



Sécurité
PCN - Horizon2020



***Appels Horizon 2020 de 2016-2017
Défi 7 - Sécurité***

***Session d'information nationale sur les
appels 2016/2017 Transport et Sécurité
Paris, 20 octobre 2015***

**Armand Nacheff - CEA,
coordinateur du PCN Sécurité français**

Missions des Points de Contact Nationaux



- Trois missions :
 - Informer et sensibiliser sur les opportunités d'Horizon 2020
 - Aider et conseiller aux modalités de fonctionnement du programme (fonction support)
 - Orienter vers les sources de financement les plus pertinentes à chaque projet
- Principe directeur proposé par la Commission Européenne
- Pilotage par le MENESR et les ministères techniques
 - En France, les PCNs sont des consortia

Présentation du consortium des PCNs Sécurité



- **Coordination : CEA**

- Armand Nacheff
- Dominique Sérafin



- **Représentants auprès du comité de programme: MENESR, SGDSN**

- Frédéric Laurent, MENESR
- François Murgadella, SGDSN



- **Pôle Risques - Pégase**

- Jean-Michel Dumaz
- Sébastien Giraud



- **Pôle System@tic**

- Léa Lanaud
- Isabelle de Sutter
- Jean-Pierre Tual - Gemalto



- **Mandaté par la CPU**

- **Université de Rouen** : Philippe Moguerou



- **Conseil des industries de confiance et de sécurité (CICS)**

- Philippe Dejean, Safran



D'autres appuis

- PCN Affaires juridiques et financières
- PCN PME
- PCN Accès au financement
- Réseau Entreprises Europe (EEN)
 - Services de soutien à proximité des P.M.E (Instrument PME, montage de projets, ...)
 - Plus de 600 points de contact

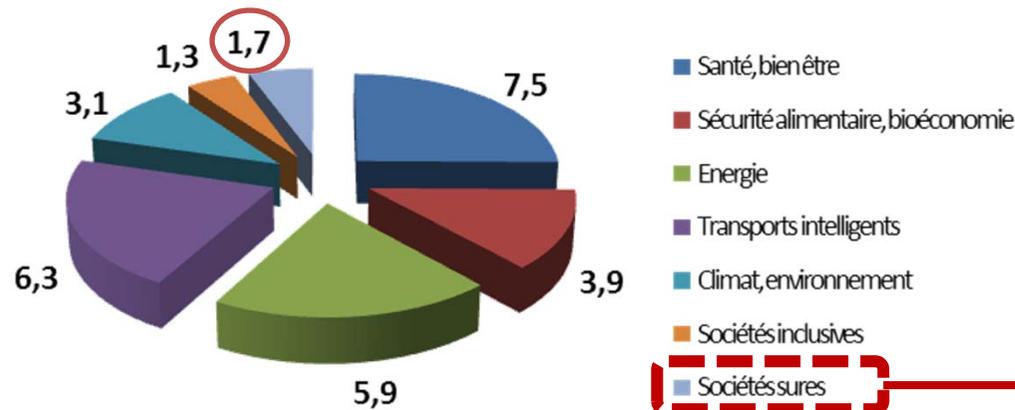


- <http://www.entreprises.gouv.fr/politique-et-enjeux/reseau-entreprise-europe/contacts-regions>

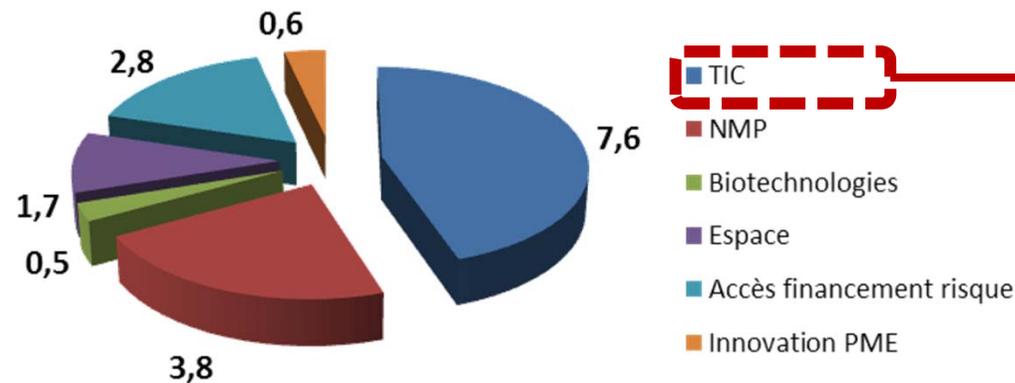
Horizon 2020: Budget de la sécurité



Défis sociétaux (Md€)



Leadership Industriel (Md€)



Orientations principales du Programme de travail Sécurité



- Participation obligatoire des **utilisateurs finaux**
dont les missions incluent :
 - Les spécifications fonctionnelles et la validation de la solution (le **haut du cycle en V**)
 - La **mise à disposition** de composants de démonstrateurs (**locaux, logiciels, systèmes, etc.**)
 - La **quantification des impacts estimés** pour améliorer la sécurité
- Orientation du programme vers des **pilotes** et des **missions de sécurité**
 - Démonstrateurs avec des TRLs généralement élevés (atteignant le niveau 8)
- Prise en compte accrue de la **dimension sociétale**
 - Les SHS doivent être complètement intégrées dans le projet
 - Sociologie des usagers
 - Mécanismes de l'innovation, etc.
- Soutien à l'**industrie** de l'UE pour être **compétitive**
 - Les business plans et les analyse économiques doivent être expliquées

Appels 2016-2017



- **Publiés par la Commission le 14 octobre 2015**
 - http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-transport_en.pdf
- Budget total estimé pour le défi Sécurité :
 - Appels 2016 : 186 M€
 - Appels 2017 : 197 M€
- Calendrier :
 - Echéances de soumission
 - **Variables pour Digital Security (Février, avril et août)**
 - **à 17h le 3^{ième} jeudi du mois d'août** pour les autres appels (CIP, SEC, des DS)

