTECTION, EXPERTISE JUDICIAIRE

Les propositions doivent

- améliorer les connaissances sur ces produits chimiques dangereux
- développer des technologies pour contrer les incidents et y répondre
- intensifier les messages de dissuasion, tout en considérant les inconvénients que les mesures de sécurité imposent aux opérateurs et utilisateurs des espaces publics
- démontrer comment elles s'appuieront efficacement sur les projets H2020 pertinents précédents et créeront des synergies avec les projets H2020 en cours

Les propositions ne doivent porter que sur l'un des sujets suivants (A ou B exclusivement) :

A. Poursuivre des travaux déjà réalisés sur certains précurseurs d'explosifs dans le cadre de projets antérieurs du 7ième PCRD (FP7) et du programme H2020, notamment sur des nouveaux précurseurs non encore étudiés

B. Etudier l'utilisation de produits chimiques et éventuellement de leurs précurseurs, autres que les explosifs et les précurseurs d'explosifs dans A. Puis proposer des moyens de réduire la vulnérabilité du public à leur utilisation malveillante ou terroriste (du renseignement initial à l'attaque)

SU-BES

Border and External Security

SU-BES : 2020

Année	Topic (Type d'Action)	Titre	Budget (M€)	Date limite
2020	SU-BES01-2018-2019-2020 (RIA)	Facteurs humains et aspects sociaux, sociétaux et organisationnels de la sécurité aux frontières et extérieure	5,0	27 août 2020
	SU-BES02-2018-2019-2020 (RIA)	Technologies visant à renforcer la sécurité aux frontières et la sécurité extérieure	21,0	
	SU-BES03-2018-2019-2020 (IA)	Démonstration de solutions pour renforcer la sécurité aux frontières et la sécurité extérieure	10,0	

SU-BES01-2018-2019-2020

FACTEURS HUMAINS ET ASPECTS SOCIAUX, SOCIÉTAUX ET ORGANISATIONNELS DE LA SÉCURITÉ AUX FRONTIÈRES ET EXTÉRIEURE

Plus de sous-sujets ouverts en 2020

- **Type d'action** Action de Rechercher et d'Innovation (RIA)
- **TRL de sortie** non spécifié
- **Durée du projet** non spécifiée
- **Budget par projet** ~5 M€
- **Budget total** 5 M€
- **Conditions d'éligibilité** Participation d'au moins 3 opérationnels de 3 États membres ou pays associés
- **Date limite** 27 août 2020

- **Challenges** des gardes-frontières de l'UE

  Sous-topic 3: [2020]

  - ❑ la gestion des flux de personnes
  - ❑ la contrebande
  - ❑ l'utilisation de faux documents
  - ❑ l'évaluation de l'impact des menaces extérieures sur la sécurité intérieure
  - ❑ Le développement d'un modèle de comparaison des menaces extérieures pour une meilleure connaissance de la situation

SU-BES01-2018-2019-2020 - SCOPE

SOUS-TOPIC 3 : [2020] DÉVELOPPER DES INDICATEURS DE MENACES AUX FRONTIÈRES EXTÉRIEURES DE L'UE SUR LA BASE DE MÉTHODOLOGIES SOLIDES D'ÉVALUATION DES RISQUES ET DE LA VULNÉRABILITÉ

- Améliorer l'efficacité des contrôles aux frontières, y compris aux frontières aériennes, terrestres et maritimes,
  - en mettant au point des indicateurs composites dynamiques des menaces extérieures,
  - en comparant les différentes menaces se produisant simultanément à la frontière
  - en proposer des mesures prioritaires d'atténuation.
- Analyser la synergie et les interrelations antre les nombreuses détections à la frontière
- Etudier l'impact de ces détections sur la sécurité intérieure
- Faire un démonstrateur dans un environnement pertinent pour démontrer l'adéquation des concepts proposés à l'usage auquel ils sont destinés

- *Lecture*
  - Modèle d'analyse commune et intégrée des risques https://frontex.europa.eu/assets/CIRAM/fr_CIRAM_brochure_2013.pdf
  - Evaluation des vulnérabilités https://frontex.europa.eu/intelligence/vulnerability-assessment/

SU-BES02-2018-2019-2020

TECHNOLOGIES VISANT À RENFORCER LA SÉCURITÉ AUX FRONTIÈRES ET LA SÉCURITÉ EXTÉRIEURE

- **Type d'Action** Action de Rechercher et d'Innovation (RIA)
- **TRL de sortie** 5 à 6
- **Durée du projet** non spécifiée
- **Budget par projet** ~7 M€
- **Budget total** 21 M€
- **Conditions d'éligibilité** Participation d'au moins 3 Garde-côtes / Garde-frontières de 3 États membres ou pays associés
- (ou au moins 5 Garde-côtes / Garde-frontières pour le sous-topic ouvert)
- **Date limite** 27 août 2020

- **Challenges**
  - ❑ Trafic de marchandises illicites et dissimulés par des organisations criminelles utilisant des outils ultra sophistiqués
  - ❑ Les nouvelles technologies employées doivent être
    - Abordables
    - Acceptées par les citoyens
    - Adaptées pour répondre aux besoins des praticiens

SU-BES02-2018-2019-2020

SOUS-TOPIC 5 :[2020] TECHNOLOGIES DISRUPTIVES POUR L'IDENTIFICATION NON INTRUSIVE DES OBJETS CACHÉS

Besoins partagé par les gardes-frontières, les douanes et les services répressifs (LEA)

- **Détection et identification des marchandises illégales** aux frontières extérieures : ports, quais, gares ferroviaires, etc.
  dissimulées dans des conteneurs, des wagons, des camions
  - Comme drogues, armes, explosifs, matières radiologiques et nucléaires

Les projets devraient faire de la recherche pour

- l'utilisation **de technologies de détection plus puissantes** sans qu'il soit nécessaire d'ouvrir des conteneurs

- La **mise au point d'un système de capteurs**
  - produisant une **vision tridimensionnelle** détaillée de la structure interne d'un conteneur ou d'un camion
  - **Convivial** à être utilisé sur le terrain
  - s'exécutant en un **temps limité**
  - **déployable de manière souple** et mobile
  - **Permettant la collecte et un échange rapides d'informations avec d'autres systèmes** de faciliter une localisation et une identification plus rapides et plus précises des cargaisons illicites

- les solutions devraient permettre l'interopérabilité avec les systèmes d'information frontaliers et douaniers
  - Pour optimiser le processus global d'inspection/filtrage des conteneurs selon une approche fondée sur les risques

- Les propositions doivent être testées et validées dans l'environnement pertinent

SU-BES02-2018-2019-2020

TECHNOLOGIES VISANT À RENFORCER LA SÉCURITÉ AUX FRONTIÈRES ET LA SÉCURITÉ EXTÉRIEURE

- Sous-topic: [2018-2019-2020] Ouvert

SU-BES03-2018-2019-2020

DÉMONSTRATION DE SOLUTIONS POUR RENFORCER LA SÉCURITÉ AUX FRONTIÈRES ET LA SÉCURITÉ EXTÉRIEURE

- **Type d'action** — **Action d'Innovation (IA)**
- **TRL de sortie** — 6 à 8
- **Durée du projet** — maximum **18 mois**

- **Budget par projet** — 5M€
- **Budget total** — 10 M€ in 2019
- **Taux de financement exceptionnels** — Le coût du carburant est exclu des coûts éligibles

- **Conditions d'éligibilité** — Participation d'au moins 3 Garde-frontières de 3 États membres ou pays associés (ou au moins 5 Garde-frontières pour le sous-topic ouvert) - pas de garde-côtes
  Les consortiums doivent être coordonnés par un praticien sous autorité civile.

