GTN Horizon 2020 « Défi sécurité »

MENESR – 17/01/18

Ordre du jour

- **Point Europe**
  - Résultats appel 2017
  - Amendements WP 2018

- **Point actualité COFIS**

- **Divers**
  - Concours innovation
  - Calendrier
  - Vers FP9

POINT EUROPE

HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Appels SEC 2017 en quelques chiffres

- Propositions
  - 299 propositions éligibles soumises dont 136 à participation FR (45%) et 17 à coordination FR (5 RIA, 9 IA, 1 PCP et 2 CSA ; 26% de la demande totale FR)
  - 3748 participations dont 243 FR (6%)
  - 1912 participants dont 116 FR (6%)
  - Demande totale de 1,2 Md€ dont 90 M€ par acteurs FR (7,3%)

- Projets
  - 42 projets retenus dont 24 à participation FR (57%) et 4 à coordination FR (3 IA et 1 PCP ; 39% de la sub. totale FR)
  - 603 participations dont 42 FR (7%)
  - 455 bénéficiaires dont 30 FR (7%)
  - Subvention totale de 195 M€ dont 16,4 M€ pour FR (8,4%)
  - Taux de succès de 15,9% (18,3% pour FR)

Evaluators: Nationality

184 Evaluators*

115 (62 %) Male

69 (38 %) Female

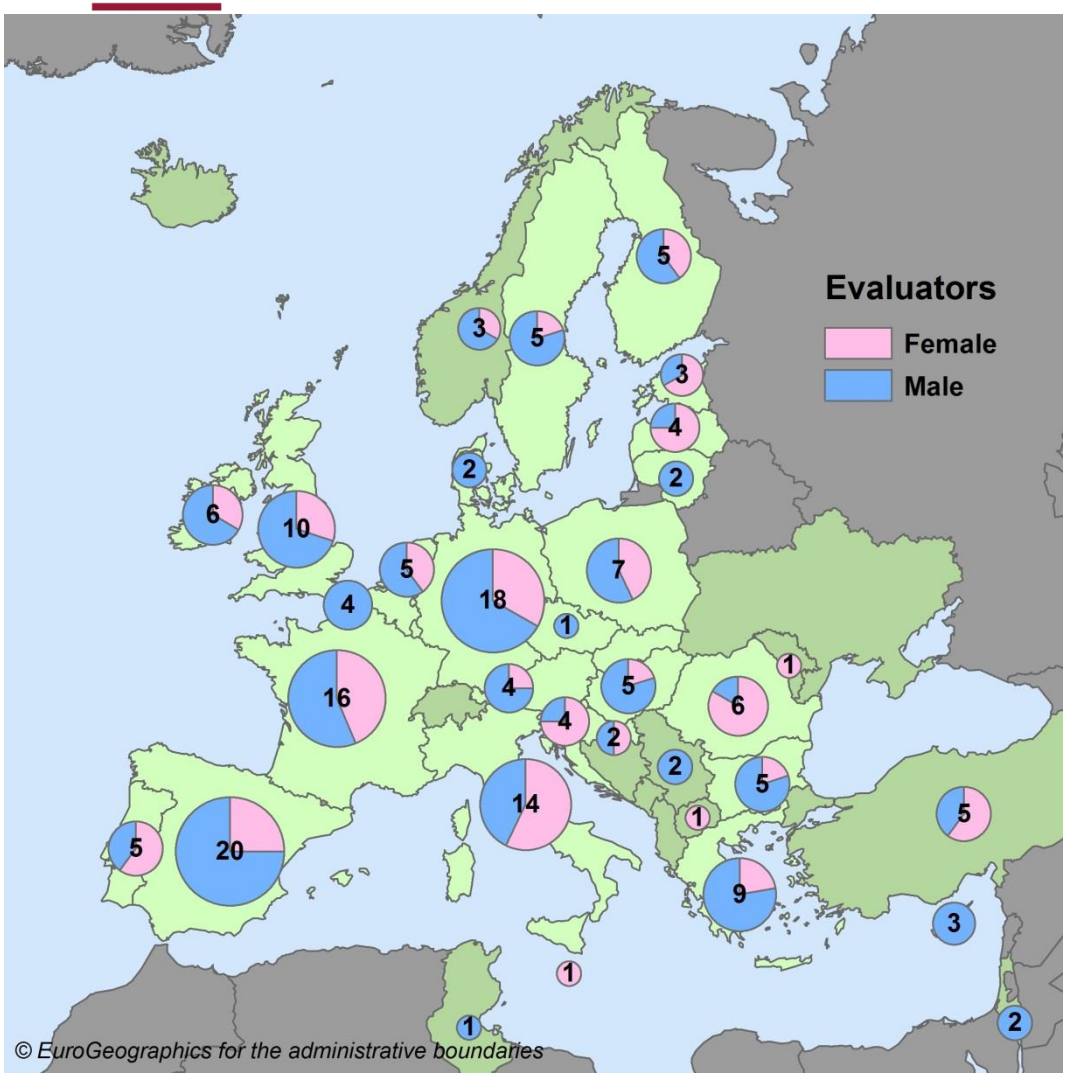
166 (90%) from Member States

15 (8%) from Associated Countries

3 (2%) from 3rd countries

All MS represented except SK and LU

*Not including:
- 24 Independent Rapporteurs
- 9 Ethics Experts
- 1 Observer



European Commission

Research Executive Agency

Applications: All Calls

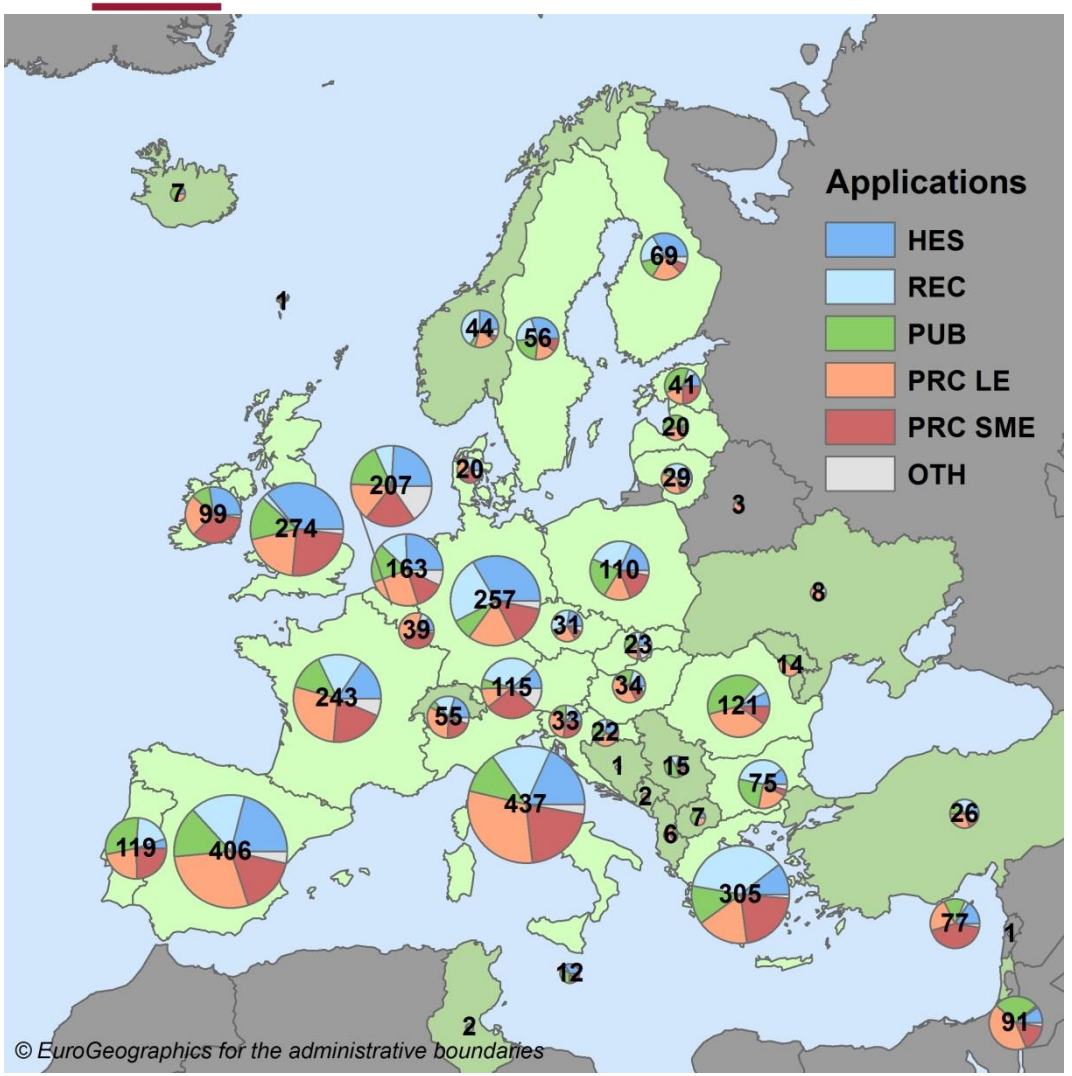
European Commission

3,748 applications by 1,953 unique applicants

- **Member States :** 3,437 applications
- **Assoc. Countries :** 280 applications
- **3rd Countries :** 31 applications

Applications per sector:

- HES: 749 (20%)
- REC: 627 (17%)
- PUB: 601 (16%)
- PRC LE: 911 (24%)
- PRC SME: 698 (19%)
- OTH: 162 (4%)