Principaux changements

WP 2016-17 par rapport au WP2014-15 (1/2)



Moins de topiques

- 1 CIP (il y aura 5 projets)
- 5 DRS
- 7 FCT
- 8 BES
- 1 GM
- 8 DS

Total : **30** topiques en 2016-2017 versus 50 en 2014-2015
avec des budgets identiques

- Les **utilisateurs finaux** (practitioners) **cibles sont identifiés**
 - Leur participation est obligatoire

Européénisation de la demande des praticiens

- Le point d'inflexion essentiel dans le programme 2016-17 est :
 - L'«Européénisation» de la demande des utilisateurs finaux pour des solutions innovantes et des offres industrielles d'innovations.
 - 4 nouvelles initiatives stratégiques, avec un budget total de **100M€** (sur les 380M€)
 1. un **CSA destiné aux praticiens de la sécurité pour consolider les besoins** et encourager les investissements publiques et privées :
 - échange des points de vues
 - analyse des lacunes des outils actuels
 - Définition des priorités des futurs axes et efforts de R & D.
 2. Un **CSA pour promouvoir une structuration du tissu industriel** de l'Europe dans le domaine de protection contre les attaques **NRBC**
 3. **3 PCP** de télécom en cas de crise, de système d'information pour soutenir les actions civiles extérieures de l'UE et d'outils pour les laboratoires de médecine légale
 4. IA pour faciliter la synergie nécessaire entre les mondes de la **sécurité "physiques" et numériques pour la protection des infrastructures critiques**

Thèmes des appels 2016-2017



CIP

- Water Systems
- Energy Infrastructure (power plants and distribution)
- Transport Infrastructure and means of transportation
- Communication Infrastructure
- Health Services
- Financial Services

SEC-DRS

- Integrated tools for risk mgt and disaster resilience (natural, accidental, or intentional)
- Situational awareness systems
- Toxins measurement
- CBRN cluster
- Broadband Comm. Systems

SEC-FCT

- Violent radicalization protection
- Prevention Investigation Mitigation
- Forensics Trace, DNA Toolkits
- Explosive detection
- Detection and data fusion (in sewage networks, air quality monitoring systems, ...)

SEC-BES

- Reducing cost in land border security
- Data fusion for maritime security
- control systems border security
- Information systems to support EU external policy
- Risk-based screening border crossing
- Through-foliage detection
- Big Data for customs
- no gate crossing point solutions

DS

- Assurance certification
- Cybersecurity for SMEs
- Health data security
- Economics of cyber security
- Cryptography
- Advanced threats
- Privacy, data protection
- EU cooperation



CIP



CIP topics – 2016-2017



Topic (Type of Action)	Budget (M€)	Deadline	Title
CIP-01-2016-2017 (IA)	20.0	25 / 08 / 2016	Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe
CIP-01-2016-2017 (IA)	20.0	24 / 08 / 2017	

Budget total = 40M€

transports

Un projet concernera les transports et moyens de transportation

Appel CIP – ce qui est demandé



- Assurer la sécurité et la résilience de toutes les fonctions exercées par les installations, les populations voisines et l'environnement
 - prévention, détection, réaction
 - en cas d'échec, atténuation des conséquences

- 1. Prise en compte **des menaces et incidents cyber et des attaques physiques**
 - par exemple bombardement, survols ou crash d'avion ou de drone, propagation des incendies, inondations, activité sismique, radiations de l'espace, etc.)

- 2. Prise en compte
 - de la gestion systémique de la sécurité,
 - des combinaisons de menaces physiques et cyber,
 - de leurs interconnexions et leurs effets en cascade

- 3. Prise en compte
 - Du partage de l'information avec le public dans le voisinage des installations,
 - de la protection des équipes de secours, de sécurité et des surveillance

Critical Infrastructure Protection (CIP)



- **CIP 01 – 2016 et 2017**

DG CNECT + DG Home

Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.

- Type d'action: **IA**
- TRL à l'issue des projets : **7**
- Budget par projets : **~8 M€/projet**
- Budget total de l'action : **20 M€/an**
- soit 2 à 3 par an
- Spécificités:
 - 1 seul projet par Infrastructure Critique (IC) sur l'ensemble de la période 2016-17
 - **Au moins 2 opérateurs d'IC partenaires**
 - Implication de l'industrie (et de PME) obligatoire
- ICs:
 1. *Water Systems,*
 2. *Energy Infrastructure (power plants and distribution),*
 3. ***Transport Infrastructure and means of transportation,***
 4. *Communication Infrastructure,*
 5. *Health Services,*
 6. *Financial Services.*

Sujet Protection du transport aérien éligible



BES



BES topics – 2016-2017



transports
transports

Topic (Type of Action)	Budget (M €)	Deadline	Title
~T SEC-14-BES-2016 (RIA)	10.0	25 / 08 / 2016	Reducing technology cost: land border security
SEC-19-BES-2016 (IA)	24.0	25 / 08 / 2016	Data fusion for maritime security applications
SEC-20-BES-2016 (IA)		25 / 08 / 2016	Border Security: autonomous systems
SEC-13-BES-2017 (PCP)	10.0	24 / 08 / 2017	Information System for the EU external policy
~T SEC-15-BES-2017 (IA)	8.0	24 / 08 / 2017	Risk-based screening at border crossing
SEC-16-BES-2017 (RIA)	8.0	24 / 08 / 2017	Through-foliage detection
~T SEC-17-BES-2017 (RIA)	10.0	24 / 08 / 2017	Big data and data analytics for customs
~T SEC-18-BES-2017 (RIA)	6.0	24 / 08 / 2017	Acceptance of "no gate crossing point solutions"

Budget total = 42 M€

Border Security (SEC-13-BES)



- SEC-13-BES-2017:

Next generation of information systems to support EU external policies

Soutenir le développement d'une plateforme de surveillance, d'échange d'informations et de contrôle des opérations pour les missions extérieures

- Type d'action: **PCP**
- TRL à l'issue des projets : **8**
- Budget par projets : **10 M€/projetxx**
- Budget total : **10 M€**
- 1 projet

- Coordination avec European Defence Agency (EDA)
- au moins 3 end-users de 3 EM,
- Règles d'IPR additionnelles

Border Security (SEC-14-BES)



- SEC-14-BES-2016:
Towards reducing the cost of technologies in land border security applications

La réduction des coût peut être le résultat d'une intégration de plusieurs technologies, de la mise en place de solutions portables, de la conception de plates-formes informatiques plus homogènes, de le partage d'une interface commune à toutes les bases de données opérationnelles, etc.