- **Date limite** — 27 août 2020

- **Challenge**
  - ❑ Des solutions pour améliorer la sécurité aux frontières nécessitent d' être démontrées dans un environnement opérationnel pour être validées par les garde-frontières

SU-BES03-2018-2019-2020

SOUS-TOPIC 3 :[2020] AMÉLIORATION DES SYSTÈMES DE SUIVI DES NAVIRES, D'ANALYSE DU COMPORTEMENT ET DE DÉTECTION AUTOMATIQUE DES ANOMALIES - CHALLENGE (1/2)

- Challenge
  - Les systèmes actuels de notification maritime produisent d'énormes quantités de données qui ne peuvent être exploitées par les opérateurs humains dans les centres de contrôle maritime.
  - La quantité de données disponibles va augmenter davantage avec l'introduction du système d'échange de données VDES (VHF Data Exchange System).
  - Des sources non homogènes d'informations accessibles sur les navires pourraient être utilisées pour effectuer des analyses de risques sur chaque navire
  - Les systèmes de reporting traditionnels ne suffisent pas à eux seuls à permettre une détection fiable des anomalies

SU-BES03-2018-2019-2020

SOUS-TOPIC 3 :[2020] AMÉLIORATION DES SYSTÈMES DE SUIVI DES NAVIRES, D'ANALYSE DU COMPORTEMENT ET DE DÉTECTION AUTOMATIQUE DES ANOMALIES - SCOPE (2/2)

- Projets
  - Construire un système de détection des anomalies plus précis et plus robuste
  - Les solutions doivent utiliser 3 sources d'information :
    1. données des systèmes de notification et de surveillance contenant par exemple des informations sur un trajet de navire
    2. bases de données pertinentes contenant des informations historiques sur les navires et/ou conteneurs
    3. données en temps réel ou quasi réel résultant d'autres sources de notification ou de surveillance
  - La combinaison de ces sources d'information devrait produire **un chiffre de notation du risque** pour attribuer automatiquement le niveau de risque aux navires
  - Les solutions devraient être basées sur des algorithmes capables de s'adapter aux composants avec lesquels ils interagissent comme des composants d'intelligence artificielle et d'apprentissage, appliqués aux systèmes existants de notification des navires.
  - Tester et valider la solution dans un environnement opérationnel réel
  - Recommander des approches pour la mise sur le marché de la solution

Eviter la duplication avec d'autres projets y compris dans le programme de défense (PADR-US-01-2017)

SU-BES03-2018-2019-2020

DÉMONSTRATION DE SOLUTIONS POUR RENFORCER LA SÉCURITÉ AUX FRONTIÈRES ET LA SÉCURITÉ EXTÉRIEURE

- Sous-topic: [2018-2019-2020] Ouvert

SU-GM

General Matters

SU-GM : 2020

Année	Topic (Type d'Action)	Titre	Budget (M€)	Date limite
2020	SU-GM01-2018-2019-2020 (CSA)	Réseaux paneuropéens de praticiens et d'autres acteurs dans le domaine de la sécurité	7,0	27 août 2020
	SU-GM02-2018-2020 (PCP)	Achats stratégiques pré-commerciaux de systèmes novateurs et évolués pour soutenir la sécurité	24,0	

SU-GM01-2018-2019-2020

RÉSEAUX PANEUROPÉENS DE PRATICIENS ET D'AUTRES ACTEURS DANS LE DOMAINE DE LA SÉCURITÉ

- **Type d'action** Action de Support et de Coordination (CSA)
- **TRL de sortie** non spécifié
- **Durée du projet** non spécifiée
- **Budget par projet** **3,5** M€
- **Budget total** 7 M€
- **Conditions d'éligibilité** Participation d'au moins 8 opérationnels de 8 États membres ou pays associés
  25% du budget total est consacré sur l'interaction avec toutes les parties prenantes pour l'évaluation de la faisabilité
- **Date limite** 27 août 2020

- **Challenge**

  Les organisations de praticiens ont peu de marge de manœuvre pour libérer la main-d'œuvre afin d'allouer du temps et des ressources pour surveiller l'innovation et la recherche qui pourraient leur être utiles.

  Ils ont peu d'occasions d'interagir avec le milieu universitaire ou l'industrie sur ces questions.

SU-GM01-2018-2019-2020

A. 2019-2020] PRATICIENS (UTILISATEURS FINAUX) DANS LA MÊME DISCIPLINE ET DANS TOUTE L'EUROPE *(1/3)*

Les praticiens sont invités à se rencontrer :

1) suivre les projets de R&I en vue de recommander l'adoption ou l'industrialisation des résultats
2) exprimer des exigences communes en ce qui concerne les innovations qui pourraient combler les lacunes en matière de capacités,
3) indiquer les priorités dans les domaines nécessitant une normalisation accrue.

En 2020, les propositions sont invitées à couvrir l'une des deux options suivantes :

- ❑ Option 1 : les services de sécurité et de renseignement
- ❑ Option 2 : lutte contre la cybercriminalité

SU-GM01-2018-2019-2020

A. 2019-2020] PRATICIENS (UTILISATEURS FINAUX) DANS LA MÊME DISCIPLINE ET DANS TOUTE L'EUROPE *(2/3)*

TRANSFORMATIONS ET RÉFORMES de la sécurité et du renseignement en Europe

- Option 1 : les services de sécurité et de renseignement
  - La menace terroriste persistante est de plus en plus diversifiée et complexe
  - Les services de renseignement et de sécurité ont des besoins de recherche différents de ceux des LEA
  - L'utilisation d'outils à la pointe de la technologie est la clé de la performance de ces services

  Par conséquent,

  - un réseau de praticiens des services de sécurité et de renseignement est important pour
    - identifier les technologies émergentes et les nouvelles menaces potentielles
    - identifier des besoins futurs en matière de recherche , comme big data et l'IA
    - la programmation future de la recherche sur la sécurité
  - Ce réseau pourrait se concentrer sur l'interaction avec les projets H2020 existants pertinents

En coopération avec la Commission, des méthodes de travail seraient définies pour protéger les besoins spécifiques des services de sécurité et de renseignement participant au consortium.