Research Executive Agency

Requested Funding – All Calls

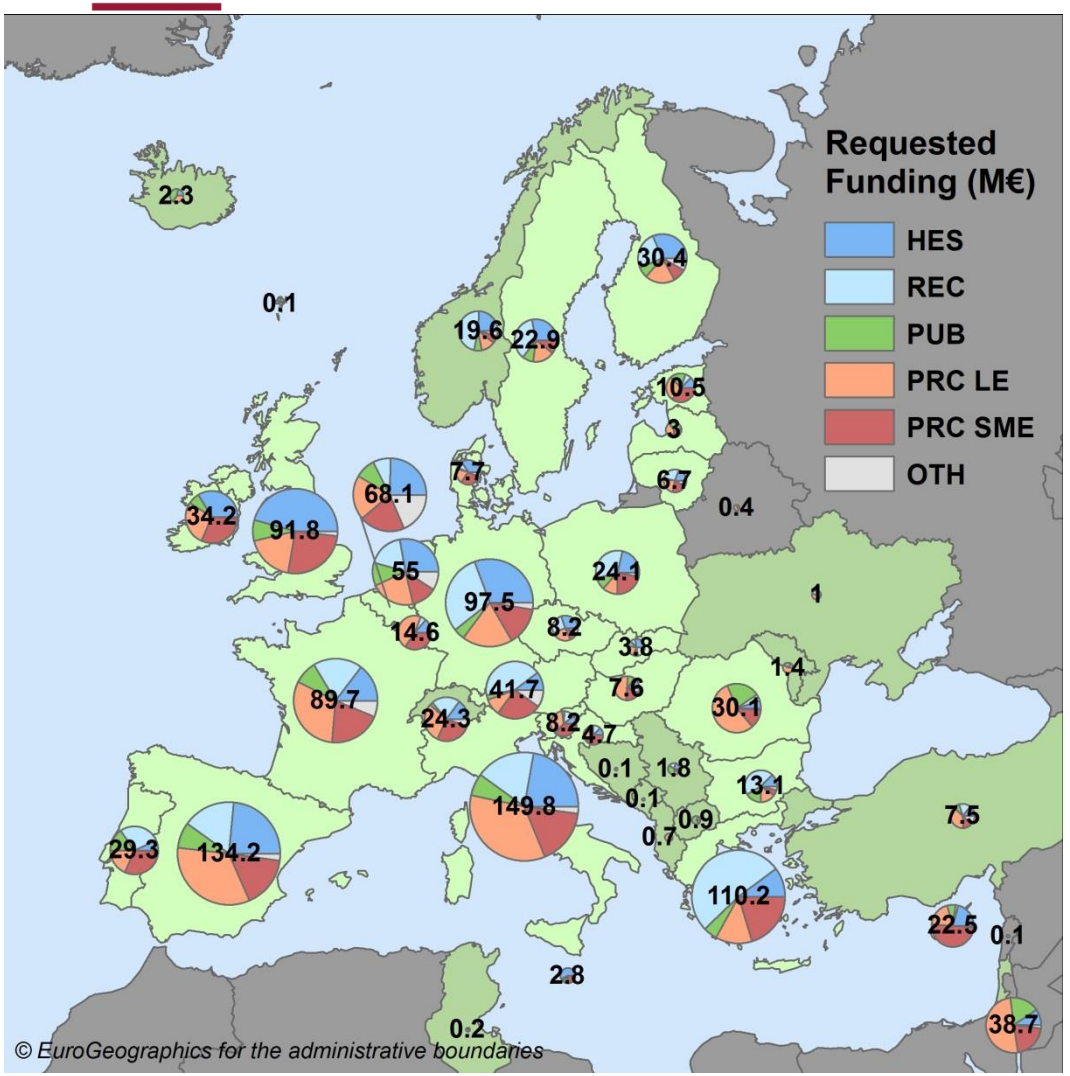
European Commission

1,225 M€ total requested funding

- **Member States**: 1,122 M€
- **Assoc. Countries**: 99 M€
- **3rd Countries**: 4 M€

Requested funding by sector:

- HES: 271 M€ (22%)
- REC: 252 M€ (21%)
- PUB: 100 M€ (8%)
- PRC LE: 312 M€ (26%)
- PRC SME: 239 M€ (19%)
- OTH: 51 M€ (4%)



Research Executive Agency

Applications: Mainlist All Calls

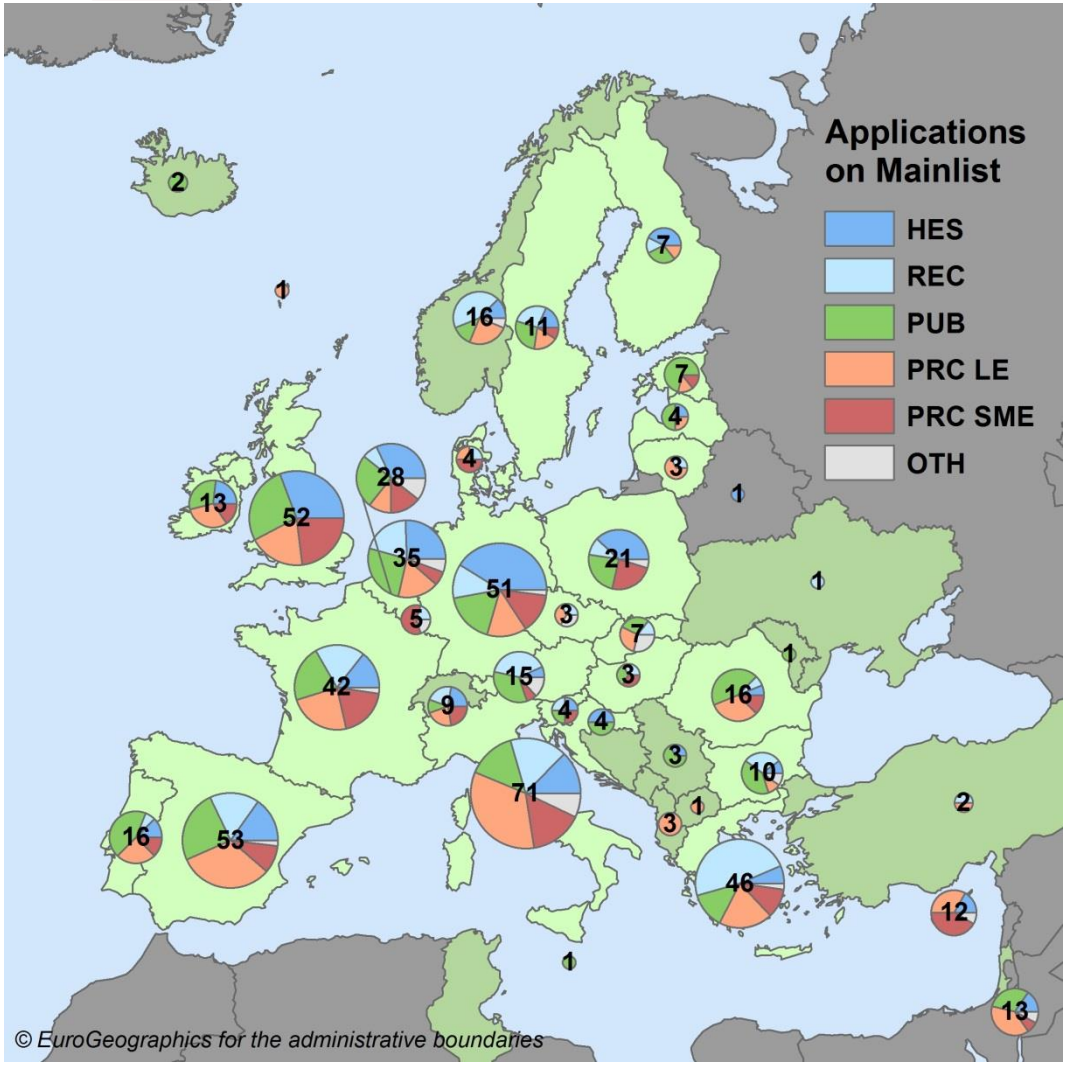
European Commission

603 applications by 462 unique applicants

- **Member States :** 544 applications
- **Assoc. Countries :** 52 applications
- **3rd Countries :** 7 applications

Applications per sector:

- HES: 117 (20%)
- REC: 102 (17%)
- PUB: 141 (23%)
- PRC LE: 135 (22%)
- PRC SME: 83 (14%)
- OTH: 25 (4%)