- Type d'action: **RIA**
- TRL à l'issue des projets : **6**
- Budget par projets : **5 M€/projet**
- Budget total : **10 M€**
- Maximum 2 projets financés

- Coordination avec European Defence Agency (EDA)

- Au moins 3 autorités de contrôle des frontières de l'UE ou 3 membres de Schengen
- Les Etats doivent être les bénéficiaires de la convention de subvention.
- Eviter que la proposition empiète sur le travail fait dans le cadre du projet FP7 EWISA:
http://cordis.europa.eu/project/rcn/192052_en.html

Border Security (SEC-15-BES)



- SEC-15-BES-2017:
Risk-based screening at border crossing

*Contrôler moins de biens et d'individus
en sélectionnant sur la base des risques des flux*

- Type d'action: **IA**
- TRL à l'issue des projets : **7**
- Budget par projets : **8 M€/projet**
- Budget total : **8 M€**
- un seul projet financé

- Au moins 3 autorités de contrôle des frontières ou autorités douanières de l'UE
ou 3 États membres de Schengen

Border Security (SEC-16-BES)



- SEC-16-BES-2017:
Through-foliage detection, including in the outermost regions of the EU

Les technologies de surveillance, de détection, de suivi et d'identification des personnes et des véhicules traversant la frontière dans les régions forestières restent très immatures. Le flux croissant d'immigration irrégulière à travers la frontière de, par exemple, la Turquie, l'Ukraine, la Biélorussie, la Russie ou le Brésil rend la question encore plus critique que dans le passé.

- Type d'action: **RIA**
- TRL à l'issue des projets : **5 ou 6**
- Budget par projets : **8 M€/projet**
- Budget total : **8 M€**
- max. 1 projet

- Coordination avec European Defence Agency (EDA)
- 3 end-users de 3 EM

Border Security (SEC-17-BES)



- SEC-17-BES-2017:

Architectures and organizations, big data and data analytics for customs risk management of the international goods supply chain trade movements

Tout en facilitant le commerce légitime, une gestion efficace des risques dans la chaîne d'approvisionnement internationale est essentielle pour assurer la sécurité et sûreté des résidents de l'UE et pour protéger les intérêts financiers et économiques de l'UE.

Améliorer la gestion par les douanes des risques et de la sécurité de la chaîne d'approvisionnement.

Afin de rendre les contrôles plus efficaces, nécessité pour la douane et d'autres autorités

- *d'acquérir des données de qualité sur les mouvements de la chaîne d'approvisionnement*
- *et de les exploiter*

- Type d'action: **RIA**
- TRL à l'issue des projets : **non spécifié**
- Budget par projets : **5 M€/projet**
- Budget total : **10 M€**
- 3 end-users de 3 EM

Border Security (SEC-18-BES)



- SEC-18-BES-2017:
Acceptance of "no gate crossing point solutions"

Pour le voyageur, il serait idéal de traverser les frontières sans être ralenti.

Grâce à une grande variété de technologies, de systèmes, de réseaux de capteurs et de méthodes d'évaluation des risques, il est probable que dans les 10 prochaines années la traversée des frontières d'une manière transparente deviendra possible.

Les contrôles seront ainsi effectués aux frontières ou à n'importe quel endroit d'une manière mobile afin de vérifier les données des voyageurs tout au long leurs voyages.

L'utilisation intensive de ces techniques peut porter atteinte la vie privée. Donc, l'acceptation sociale et politique de ces techniques est nécessaire avant leur mise en œuvre.

- Type d'action: **RIA**
- TRL à l'issue des projets : **non spécifié**
- Budget par projets : **3 M€/projet**
- Budget total : **6 M€**
- max. 2 projets
- 3 end-users de 3 EM

Border Security (SEC-19-BES)



- SEC-19-BES-2016:
Data fusion for maritime security applications

Le but est de traiter des données pour en produire d'autres de qualité supérieure pour le domaine maritime. Les données traitées peuvent être :

- *des données homogènes ;*
- *des données brutes et hétérogènes venant de capteurs, radars, caméras, satellites, ...*
- *des images se chevauchant produites par plusieurs sources*
- *des données en temps réel ou venant de sources non connectées, etc.*

- Type d'action: **IA**
- TRL à l'issue des projets : **7**
- Budget par projets : **8 M€/projet**

- Coordination avec European Defence Agency (EDA)

- Au moins 3 autorités de contrôle des frontières de 3 États membres ou associés.
- Au moins 3 organisations de l'industrie indépendantes établies dans 3 pays différents.