SU-GM01-2018-2019-2020

A. 2019-2020] PRATICIENS (UTILISATEURS FINAUX) DANS LA MÊME DISCIPLINE ET DANS TOUTE L'EUROPE *(3/3)*

- Option 2 : lutte contre la cybercriminalité
  - Dans le domaine de la cybercriminalité, la technologie et les scénarios de menaces évoluent à grand rythme
  - Il manque encore une cartographie précise des capacités spécifiques des autorités des États membres
  - Puisque la cybercriminalité n'a pas de frontières, il faut identifier des défis et des solutions communes
  - Un réseau spécialisé de praticiens dans le traitement des preuves numériques est utile

Le réseau sur la lutte contre la cybercriminalité contribuera à mieux hiérarchiser et planifier les futures recherches :

1. Assurer la liaison avec les parties prenantes concernées afin d'anticiper les besoins et lacunes futurs en matière de capacités
2. Cataloguer, agréger, traiter et exploiter les connaissances sur l'état actuel et futur des technologies
3. Communiquer les résultats pertinents aux communautés concernées, fournissant ainsi le feedback nécessaire au cycle de recherche, ainsi qu'aux autres initiatives technologiques en faveur du renforcement des capacités lancées au niveau communautaire ou national

SU-GM02-2018-2020

ACHATS STRATÉGIQUES PRÉ-COMMERCIAUX DE SYSTÈMES NOVATEURS ET ÉVOLUÉS POUR SOUTENIR LA SÉCURITÉ

- **Type d'Action** Achat pré-commercial (PCP)
- **TRL de sortie** 8
- **Project duration** not specified

- **Budget par projet** 2 à 12 M€
  Les taux de financement sont limités à 70 % des coûts éligibles.
  Les demandeurs peuvent demander un taux de financement moins élevé afin d'accroître l'effet de levier.
- **Budget total** 24 M€

- **Conditions d'éligibilité** la participation d'au moins 3 organisations de praticiens concernées,
  ainsi que de 3 "acheteurs" potentiels de systèmes de 3 pays différents de l'UE ou associés est requise.

  Le sous-topic 2020 n'est ouvert qu'aux entités ayant participé aux actions relevant du sous-topic 1 (CSA)
- **Date limite** 27 août 2020
- **Challenge**
  - ❑ Des solutions innovantes sont nécessaires lorsque des ressources provenant de différents pays sont nécessaires pour travailler plus ensemble.
  - ❑ Ces solutions devraient soutenir le développement de l'Union européenne en matière de sécurité.

SU-GM02-2018-2020 - SCOPE

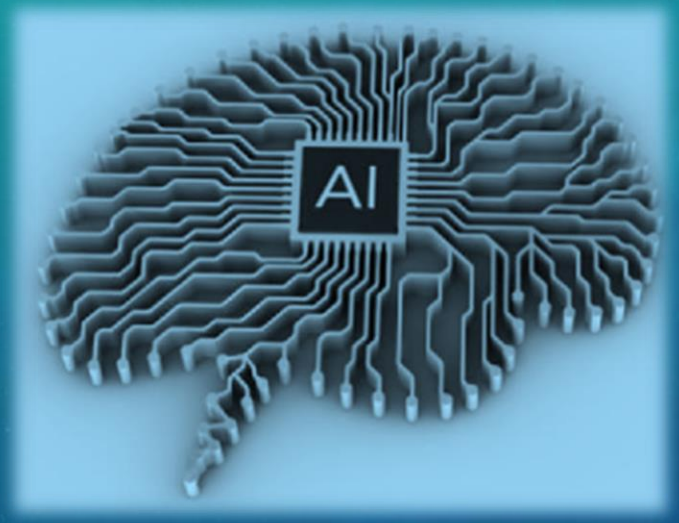
ACHATS STRATÉGIQUES PRÉ-COMMERCIAUX DE SYSTÈMES NOVATEURS ET ÉVOLUÉS POUR SOUTENIR LA SÉCURITÉ

Les propositions doivent

- s'appuyer sur les résultats du sous-topic 1 (le CSA).
- Traiter les aspects suivants :
  - Compléter le cycle de maturation de certaines technologies
  - Trouver un groupe consolidé d'acheteurs potentiels ayant des besoins et des exigences communs qui s'engagent à mener une action PCP
  - Montrer qu'il existe une communauté quantifiable et identifiable d'acheteurs potentiels (au-delà du consortium) qui partageraient dans une large mesure les besoins et exigences communs;
  - Prouver que l'état de l'art et le marché (y compris la recherche) ont été explorés et cartographiés, et qu'il existe différentes alternatives techniques pour relever le défi proposé
  - Prouver que le futur processus d'appel d'offres du PCP est clair et que tout sera prêt en temps voulu pour lancer l'appel d'offres pour l'acquisition de services de R&D

SU-AI

Intelligence artificielle pour les forces de sécurité



SU-AI
L'INTELLIGENCE ARTIFICIELLE POUR LES FORCES DE L'ORDRE

Year	Topic (Type of Action)	Title	Budget (M€)	Deadline
2020	SU-AI01-2020 (CSA)	Développement d'une feuille de route	1,5	27 Août 2020
	SU-AI02-2020 (1A)	Technologies, outils et solutions	17,0	
	SU-AI03-2020 (CSA)	Facteurs humains et aspects SHS	1,5	

INTELLIGENCE ARTIFICIELLE (IA)

Approche demandée dans Horizon 2020

APPEL H2020-SU-AI-2020

- L'intelligence artificielle (IA) fait référence à toute machine ou algorithme capable