Research Executive Agency

Req. Funding: Mainlist All Calls

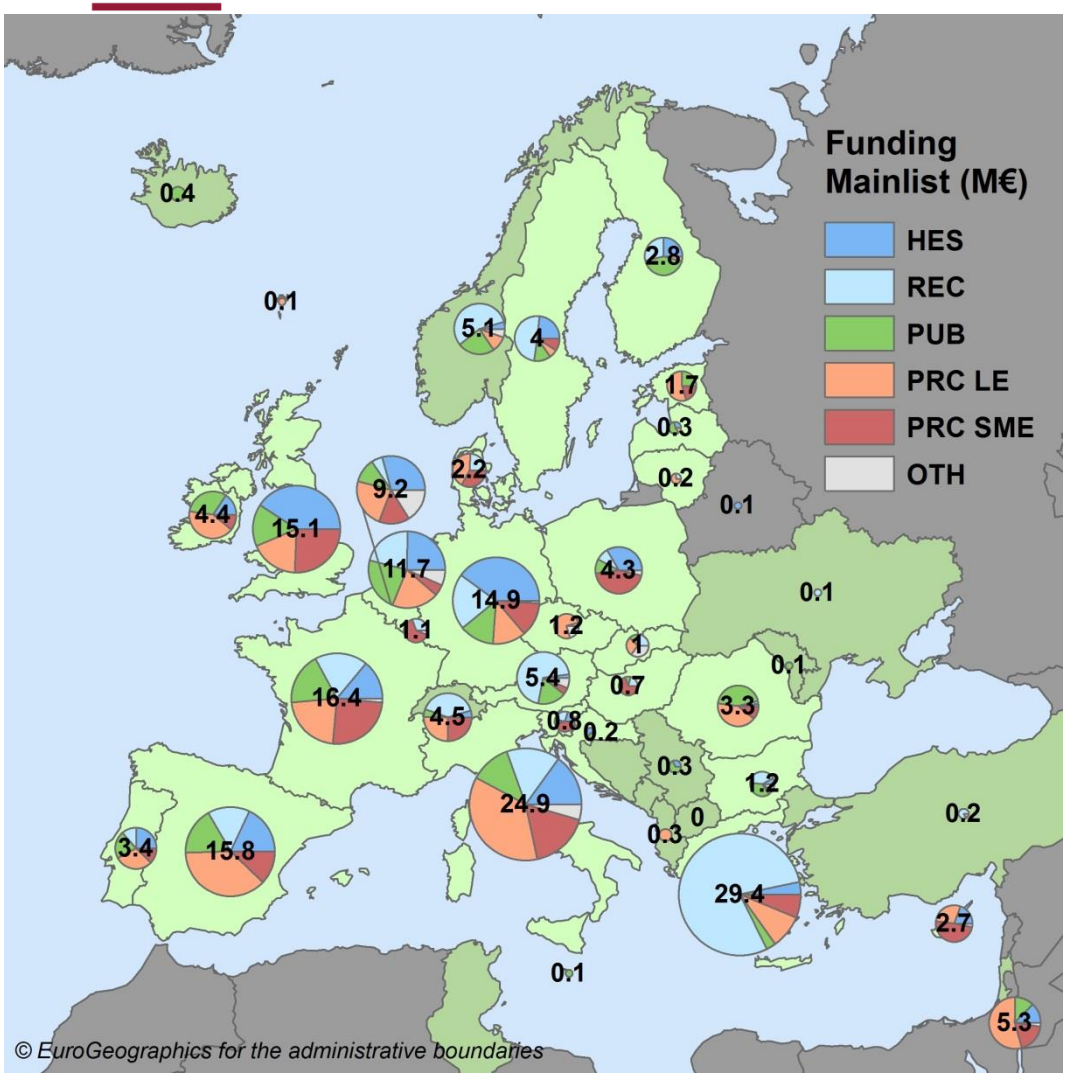
European Commission

194.8 M€ total requested funding

- **Member States**: 178.2 M€
- **Assoc. Countries**: 16.4 M€
- **3rd Countries**: 0.2 M€

Requested funding by sector:

- HES: 34.6 M€ (18%)
- REC: 53.0 M€ (27%)
- PUB: 28.1 M€ (15%)
- PRC LE: 43.8 M€ (22%)
- PRC SME: 29.5 M€ (15%)
- OTH: 5.8 M€ (3%)



Research Executive Agency

SEC-07-FCT-2016-2017
SEC- 18-BES-2017

Full coverage of the SEC-07 sub-topics:

- **Mass gatherings 2016**
- **Cybercriminal behaviours 2017**
- **Financial crime 2017**
- **Petty crime 2017**
- **Domestic violence 2017**

Coverage of SEC-18

- **Acceptance of no gate crossing point solutions**

SEC-12-FCT-2016-2017

All fixed sub-topics (and one open topic) were already covered in 2016.

Five open topics projects selected in 2017:

- Tools for fighting oNline Illegal TrAfficking
- IoT Platform of Crime and Terrorism DetectiON,
- Early-Warning in fighting Organised Crime and Terrorism
- Multimedia Analysis and Correlation Engine for Organised Crime Prevention and Investigation
- Scalable privacy preserving intelligence analysis for resolving identities

SEC-21-GM-2016-2017

Six projects financed:

Two geographical area projects (no proposal covering only baltic)

- **Danube financed 16**
- **Arctic and Mediterranean**

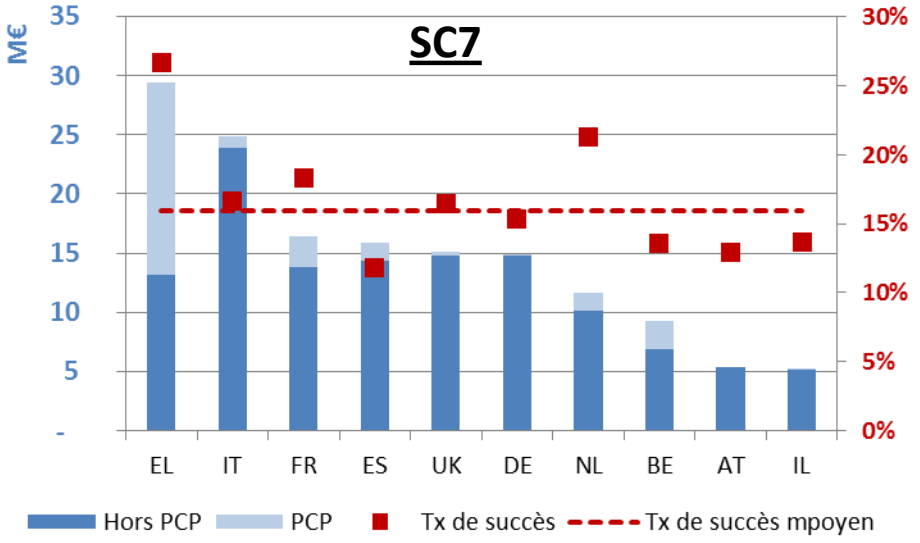
Three thematic (practitioners)