Border Security (SEC-20-BES)



- SEC-20-BES-2016:
Border Security: autonomous systems and control systems

*La surveillance des frontières et des régions inhabitées est plus efficace quand les drones et véhicules sans pilote deviennent des **agents autonomes à grande endurance, capables de fonctionner dans des environnements complexes.***

*Un **système de contrôle utilisant des technologies de graphique 3D avancées** sera nécessaire pour représenter fidèlement la position des objets externes et des objets de surveillance incluant les agents autonomes.*

La proposition doit couvrir un des deux sujets:

- **La surveillance autonome**
- **Système de contrôle en 3D**

- Type d'action: **IA**
- TRL à l'issue des projets : **6-7**
- Budget par projets : **8 M€/projet**
- Practitioners y compris les autorités de la police des frontières de 5 États membres ou de Shengen
- Participation des PME obligatoire



DRS



DRS topics – 2016-2017



Topic (Type of Action)	Budget (M€)	Deadline	Title
~T SEC-01-DRS-2016 (IA)	8.0	25 / 08 / 2016	Integrated tools for response planning
SEC-02-DRS-2016 (CSA)	1.5	25 / 08 / 2016	Situational awareness systems to decision making
SEC-03-DRS-2016 (IA)	8.0	25 / 08 / 2016	Biological toxins measurements
SEC-05-DRS-2016-2017 (CSA)	2.0	25 / 08 / 2016	CBRN cluster
SEC-04-DRS-2017 (PCP)	10.0	24 / 08 / 2017	Broadband communication systems
SEC-05-DRS-2016-2017 (RIA)	14.0	24 / 08 / 2017	CBRN cluster

Budget total = 43.5 M€

Disaster-Resilience (SEC-01-DRS)



- SEC-01-DRS-2016:
***Integrated** tools for response planning and scenario building*

Outils intégrés pour la planification des interventions, l'élaboration des scénarii et la mise en situation

- Type d'action: **IA**
- TRL à l'issue des projets : **7-8**
- Budget par projets : **~ 8 M€/projet**
- Budget total de l'action : **8 M€**
- Très probablement 1 seul projet financé -- max 2 projets

- **Participation obligatoire d'au moins une entité de chacune des 5 catégories de premiers intervenants suivantes :**
 - **firefighting units,**
 - **medical emergency services,**
 - **police departments,**
 - **civil protection units,**
 - **control command centres**

- Participation obligatoire de PME

Disaster-Resilience (SEC-02-DRS)



- SEC-02-DRS-2016:
CSA on situational awareness systems to support civil protection preparation and operational decision making

Préparation des spécifications du centre de surveillance, d'appréciation de la situation et de commandement de l'action d'aide d'urgence
(C'est DRS-5-2014 qui n'a pas eu de projet)

- Type d'action: **CSA**
 - Budget par projets : **1,5 M€**
 - Budget total de l'action : **1,5 M€**
 - 1 projet financé
- L'UE peut contribuer à des actions ultérieures (PCP, PPI, ...) pour lancer des appels d'offres afin de rendre disponibles des prototypes d'un tel système
 - Des règles additionnelles de propriété intellectuelle sont demandées :
 - Engagement à fournir des licences raisonnables et non discriminatoires (FRAND)

Disaster-Resilience (SEC-03-DRS)



- SEC-03-DRS-2016:
Validation of biological toxins measurements after an incident: Development of tools and procedures for quality control

*Concerne les menaces de bioterrorisme (le B du NRBC)
développer une approche à l'échelle européenne pour améliorer la maîtrise et la validation des mesures de toxines biologiques (comme ce qui a été fait dans le cas des menaces chimiques)*

- Type d'action: **IA**
- TRL à l'issue des projets : **non spécifié**
- Budget par projets : **8 M€/projet**
- Budget total de l'action : **8 M€**
- 1 projet financé

- **au moins 3 laboratoires de contrôle doivent participer au projet**

Disaster-Resilience (SEC-04-DRS)



- SEC-04-DRS-2017:
PCP for broadband communication systems

*Chaque État membre a aujourd'hui son propre système de radiocommunication large bande, pour ses forces de sécurité (police, premiers intervenants, etc.)
Ce topique est la suite de DRS-18-2015 (qui est une CSA) et sera donc modifié dans la mise à jour du programme de travail 2017 suivant les exigences du projet CSA sélectionné.*

- Type d'action: **PCP**
- TRL à l'issue des projets : **8**
- Budget par projets : **10 M€/projet**
- Budget total de l'action : **10 M€**
- un seul projet réunissant **au moins 8 ou 12 Etats Membres ou Pays Associés**
- Règles additionnelles de propriété intellectuelle

Disaster-Resilience (SEC-05-DRS)



SEC-05-DRS-2016-17:
CBRN cluster

pour promouvoir la synergie entre PME développant des technos NRBC

Part a) 2016:

- Fournir une plateforme intégrant des technologies NRBC ainsi qu'une interface avec les institutions financières incluant le nouvel instrument InnovFin pour aider à financer les entreprises innovantes.
- Fournir un catalogues de technologies nécessaires à être développées
- Connaître les résultats du projet FP7 EDEN: <https://www.eden-security-fp7.eu/> (de 1/9/2013 au 31/8/2016)

- Type d'action: **CSA**
- Budget par projets : **2 M€/projet**
- Budget total de l'action : **2 M€**
- 1 projet financé

Part b) 2017:

- Développer des technologies NRBC identifiée dans le catalogue du CSA

- Type d'action: **RIA**
- TRL à l'issue des projets : **4 à 8**
- Budget par projets : **~3,5 M€/projet**
- Budget total de l'action : **14 M€**
- 4 projets financés
- Chaque projet RIA doit être coordonné par une PME
- Les bénéficiaires des les projets RIA doivent être indépendants des bénéficiaires du projet CSA

FCT topics – 2016-2017



Topic (Type of Action)	Budget (M€)	Deadline	Title
SEC-06-FCT-2016 (RIA)	17.0	25 / 08 / 2016	violent radicalization protection
~ T SEC-07-FCT-2016-2017 (RIA)		25 / 08 / 2016	Human Factor to mitigate terrorist acts
SEC-08-FCT-2016 (RIA)	27.25	25 / 08 / 2016	Forensics a) trace qualification, b) DNA use
~ T SEC-11-FCT-2016 (RIA)		25 / 08 / 2016	Detection techniques on explosives
~ T SEC-12-FCT-2016-2017 (RIA)		25 / 08 / 2016	Prevention, investigation, and risk mitigation
SEC-07-FCT-2016-2017 (RIA)	6.0	24 / 08 / 2017	Human Factor to mitigate terrorist acts
SEC-09-FCT-2017 (PCP)	10.0	24 / 08 / 2017	Tools and techniques for forensic laboratories
SEC-10-FCT-2017 (IA)	16.0	24 / 08 / 2017	Integration of detection capabilities and data fusion with utility providers'
~ T SEC-12-FCT-2016-2017 (RIA)	10.0	24 / 08 / 2017	Prevention, investigation, and risk mitigation

Budget total = 86 M€

Fight against terrorism (SEC-06-FCT)



- SEC-06-FCT-2016:

Developing a comprehensive approach to violent radicalization in the EU from early understanding to improving protection

Les racines de la radicalisation ne sont pas bien connues. La compréhension de ce qui motive le processus de radicalisation et de la réaction des individus aux contre-mesures prises pour faire face à ce phénomène, est nécessaire pour apporter une réponse ciblée.