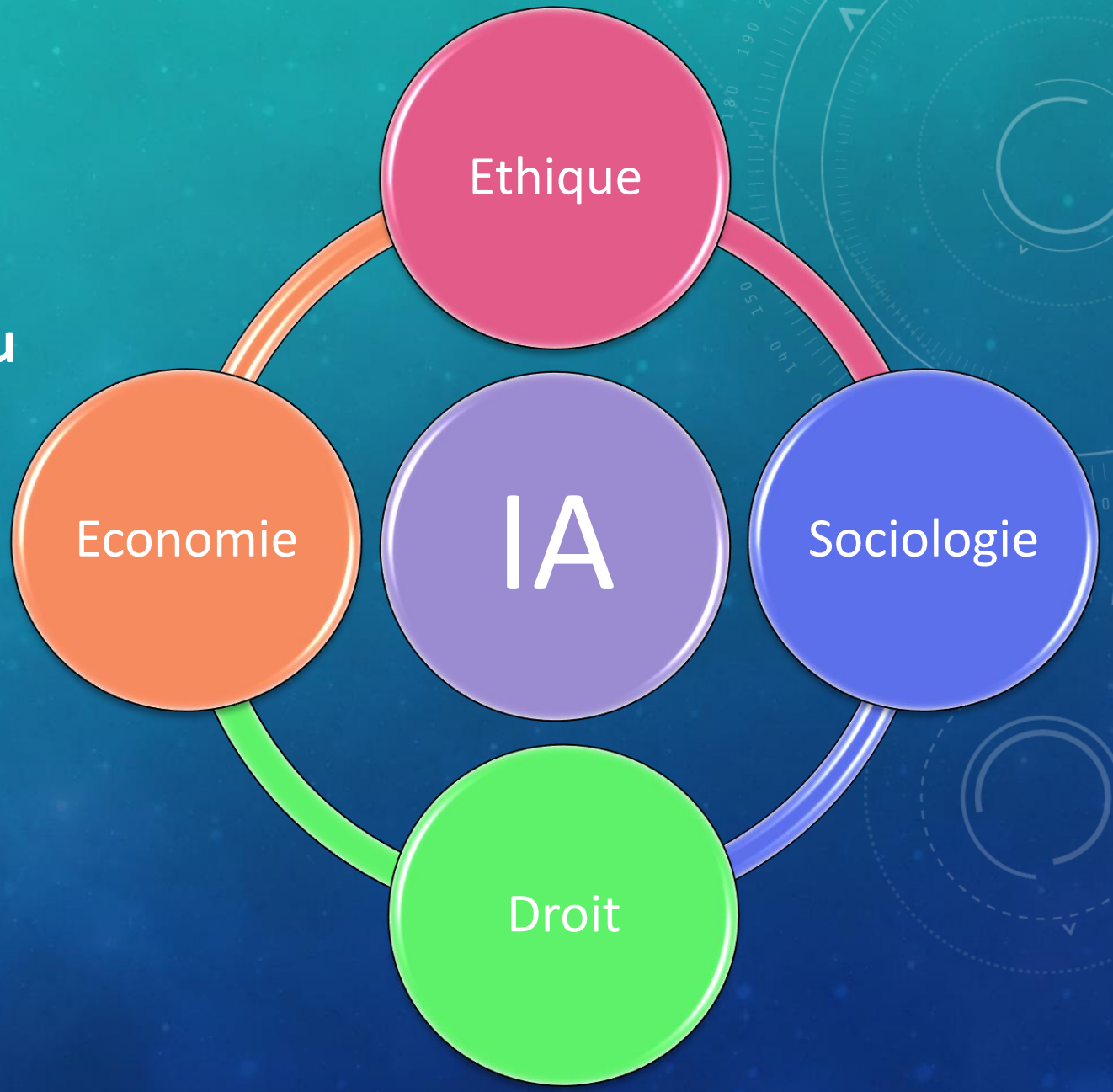
1. d'observer son environnement,
2. d'apprendre,
3. et peut prendre des mesures intelligentes ou proposer des décisions (en se basant sur les connaissances et l'expérience acquises)

DES TECHNOLOGIES DE L'IA

IA ET SHS

Approche plaçant les personnes au centre du développement de l'IA

« IA centré sur l'être humain »



Horizon 2020 Sociétés Sûres

L’APPEL INTELLIGENCE ARTIFICIELLE

3 TOPICS SUR L'INTELLIGENCE ARTIFICIELLE (IA)

Action de Coordination et de Support (CSA)

SU-AI01-2020:

*Developing a **research roadmap** regarding Artificial Intelligence in support of Law Enforcement*

*Durée du projet : **5 ans** - Budget : **1,5 M€***
Au moins 3 autorités chargées d'appliquer la loi (LEA)

SU-AI03-2020:

***Human factors**, and ethical, societal, legal and organisational aspects of using Artificial Intelligence in support of Law Enforcement*

*Durée du projet : **2 ans** - Budget : **1,5 M€***
Au moins 3 LEA

Action d'Innovation (IA)

SU-AI02-2020:

Secure and resilient Artificial Intelligence **technologies, tools and solutions** in support of Law Enforcement and citizen protection, cybersecurity operations and prevention and protection against adversarial Artificial Intelligence

*Durée du projet : **5 ans** - Budget : **17 M€***
Au moins **5** LEA

LES 2 SUJETS DE TYPE CSA

ACTIONS DE SUPPORT ET DE COORDINATION

SU-AI01-2020 : DÉVELOPPEMENT D'UNE **FEUILLE DE ROUTE** DE RECHERCHE SUR L'IA POUR LE MAINTIEN DE L'ORDRE

- **Produire des recommandations** mises à jour tous les six mois

- **Fournir une feuille de route de l'UE sur l'IA pour les LEA** répondant à leurs besoins opérationnels et de coopérations, en identifiant :

1. **Les domaines clés pour lesquels l'IA serait bénéfique pour les LEA**
2. **Les moyens de prévention liés à l'utilisation malveillante et criminelle de l'IA**

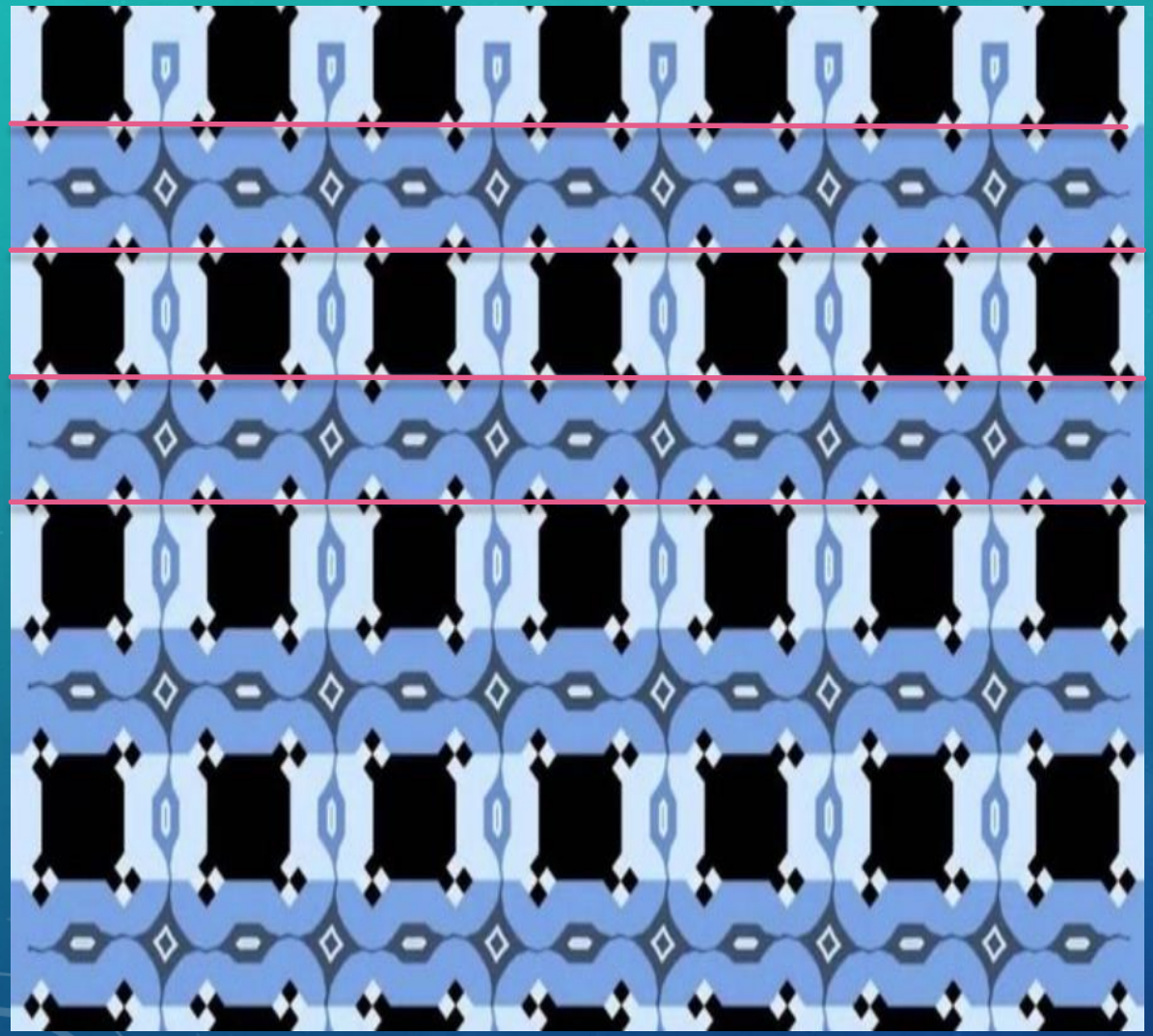
} ***Utilisation de l'IA à la fois par les bons et les méchants.***
Double nature fondamentale des outils