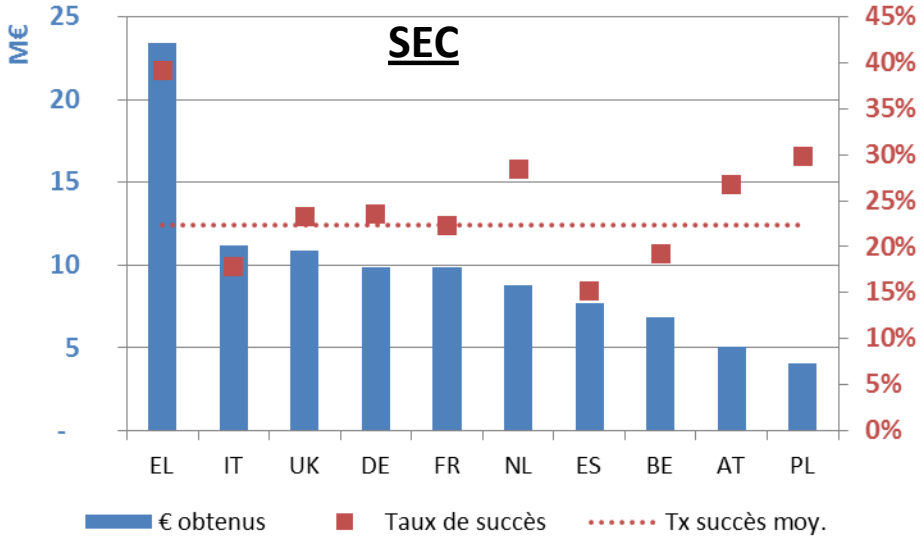
- **Explosives, Customs, Emergency medical services**