- Type d'action: **RIA**
- TRL à l'issue des projets : **non spécifié**
- Budget par projets : **3 M€/projet**
- **Agences repressives (LEA) d'au moins 5 Etats Membres ou Associés**

Fight against terrorism (SEC-07-FCT)

- SEC-07-FCT-2016-2017:

Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts

5 sous-sujets (1 proposition adresse 1 et 1 seul sous-sujet) pour se protéger contre

- 1. *Le mouvement de foules lors de rassemblements de masse***
- 2. Les comportements cybercriminels*
- 3. *La corruption et la criminalité financière***
- 4. La petite délinquance à incidence élevée*
- 5. La violence familiale*

- Type d'action: **RIA**
- TRL à l'issue des projets : **non spécifié**
- Budget par projets : **3 M€/projet**
- 1 projet financé au maximum par sous-sujet

- **Seulement les projets non couverts en 2016 sont éligibles pour 2017**
- **Participation de le Police Technique et Scientifique (forensics lab) d'au moins 5 Etats Membres ou Associés**
- **Work package pour un démonstrateur, obligatoire dans la proposition**

Fight against terrorism (SEC-08-FCT)



- SEC-08-FCT-2016:

Forensics techniques on: a) trace qualification, and b) broadened use of DNA

Les propositions portant sur a) devraient contribuer à une meilleure identification et compréhension des traces liées à la criminalité et les activités qui ont conduit à la déposition de ces traces

Les propositions portant sur b) devraient contribuer à l'amélioration de la capacité à obtenir des informations fiables à partir d'échantillons d'ADN.

- Type d'action: **RIA**
- TRL à l'issue des projets : **5**
- Budget par projets : **5 M€/projet**

- **Participation de le Police Technique et Scientifique (forensics lab) d'au moins 5 Etats Membres**

Fight against terrorism (SEC-09-FCT)



- SEC-09-FCT-2016:

Toolkits integrating tools and techniques for forensic laboratories

4 phases définis

- Type d'action: **PCP**
- TRL à l'issue des projets : **8**
- Budget par projets : **10 M€/projet**
- 1 projet financé

- Des forensics labs ou instituts de 5 Etats Membres ou organisations internationales doivent participer
- Des règles additionnelles de propriété intellectuelle sont demandées

Fight against terrorism (SEC-10-FCT)

- SEC-10-FCT-2016:
Integration of detection capabilities and data fusion with utility providers' networks

Détection de précurseurs d'explosifs et de produits chimiques illicites (drogues) dans les systèmes d'égout

- Type d'action: **IA**
- TRL à l'issue des projets : **7-8 sur les capteurs**
6 sur les SI et plateforme mobile
- Budget par projets : **8 M€/projet**
- Maximum 2 projets financés
- Coordination avec European Defence Agency (EDA)
- au moins 2 opérateurs et 3 unités contre le terrorisme ou démineurs de 3 Etats Membres
- Démonstration dans au moins 2 villes (1 ville de plus d'1 million habitants et une autre ayant entre 100 et 300 mille habitants) de 2 EM utilisant des systèmes d'égouts différents

Fight against terrorism (SEC-11-FCT)



- SEC-11-FCT-2016:

Detection techniques on explosives: Countering an explosive threat, across the timeline of a plot

Les méthodes et techniques à prendre en considération comprennent:

- 1. Le repérage de ceux qui se préparent pour une attaque*
- 2. L'inhibition de précurseurs chimiques*
- 3. La détection de produits chimiques spécifiques, fabriques de bombes, et / ou engins explosifs improvisés*
- 4. Neutralisation des engins explosifs improvisés (IED)*
- 5. Identification de la faiblesse des défenses actuelles contre les IED, et possible améliorations*

Pas de développement technologique, mais plutôt un renforcement de la recherche opérationnelle

- Type d'action: **RIA**
- TRL à l'issue des projets : **non spécifié**
- Budget par projets : **5M€/projet**

- Coordination avec European Defence Agency (EDA)
- au moins 3 unités anti-terroristes de 3 Etats Membres

Fight against terrorism (SEC-12-FCT)



- SEC-12-FCT-2016-2017:

Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism

4 sous-sujets (1 proposition adresse 1 et 1 seul sous-sujet) pour se protéger contre

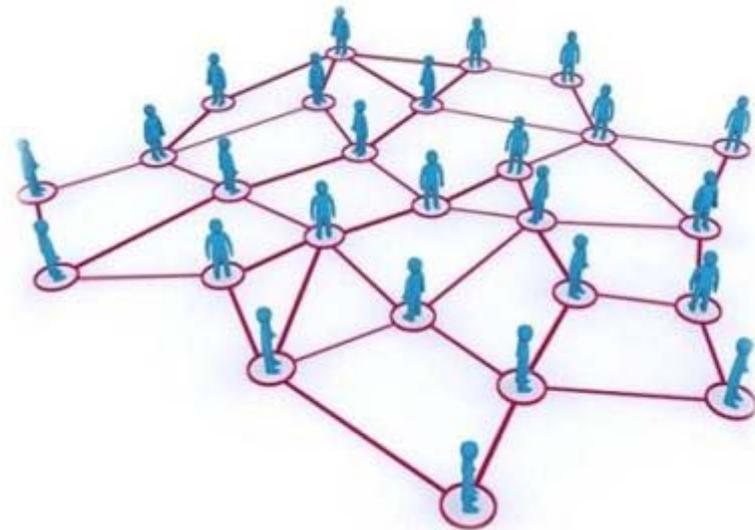
- 1. Cybercriminalité: monnaies virtuelles, de-anonymisation, traçage, ... dans le darknet (web caché)*
- 2. Détection et neutralisation des drones légers suspects*
- 3. Analyse vidéo pour l'enquête juridique*
- 4. Autres*