3. **les exigences en matière de cybersécurité des systèmes basées sur l'IA**
4. **Les domaines pour lesquels l'IA pourrait être attaquée**

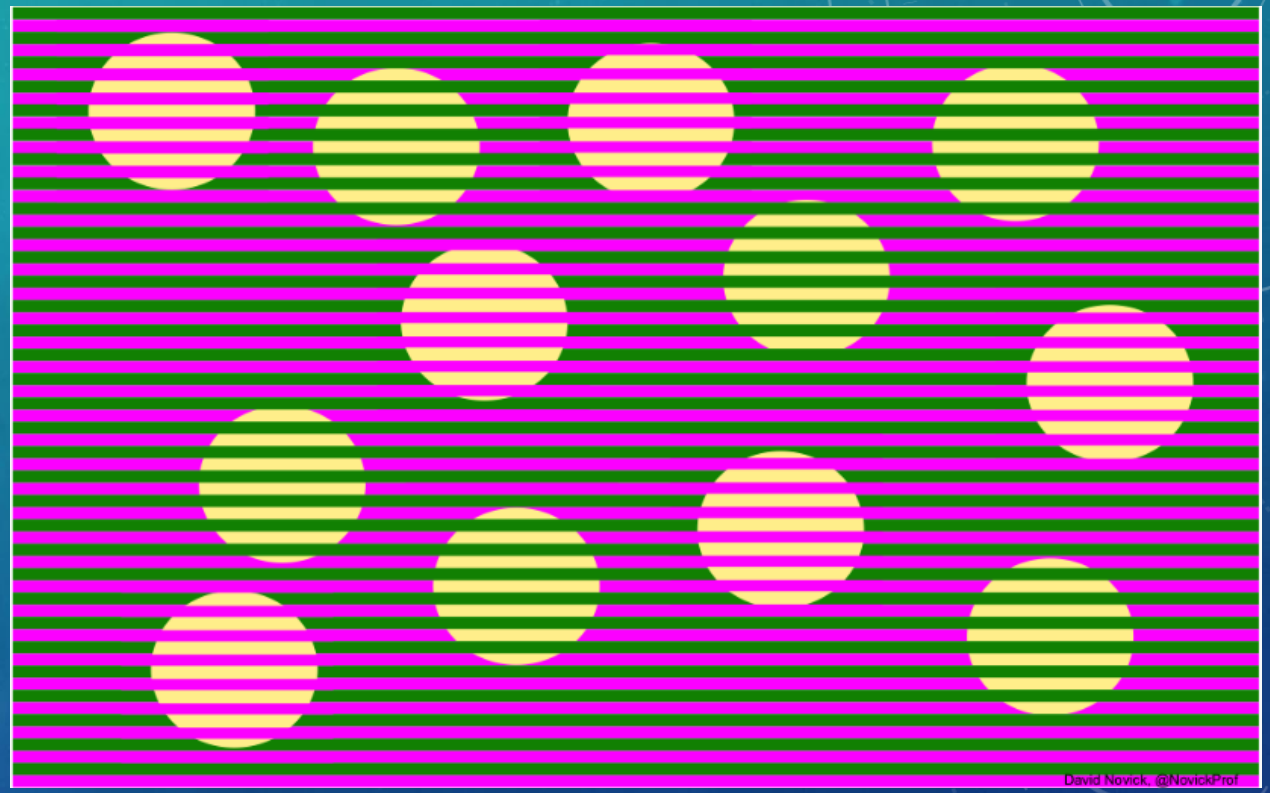
} ***Cyber sécurité des systèmes augmentés par l'IA***

CETTE ILLUSION FAIT APPARAÎTRE DES DROITES PARALLÈLES COMME NON //

Cette illusion fait apparaître des droites // comme non //



Tous ces disques sont de même couleur RVB 255 238 138



On peut attaquer des systèmes basés sur l'intelligence artificielle
comme ces illusions attaquent l'intelligence naturelle de reconnaissance de formes dans notre cerveau

SU-AI03-2020 : FACTEURS HUMAINS ET ASPECTS ÉTHIQUES, SOCIÉTAUX, JURIDIQUES ET ORGANISATIONNELS DE L'UTILISATION DE L'IA EN SOUTIEN DES LEA

- Fournir une analyse exhaustive des aspects humains, éthiques, sociaux, sociétaux, juridiques et organisationnels liés à l'utilisation des outils d'IA pour le soutien des LEA

- Suggérer des approches pour stimuler l'acceptation des outils d'IA par la société civile et par les forces de l'ordre.

LE SUJET DE TYPE IA

ACTION D'INNOVATION

SU-AI02-2020 : TECHNOLOGIES, OUTILS ET SOLUTIONS D'IA SÉCURISÉS

Exploration puis EXPLOITATION de l'IA en sécurité

Explorer l'utilisation de l'IA dans le domaine de la sécurité

- Etude de l'état de l'art
- Proposition de projets à la pointe de la technologie et au-delà

Exploiter le potentiel de l'IA pour soutenir les LEA dans les opérations

- Démonstration d'un prototype de système dans un environnement opérationnel (TRL 7)
- Validation et qualification du système complet (TRL 8)

Sur 5 ans

SU-AI02-2020 : TECHNOLOGIES, OUTILS ET SOLUTIONS D'IA SÉCURISÉS

Fournir des outils et solutions basés sur l'IA pour :

Aider les LEA dans leurs opérations, en particulier pour

- renforcer les capacités d'enquête
- renforcer l'établissement de preuves numériques devant les tribunaux
- coopérer efficacement avec les autorités locales compétentes

Contrer l'IA malveillante utilisée par les cybercriminels

- La recherche sur les capacités et les faiblesses des systèmes IA est indispensable pour contrer les utilisations malveillantes de l'IA

Assure la cyber sécurité et la protection des systèmes, y compris contre les attaques sur l'IA

la prévention, la détection et la réponse aux incidents de cyber sécurité ciblant en particulier

- les unités de cybercriminalité des LEA,
- les centres de coopération de police et des douanes,

les équipes communes d'enquêtes,

les équipes de réponse aux incidents de sécurité informatique (CSIRT - Computer Security Incident Response Team) des LEA.