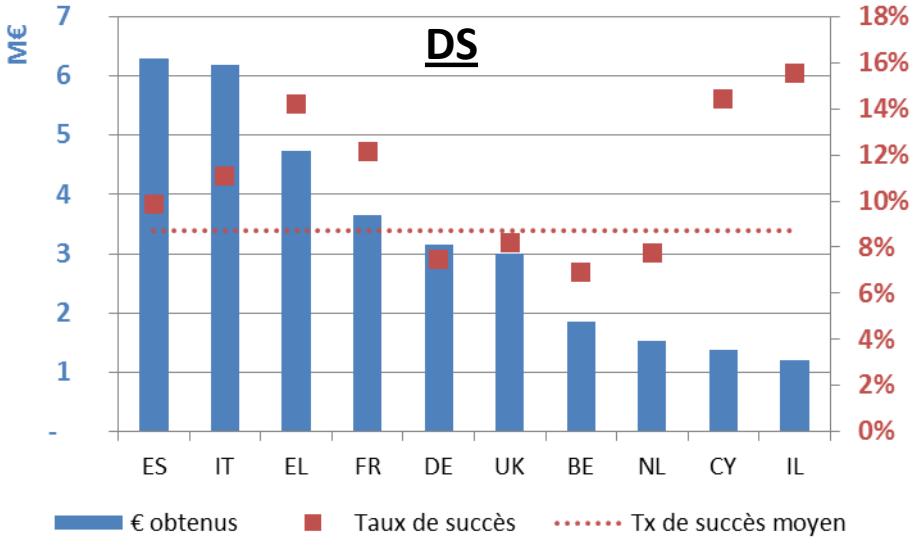
Continuation of the NCP network

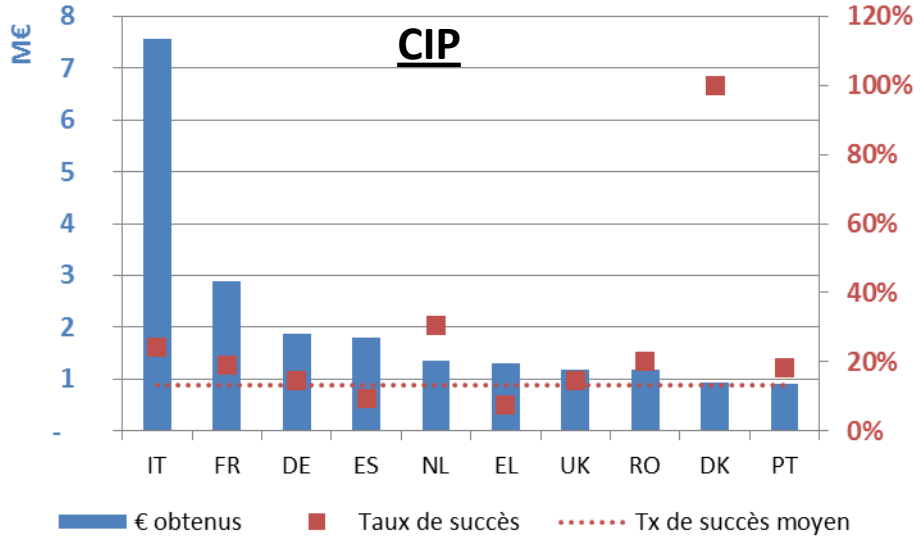
- **SEREN 4**

Analyse pays



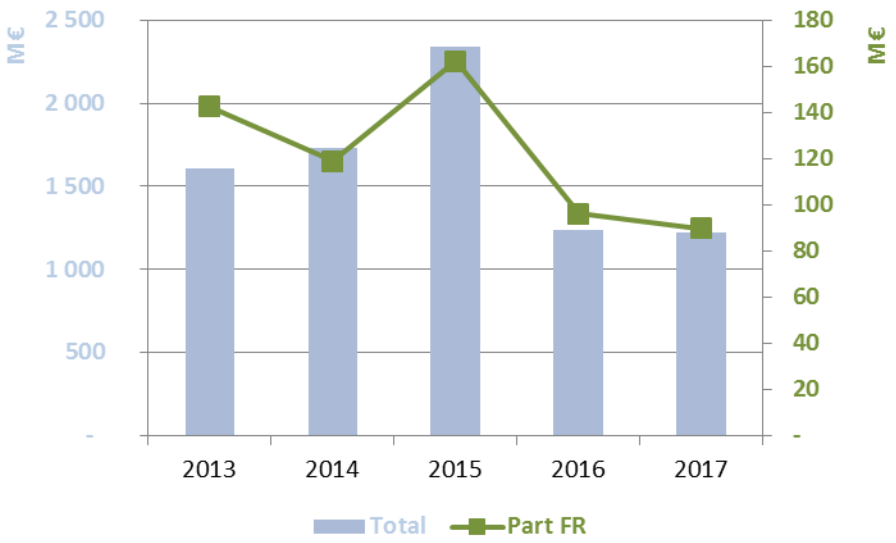




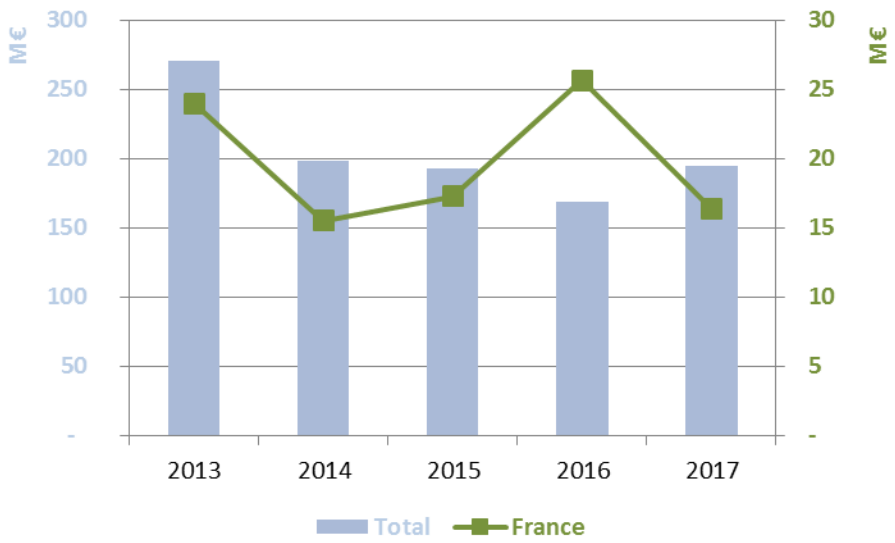


Evolution FR

Propositions



Projets