- Type d'action: **RIA**
- TRL à l'issue des projets : **6**
- Budget par projets : **5 M€/projet**
- 1 projet financé au maximum par sous-sujet

- au moins 3 **Agences Repressives** (LEA) de 3 EM (1,2,3) ou 5 LEA de 5 EM (4),
- pas de technologies de détection
- démonstrations obligatoires



GM



General Matters (GM)



- SEC-21-GM-2016-2017:
Pan European Networks of practitioners and other actors in the field of security
 - a. De même discipline
 - ✓ pompiers, intelligence, gardes frontières, douanes, spécialistes explosives, PST, forensiques, urgences médicales, think-tanks, ...
 - b. De différentes disciplines sur un secteur géographique
 - ✓ Région méditerranée, Cercle arctique et Atlantique du Nord, bassin du Danube, région de la baltique
 - c. Gestionnaire de sites de tests, de simulations, de démonstrations et de formations
 - d. PCN en 2017
 - **CSA, 15,5 M€ (2016) + 14 M€ (2017)**
 - end-users d'au moins 8 EM

SMEInst-13-2016-2017:

Engaging SMEs in security research and development



7.1. *Fighting crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs*

7.2. *Protecting and improving the resilience of critical infrastructures, supply chains and transport modes*

7.3. *Strengthening security through border management*

7.4. *Improving cyber security*

7.5. *Increasing Europe's resilience to crises and disasters*

7.6. *Ensuring privacy and freedom, including in the Internet, and enhancing the societal legal and ethical understanding of all areas of security, risk and management*

7.7. *Enhancing standardisation and interoperability of systems, including for emergency purposes*

7.8. *Supporting the Union's external security policies, including through conflict prevention and peace-building*

30 M€

- *Fast Track for Innovation - Pilot*
 - **FTI**



DS



DS



Topic (Type of Action)	Budget (M€)	Deadline	Title
DS-03-2016 (RIA)	11.0	16 Feb 2016	Digital security of health related data on a systemic level
DS-01-2016 (RIA)	13.5	12 Apr 2016	Assurance and Certification for Trustworthy and Secure ICT
DS-01-2016 (IA)	9.0	12 Apr 2016	
DS-01-2016 (CSA)	1.0	12 Apr 2016	
DS-02-2016 (IA)	22.0	25 Aug 2016	Cyber Security for SMEs
DS-04-2016 (RIA)	4.0	25 Aug 2016	Economics of Cybersecurity
DS-05-2016 (CSA)	3.0	25 Aug 2016	EU Cooperation and International Dialogues
DS-06-2017 (RIA)	18.5	25 Apr 2017	Cryptography
DS-07-2017 (RIA)	10.0	24 Aug 2017	Addressing Advanced Cyber Security Threats and Threat Actors
DS-07-2017 (IA)	8.0	24 Aug 2017	
DS-08-2017 (IA)	18.0	24 Aug 2017	Privacy, Data Protection, Digital Identities

transports

transports

transports

Digital Security (DS-01)



- DS-01-2016:

Assurance and Certification for Trustworthy and Secure ICT systems, services and components

Les systèmes cyber-physique évoluent dans un environnement complexe et dynamique, La sûreté de fonctionnement de ces systèmes critiques doit prendre en considération des systèmes non connus ou en cours de développement.

-

Dans beaucoup de systèmes

la sécurité devient profondément inter mêlée à leur sûreté de fonctionnement et au privacy.

Les défis s'intensifient

- *par l'utilisation de composants venant de parties tierces,*
- *par la forte croissances de l'internet des objets*
- *et par le déploiements d'architectures décentralisées et virtuelles.*

- *Pour faire face à ces défis, il est nécessaire de développer des méthodologie d'assurance sécurité appropriées avec des niveaux certifiés.*

– Date limite :

12 Avril 2016

Digital Security (DS-01-a)

Deadline : 12 avril 2016



- **DS-01-2016 -RIA:**

Assurance and Certification for Trustworthy and Secure ICT systems, services and components

Proposals may address security, reliability and safety assurance at individual phases of the System development Life Cycle (SDLC) and are expected to cover at least one of the areas identified below:

1. *Security requirements specification and formalization;*
2. *Security properties formal verification and proofs at design and runtime*
3. *Secure software coding;*
4. *Assurance-aware modular or distributed architecting and algorithmic;*
5. *Software code review, static and dynamic security testing;*
6. *Automated tools for system validation and testing;*
7. *Attack and threat modelling;*
8. *Vulnerability analysis;*
9. *Vendor (third-party) application security testing;*
10. *Penetration testing;*
11. *Collection and management of evidence for assessing security and trustworthiness;*
12. *Operational assurance, verification and security policy enforcement;*
13. *Adaptive security by design and during operation.*

- Type d'action: **RIA**
- TRL à l'issue des projets : **3 à 5**
- Budget par projets : **entre 3 et 4 M€ par projet**
- Budget total (a) : **13,5 M€**

Digital Security (DS-01-b)



Deadline : 12 avril 2016

- **DS-01-2016 - IA:**

Assurance and Certification for Trustworthy and Secure ICT systems, services and components

*Les propositions peuvent porter sur tout domaine et doivent adresser l'**amélioration des processus de certification de sécurité existants** pour les composants et produits TIC, de points de vue efficacité et efficience.*

En termes d'efficacité, les propositions doivent aborder les menaces émergents et la certification compositionnelle du système.