Lien avec SU-AI01

Responsabilité du COMMENT

Le QUOI est également défini dans les projets CSA

PRÉOCCUPATIONS LÉGALES, SÉCURITAIRES, ÉTHIQUES, JURIDIQUES

Lien avec SU-AI03

Formuler les actions pour :

- ❑ Réaliser une analyse comparative des dispositions juridiques existantes dans toute l'Europe
- ❑ Identifier les modifications législatives (nationales et européennes) qui pourraient être promues
- ❑ Définir les implications éthiques et opérationnelles des LEA
- ❑ Mettre en place des moyens juridiques et éthiques au niveau européen qui permettent la création d'ensembles de données européennes actualisées pour la formation et les tests, disponibles pour la communauté scientifique travaillant avec les LEAs.
- ❑ Spécifier et assurer les développements techniques qui devraient être réalisés pour soutenir tous ces aspects

MÉTHODOLOGIE : LES PROPOSITIONS DOIVENT

Développer des outils et des solutions d'IA pour les LEA

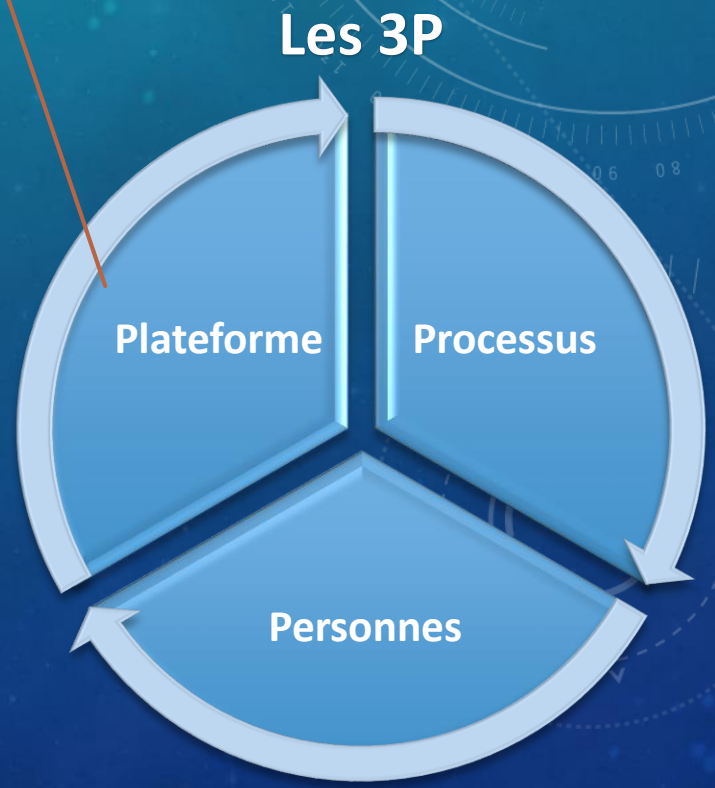
- Solutions matérielles et logicielles combinées : robotique ou traitement du langage naturel

Construire une plate-forme d'outils d'IA faciles à intégrer et interopérables

Etablir un processus associé avec des cycles de recherche et d'essais courts (AGILE)

Aboutir à une **communauté** d'IA durable comprenant des LEA, chercheurs académiques, industriels, associations, …

La plate-forme devrait permettre un accès direct des LEA à un ensemble initial d'outils



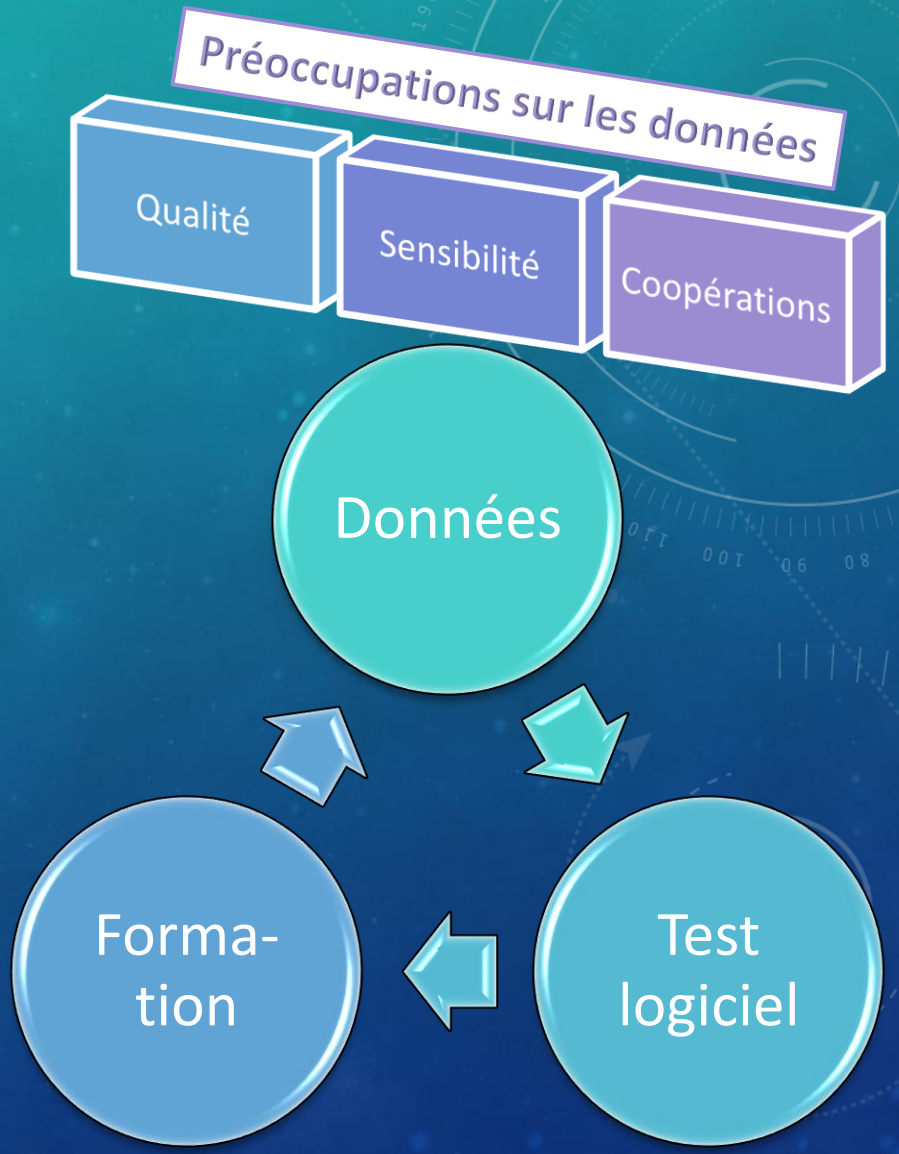
Regarder des projets tels que (mais sans s'y limiter) ASGARD, EPE, SIRIUS, les réseaux de praticiens, AI4EU, ou les activités de LEIT, notamment dans Robotics, Big Data et IoT