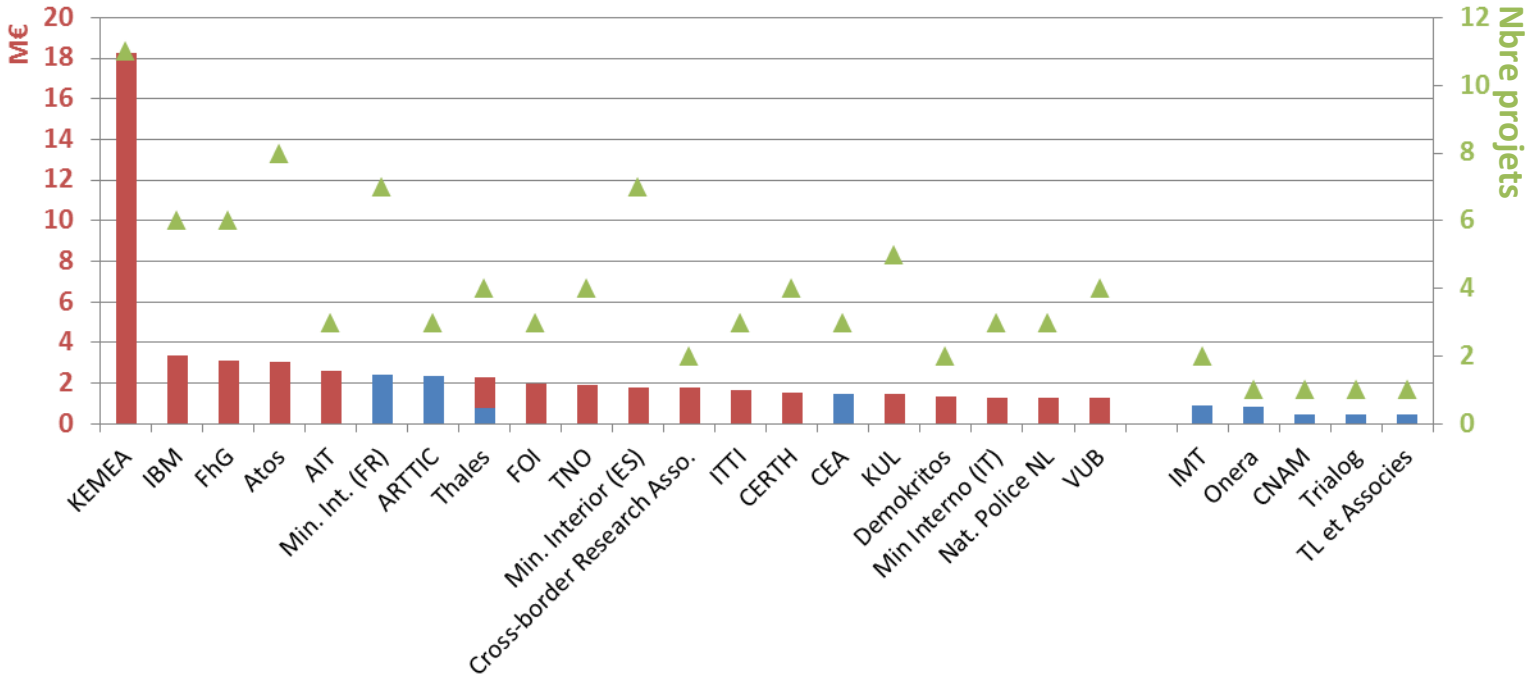


HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

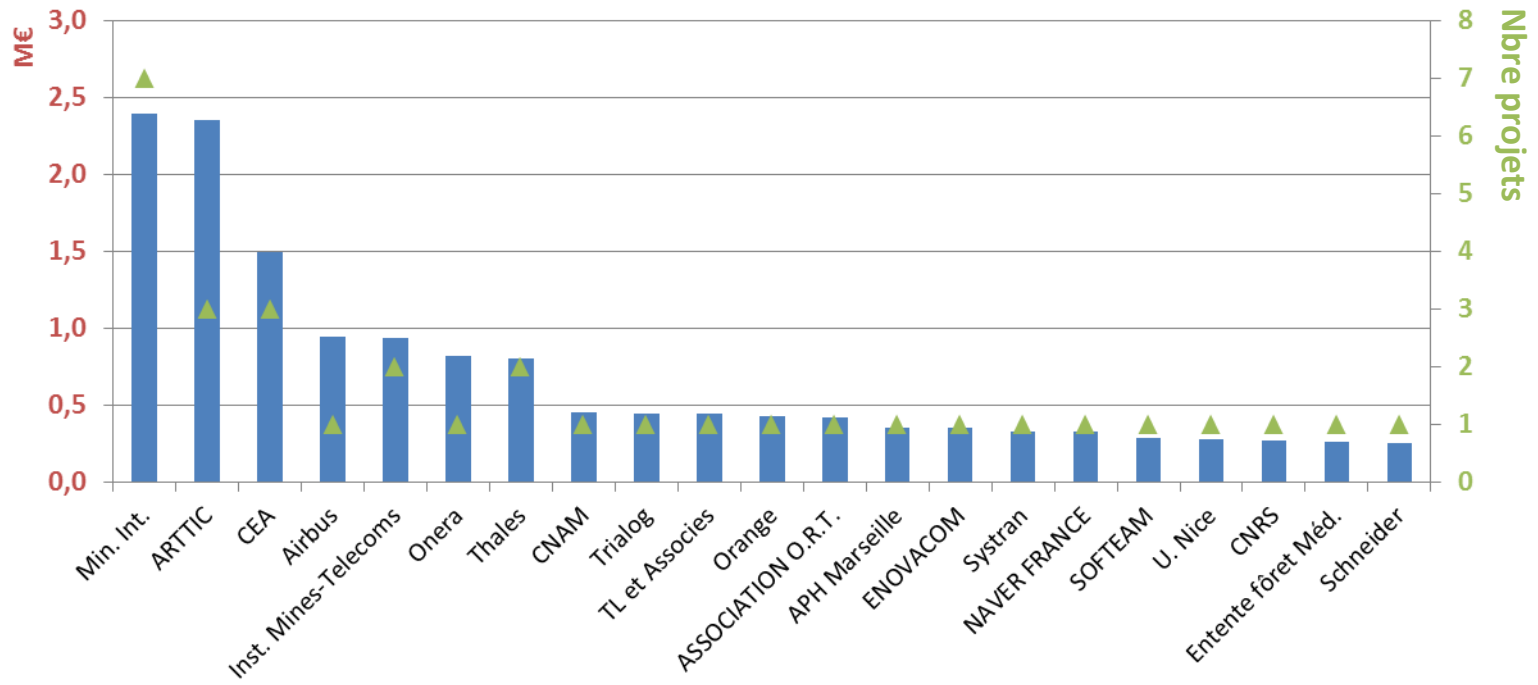
SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

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

Grands bénéficiaires (monde + FR)