En termes d'efficacité, les propositions devraient viser à réduire le coût et la durée du processus de certification.

- Type d'action: **IA**
- TRL à l'issue des projets : **6 à 7**
- Budget par projets : **entre 3 et 4 M€ par projet**
- Budget total (b) : **9 M€**
- 2 à 3 projets

Digital Security (DS-01-c)

Deadline : 12 avril 2016



- **DS-01-2016 - CSA:**

Assurance and Certification for Trustworthy and Secure ICT systems, services and components

Should address the following:

A. *Building trustworthiness: economic, legal and social aspects of security assurance and certification*

1. *Study in depth the economic and legal aspects related to assurance and certification (including **European-wide labelling**), EU and International regulatory aspects;*
2. *Explore and identify the interplay of relevant social, cultural, behavioural, gender and ethical **factors** with ICT systems with regards **to their trustworthiness and security, actual or perceived***
3. *Identify **barriers and incentives** in the market for certified products in the consumer and/or enterprise market;*
4. *Produce a **comprehensive cost/benefit model for security assurance and certification**;*

B. *Engage with multidisciplinary communities and stakeholders.*

- Type d'action: **CSA**
- Budget par projets : **1 M€ par projet**
- Budget total (c) : **1 M€**
- 1 projet

Digital Security (DS-02)

- DS-02-2016:

Cyber Security for A) SMEs, B) local public administration and C) Individuals

A, B et C subissent des menaces et des attaques de cyber sécurité.

La majorité des solutions de cyber sécurité n'ont pas été conçues pour eux.

Les contraintes budgétaires les empêchent d'investir.

Les individus doivent constamment adapter leur comportement pour éviter les pièges.

Les propositions doivent

- adresser 1 des trois besoins : A, B ou C
- développer des solutions avec un **haut degré de convivialité et d'automatisation**
- répondre aux besoins spécifiques de **l'utilisateur final**
- valider le travail par le biais des commentaires de **l'utilisateur final** et de sa participation

- Type d'action: **IA**
- TRL à l'issue des projets : **6 à 7**
- Budget par projets : **entre 3 et 4 M€ par projet**
- Budget total : **22 M€**



Digital Security (DS-03)

Deadline : 16 Février 2016

- DS-03-2016:

Increasing digital security of health related data on a systemic level

Pour obtenir la confiance des utilisateurs informatiques dans le domaine de la santé, des mesures de sécurité doivent être prises en considération, conformément à l'approche "privacy by design". Cela nécessite le stockage sécurisé des données personnelles et un échange sécurisé de ces données empêchant la perte des données, les cyber-attaques et tout accès non autorisé. Une approche systémique de la sécurité augmentera les autorisations informatiques des patients, aidera à protéger leur données de santé y compris à l'étranger, et peut-être encouragera un grand nombre d'États membres à l'appliquer et à adapter leurs législations nationales.

Les propositions doivent offrir une approche holistique pour aborder les défis de stockage sécurisé et des échanges (y compris transfrontaliers) des données de la santé

- Type d'action: **RIA**
- TRL à l'issue des projets : **3 à 5**
- Budget par projets : **entre 3 et 5 M€ par projet**
- Budget total : **11 M€**
- 2 à 3 projets

Digital Security (DS-04)



- DS-04-2016:
Economics of Cybersecurity

Des analyses sociétales, institutionnelles et économiques sont nécessaires pour comprendre les échecs en cyber sécurité.
Les structures institutionnelles ou les cadres d'incitations ne couvrent pas adéquatement les menaces cyber.

Les propositions doivent couvrir un des deux volets:

- A. Un cadre des coûts-avantages de la cyber sécurité (investissement optimal)
- B. Des modèles d'affaires et d'incitations

Avec une approche multidisciplinaire combinant

- des idées économiques, comportementaux, sociaux et d'ingénierie,
- des méthodes de mesure et de méthodologies de microéconomie, d'économétrie, de sciences sociales qualitatives, de sciences du comportement, de prise de décision, de gestion des risques et d'économie expérimentale

- Type d'action: **RIA**
- TRL à l'issue des projets : **non spécifié**
- Budget par projets : **entre 1 et 2 M€ par projet**
- Budget total : **4 M€**

Digital Security (DS-05)



- DS-05-2016:
EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation

Des échanges de points de vue et une vue d'ensemble des activités en cyber sécurité sont nécessaires pour déterminer le futur paysage mondial de la cyber sécurité et pour maximiser la synergie entre H2020 et les efforts cyber sécurité de l'UE, des états membres et des clusters régionaux

3 sous-sujets:

1. Les synergies entre H2020 et les activités de l'UE et des clusters
2. Le dialogue international avec le Japon
3. Le dialogue international avec les USA

- Type d'action: **CSA**
- Budget par projets : **2 M€ pour 1) et 0.5 M€ pour 2) et 3)**
- Budget total : **3 M€**

Digital Security (DS-06) (1/2)



- DS-06-2017:
Cryptography
- *Adresse la majorité des sujets de cryptographie : encryption, authentication, Internet des objets et privacy, crypto quantique, preuves, protocoles, etc.*
 - Type d'action: **RIA**
 - TRL à l'issue des projets : **entre 3 et 5**
 - Budget par projets : **entre 3 et 5 M€**
 - Budget total : **18,5 M€**

Digital Security (DS-06) (2/2)