LES DONNÉES SONT IMPORTANTES

- Accorder une attention particulière aux données
  - Leur qualité, structure, étiquetage, intégrité, quantité, disponibilité, origine, stockage, accès et pertinence
  - Nécessité d'une coopération étroite autour des données entre les différents systèmes nationaux (de sécurité, de justice, …)
  - La sensibilité des données de sécurité complique l'accès à de véritables ensembles de données multilingues et la création d'ensembles de données représentatifs

- Développer des jeux de données pour la formation et pour les tests au niveau européen
  - La mise à la disposition de la communauté scientifique de ces ensembles de données garantirait les progrès futurs de l'IA

- Formuler les actions qui devraient être menées pour identifier :
  - Les obstacles rencontrés par la communauté des chercheurs pour accéder aux ensembles de données utilisés par les LEA
  - Les moyens de surmonter



SU-AI02-2020: IMPACTS ATTENDUS

Court terme :

- Pour la communauté scientifique qui développe des outils d'IA en soutien des LEA, mise au point d'un ensemble de données européennes représentatives et suffisamment vastes, multilingues et multimodales de haute qualité
- Approche commune de l'UE en matière d'IA à l'appui des LEA, efforts centralisés, par exemple, concernant la question des données nécessaires à l'IA.

Moyen terme :

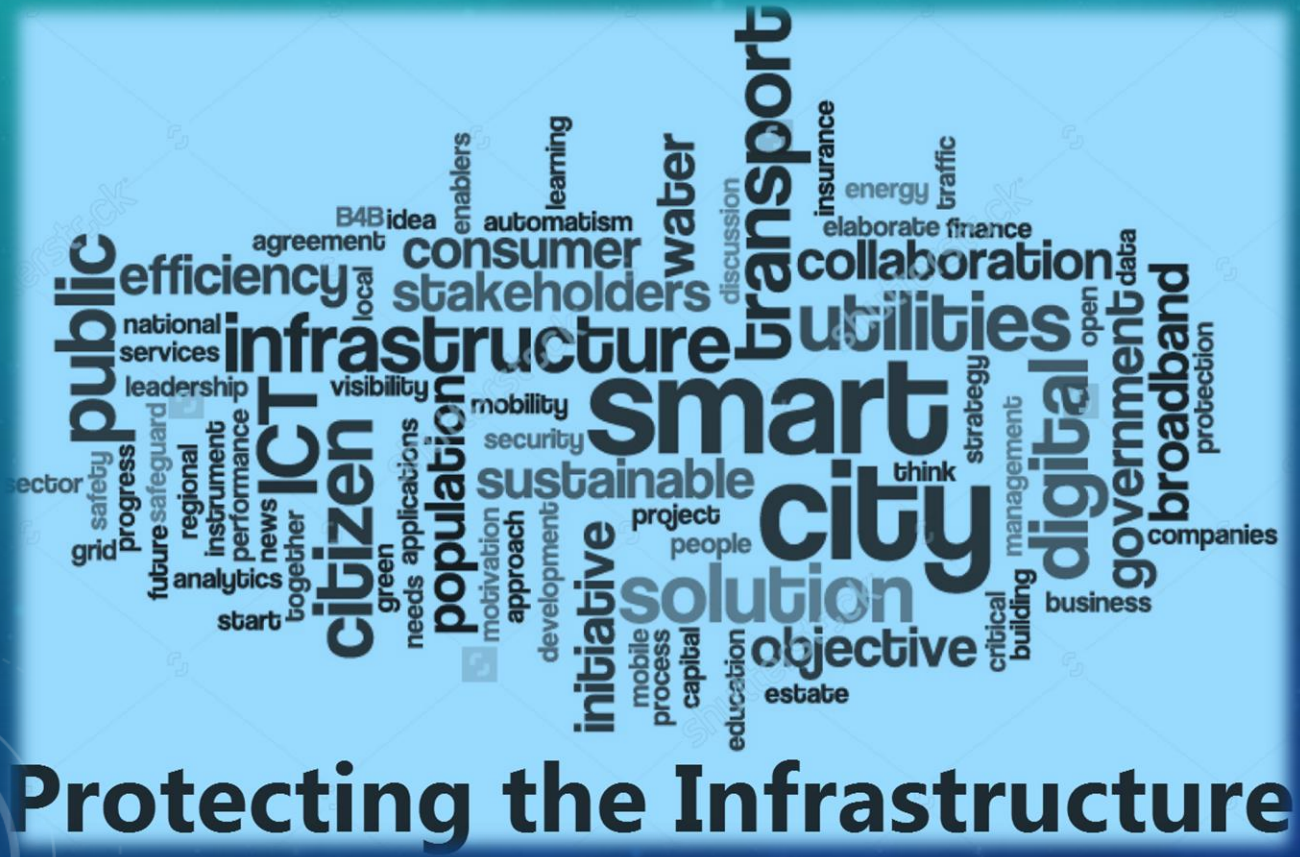
- Amélioration de la capacité des LEA à mener des enquêtes et des analyses à l'aide de l'IA
- Résilience accrue à l'IA antagoniste
- Sensibilisation des acteurs politiques de l'UE afin de les aider à créer un environnement juridique approprié pour l'IA dans les domaines de la cyber sécurité et de la lutte contre la criminalité et le terrorisme

A plus long terme :

- Modernisation du travail des LEA en Europe et amélioration de leur coopération
- Création éventuelle à l'avenir d'un centre européen d'IA à l'échelle de l'Union européenne
- Contribuer à l'établissement d'une industrie d'approvisionnement forte dans ce secteur en Europe

SU-INFRA

Protéger les infrastructures de l'Europe et les habitants des villes intelligentes



SU-INFRA : 2020

Année	Topic (Type d'Action)	Titre	Budget (M€)	Date limite
2020	SU-INFRA01-2018-2019-2020 (IA)	Prévention, détection, réponse et atténuation des menaces physiques et des cyber menaces sur les infrastructures critiques	20,7	27 Aug 2020

SU-INFRA01-2018-2019-2020 *

PREVENTION, DETECTION, RESPONSE AND MITIGATION OF COMBINED PHYSICAL AND CYBER THREATS TO CRITICAL INFRASTRUCTURE IN EUROPE

- **Type d'action** Innovation Action
- **TRL de sortie** 7
- **Durée du projet** maximum **24 mois**
- **Budget par projet** entre 7 et 8 M€
- **Budget total** 20,7 M€ in 2020
- **Conditions** d'éligibilité - participation de :

  Au moins 2 opérateurs de l'infrastructure critique choisie, de 2 États membres ou pays associés (pas nécessairement coordinateur)
  L'industrie capable de fournir des solutions de sécurité est nécessaire.