Les sujets DS-06-2017 *Cryptography*



- Functional encryption solutions **beyond the current only partial homomorphic encryption algorithms** under development
- Measurement of information leaked when allowing for flexibility and preserving data formats (e.g., **anonymization or obfuscation**)
- **Ultra-lightweight cryptology** for the Internet of Things Additional means to protect privacy (e.g. anonymity in communications)
- **Ultra-high-speed cryptographic algorithms that are fully parallelizable and energy efficient** as well as high speed encryption applied directly to the physical layer, for example using **quantum cryptograph**.
- **Security of the implementation and its validation:** implementation (hardware or software) is often the weak point of the strongest cryptographic protocols: **physical cryptanalysis, including tampering, side channel, faults injection attacks**.
- More progress in the development of toolkits that integrate encryption seamless in their **toolbox environment**.
- Authenticated encrypted token research for **mobile payment solutions** and related applications. The proposals should aim to create a real e-currency without compromising security or opening doors for criminals.
- Innovative cryptographic primitives and complementary non-cryptographic **privacy-preserving mechanisms** to enforce privacy at various levels (e.g. pairing based cryptography).
- New techniques, such as **quantum safe cryptography**, which are secure from quantum computers.
- Proposals on **quantum key distribution** addressing challenges such as improved performance (higher bit rates, increased loss and noise resilience), network integration (coexistence on existing infrastructure) and the development of new protocols beyond key distribution.
- **Automated proof techniques** for cryptographic protocols



Digital Security (DS-07 - A)

- DS-07-2017 - RIA:

Addressing Advanced Cyber Security Threats and Threat Actors

- Les cyber-attaques sont devenues plus sophistiquées, furtives, ciblées et à multi-facettes qui peuvent tirer parti des vulnérabilités zero-day et de méthodes d'attaque interdisciplinaires hautement créatifs.
- La détection et la réponse à ces attaques par des hackers bien qualifiés ont été avérées très difficiles.
- De nouvelles technologies sont nécessaires pour accroître nos capacités de détection et d'intervention.

- A) Appréciation de la situation

- développement d'approches pour détecter et répondre rapidement aux cyber-attaques
- recherche interdisciplinaire et techniques telles que la **détection des anomalies**, les outils de **visualisation**, l'analyse big data, l'analyse de la **menace**, l'inspection des **paquets de communication**, l'analyse de protocole, etc.
- Recueil **des informations légales (forensics)**
- garanti des droits fondamentaux, de la protection des données et de la vie privée, pendant la conception et développement des solutions

Impact attendu

- Amélioration des technologies et processus pour détecter et répondre aux attaques avancées

- **RIA, 2-3 M€ / projet, TRL 3-5, budget de 10 M**



Digital Security (DS-07 - B)

DS-07-2017 - IA:

B) Environnements de simulation et Formation

Développement des environnements de simulation innovants et des matériels de formation afin de préparer adéquatement les personnes chargées de la défense des organisations à haut risque pour contrer les cyber-attaques avancées :

- Outils pour créer des environnements réalistes pour la formation comme la production d'événements système bénignes et malveillants;
 - Evaluation des performances des élèves en temps réel
 - Configuration et adaptation dynamique du niveau de difficulté des exercices
 - Contrôle de la progression dans l'exercice, détecter des incohérences
 - Définition et création de nouveaux scénarios de cyber-menaces
-
- **IA: 4-5 M€ / projet, TRL 5-7, budget de 10 M€**

Digital Security (DS-08)



- DS-08-2017

Privacy, Data Protection, Digital Identities

- *Des données personnelles des utilisateurs sont souvent divulgués aux services. E.g. les mots recherchés sur des moteurs de recherche laissent des traces sensibles.*
- *La mise en œuvre du draft sur le règlement général des données présente des défis à la fois technologiques et organisationnels pour implémenter des mécanismes comme*
 - *la portabilité des données,*
 - *le droit à l'oubli,*
 - *les évaluations de l'impact de la protection des données*
 - *et les principes de responsabilité 'accountability'.*
- *De nombreux services sur Internet dépendent de la disponibilité des identités numériques sécurisées.*
 - *De nombreux pays européens ont ou sont en train de développer des services d'identité électronique*
 - *La plupart de ces projets sont conçus pour avoir un niveau de sécurité très élevé mais manquent de convivialité pour des applications commerciales.*

Digital Security (DS-08 - bis)



- DS-08-2017
Privacy, Data Protection, Digital Identities
- Les propositions doivent couvrir un des sujets suivants
 - i. *Technologies d'amélioration de la vie privée*
 - *Conception et outils pour permettre aux utilisateurs d'exposer le minimum d'information possible et de ne pas perdre le contrôle de leurs données*
 - *Cadre de gestion des risques relatifs à la vie privée, par exemple aider les particuliers à comprendre ce qui arrive à leurs données quand ils utilisent les réseaux sociaux*
 - *Les solutions open source et auditables sont encouragées*
 - ii. *Le document "General Data Protection Regulation" dans la pratique*
 - *Outils et méthodes pour aider les organisations d'implémenter GDPR*
 - iii. *Identité numérique sécurisée.*
 - *using adequate correlation of multiple **soft proofs** of identity, as opposed to the usage of a central register*
 - *"qualified anonymity", le service a seulement le **pseudonyme** de l'utilisateur*

- ❑ **Action d'Innovation (IA)**
- ❑ 2-3 M€/projet, budget de **21M€**, TRL 5-7



LE JOURNÉES D'INFORMATION SÉCURITÉ

Prochaines journées d'information



- Pour end-user

- Lyon 21/10/2015
- Paris 12/11/2015
- Paris 3/12/2015 dédiée CIP-01
- Nice 1/2/2016 dédiée SEC-21-GM

- Pour tous

- Brest 28/10/2015
 - Paris 17/11/2015 *Journée d'information défi 6 (SHS)*
 - Paris Nord 18/11/2015 (Milipol)
 - Caen 19/11/2015
 - Metz 27/11/2015 Événement de réseautage transfrontalier sur DS
 - Paris 14/1/2016 Journée d'information nationale
 - Paris 15/1/2016 Événement de réseautage européen sur SEC-05
 - Nice (à confirmer) 1/2/2016 Événement de réseautage européen sur SEC-21
-
- Dates à fixer Lyon, Toulouse, Agen, FIC 2016, WISG 2016