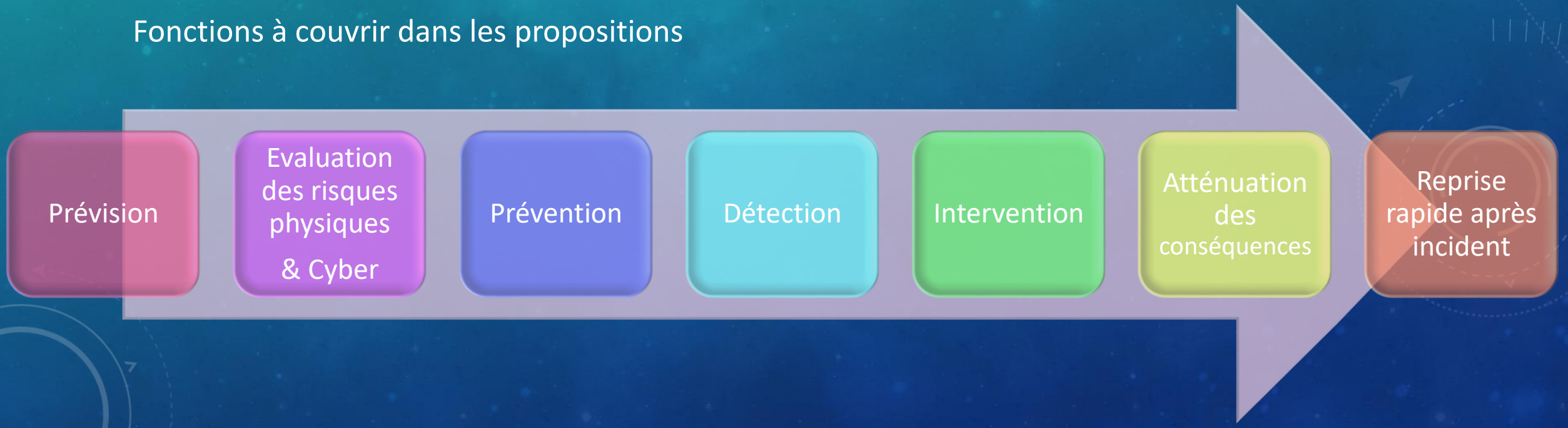
- **Date limite** 27 août 2020
- **Challenge**
  - ❑ Evénements récents montrant l'augmentation des **attaques physiques et cyber combinées** en raison de leurs interdépendances.
  - ❑ Approche **globale, mais spécifique à chaque installation**, est nécessaire pour sécuriser les installations connectées et interdépendantes des usines et systèmes existants ou futurs, publics ou privés.
  - ❑ A cause des contraintes budgétaires les nouvelles solutions de sécurité doivent être plus précises, efficaces et **rentables**, voire plus automatisées que celles qui existent actuellement.

SU-INFRA01-2018-2019-2020 : FONCTIONS A COUVRIR

Pour les infrastructures en étude

- Garantir la sécurité des **installations** (ou de la conception de nouvelles installations),
  pendant toute leur durée de vie
- Assurer la sécurité des **populations voisines** et de l'**environnement**

Fonctions à couvrir dans les propositions



SU-INFRA01-2018-2019-2020 : INTERDÉPENDANCE

A. Fournir une approche pour évaluer en détail tous les aspects de l'interdépendance
   i. Physique, par exemple :
      - Bombardements, sabotages et attaques avec diverses armes contre des installations, des bâtiments et des navires ;
      - Survols et accidents d'avions ou de drones ;
      - Propagation des incendies, inondations, glissements de terrain, conséquences désastreuses du réchauffement planétaire, activités sismiques, météorologie spatiale, menaces combinées, etc.
   ii. Cyber-menaces et incidents
      - Dysfonctionnement du SCADA, accès non autorisé au serveur, interférences électroniques, attaques distribuées, etc.
   iii. Risques en cascade résultant de ces menaces complexes,

B. démontrer l'exactitude de cette approche d'évaluation des risques
   - à l'aide d'exemples et de scénarios précis de la vie réelle
   - en comparant les résultats avec ceux d'autres méthodes d'évaluation des risques

SU-INFRA01-2018-2019-2020 :
GESTION DES MENACES - RECOMMANDATIONS - DÉVELOPPEMENT

C. Mettre au point **un système de gestion en temps réel des menaces physiques et cyber**
   - Tenir compte du vieillissement des infrastructures existantes,
   - Utiliser les meilleures pratiques disponibles basées sur les preuves, les faits, ou sur des données probantes

D. Fournir des scénarios et des recommandations sur la planification stratégique,
   - sur l'engagement de la société civile
   - sur les mesures d'investissement englobant les aspects de la prévention-détection-réponse-atténuation.

E. Proposer des méthodes innovantes pour partager les informations avec le public à proximité des installations
   - y compris par le biais des médias sociaux et avec la participation des organisations de la société civile
   - pour protéger les premiers intervenants tels que les équipes de secours, les équipes de sécurité et les équipes de surveillance, et pour assurer la continuité des services.

C. Développer des outils et des méthodes pour **minimiser les effets en cascade** et permettre une reprise rapide après incident

SU-INFRA01-2018-2019-2020 : LES INFRASTRUCTURES ÉLIGIBLES

- Systèmes d'eau
- Infrastructures énergétiques (centrales et distribution d'énergie, plates-formes offshore)
- Infrastructures de transport (aéroports, ports, chemins de fer, nœuds urbains multimodaux)
- Infrastructures de communication et segments terrestres des systèmes spatiaux
- Services sanitaires
- E-commerce et infrastructure postale,
- Sites et usines industriels sensibles
- Services financiers

Interrelations entre les infrastructures critiques

Ne pas proposer des projets similaires à ceux financés depuis 2016

Chaque année, une liste des infrastructures exclues de l'appel sera publiée
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-infra01-2018-2019-2020

SU-INFRA01-2018-2019-2020 : PARTICIPATION DES PARTIES PRENANTES

Les consortia devraient impliquer le plus grand nombre possible de bénéficiaires concernés, notamment :

- les propriétaires et exploitants d'infrastructures - au moins 2 opérateurs de l'infrastructure critique choisi
- les premiers intervenants,
- l'industrie - la participation de l'industrie capable de fournir des solutions de sécurité est nécessaire

- les technologues et les spécialistes des sciences sociales, etc.
- La participation des PME est fortement encouragée.
- La coopération internationale est encouragée, en particulier avec les partenaires de recherche internationaux dans le cadre du Forum IFAFRI : https://www.internationalresponderforum.org/

SU-INFRA01-2018-2019-2020 : IMPACTS ATTENDUS

Court terme :

- Démonstrations in situ au public le plus large, au-delà des participants au projet

Moyen terme

- Plans de gestion des risques de sécurité intégrant des aspects systémiques, physiques et informatiques.
- Outils, concepts et technologies permettant de lutter contre les menaces physiques et cyber
- Le cas échéant, des bancs d'essais pour les systèmes d'automatisation afin de vérifier la protection cyber et physiques, par rapport aux normes et directives en vigueur.

Long terme

- Convergence des normes de sécurité et de sûreté et établissement préalable de mécanismes de certification
- Interfaces sécurisées et interopérables entre différentes infrastructures critiques pour éviter les effets en cascade
- Contributions aux cadres sectoriels ou aux initiatives réglementaires pertinents