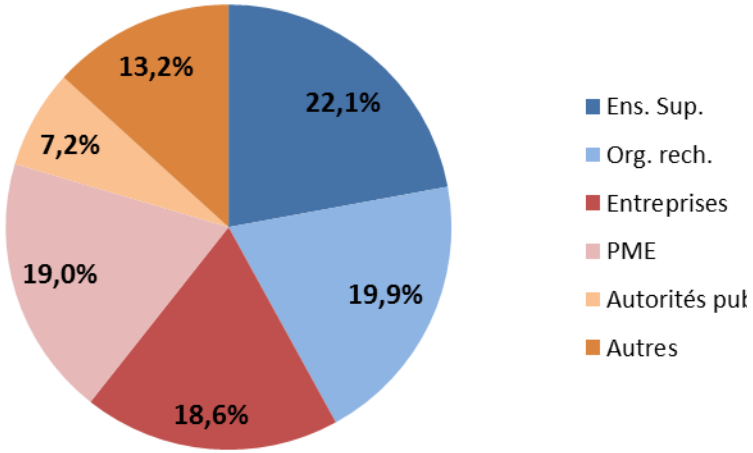


Grands bénéficiaires FR

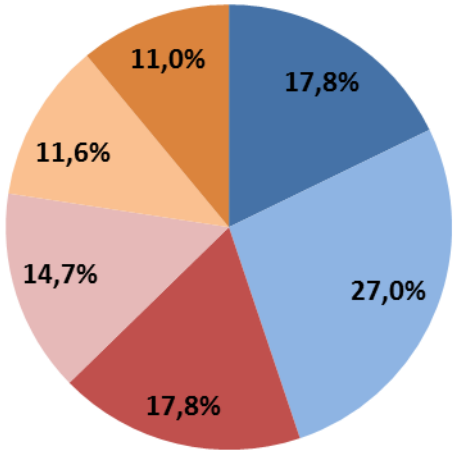


Typologie

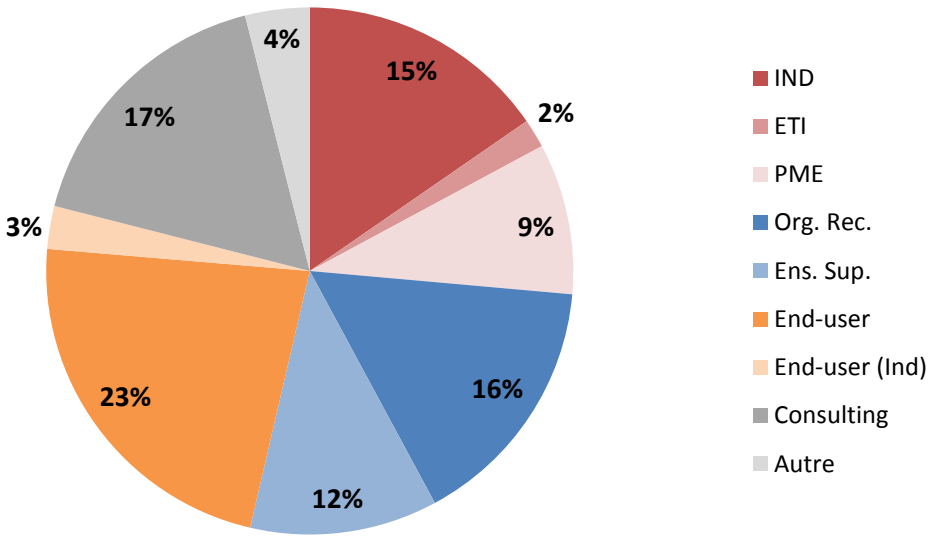
Propositions



Projets



Typologie bénéficiaires FR



Focus Cyber

- DS-07-2017: Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors
  - RIA - Situational Awareness
    - Eurecom, Scheider
  - IA - Simulation Environments, Training
    - 0 bénéficiaire FR

- DS-08-2017: Cybersecurity PPP: Privacy, Data Protection, Digital Identities

UPDATE WP LEIT/ICT

HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

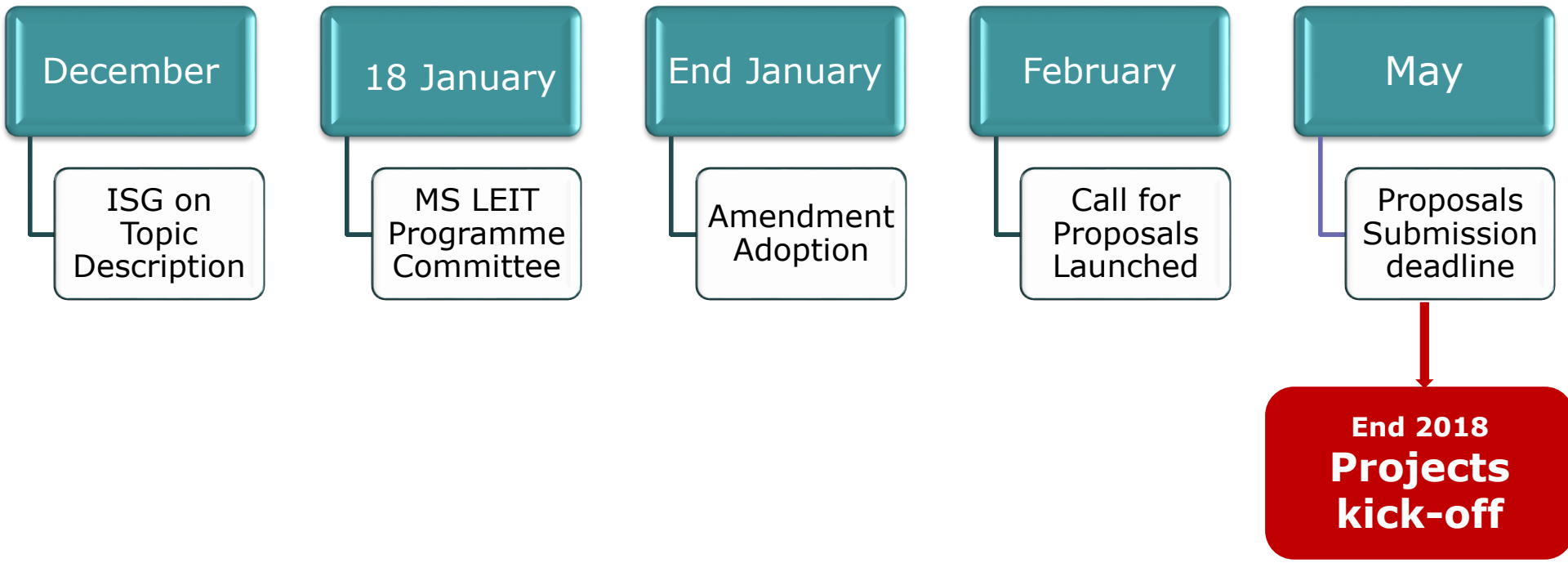
MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

H2020 – WP2018-2020 Pilot for a Cybersecurity Competence Network

SU-ICT-03-2018

DG CONNECT
Cybersecurity & Digital Privacy

2018 – 2020 Work Programme Amendment & Pilot Project



European Commission

Pilot Project Topic in a nutshell

Scope

- Propose & test network and central hub's governance model
- Help solve key industrial challenges through R&I activities related to next generation industrial and civilian cybersecurity technologies (including dual-use), applications and services;

Actors

- Cybersecurity R&D&I centres across Europe
- Consortium of minimum 9 Member States or Associated Countries & 20 partners
- Involvement and close collaboration with industry actors required

Impact

- Cybersecurity solutions, products or services for the identified critical challenges developed;
- Member States' cybersecurity research and innovation competence and capacities strengthened;
- Possible governance model for the network and the Centre tested through pilot projects

Instrument & Budget

- Innovation & Research Action
- €50 Mio in total; ~€16 Mio per project

Background

Policy context (1/3)

State of the Union 2017 - speech of the President of the Commission (13/09/2017)

- ✓ cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks;
- ✓ there is a need for a Europe that protects, empowers and defends;
- ✓ the priority is to better protect Europe in the digital age;

Cybersecurity Package 2017 (13/09/2017)

Joint Communication JOIN(2017)450: The Commission announced the intention to create a

Policy context (2/3)

Conclusions from the Tallinn Digital Summit (29/09/2017):

- *"We should make Europe a leader in cybersecurity by 2025, in order to ensure the trust, confidence, and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."*
- *"Europe needs a common European approach to cybersecurity. Europe has to function as a single European cyberspace and a single cybersecurity market, including in terms of world-class and state-of-the-art security certification and joint*

Policy context (3/3)

Council Conclusions (20 November 2017)

... "21. WELCOMES the intention to set up a Network of Cybersecurity Competence Centres to stimulate the development and deployment of cybersecurity technologies and to offer an additional impetus to innovation for the EU industry on the global scene in the development of next-generation and breakthrough technologies, such as artificial intelligence, quantum computing, blockchain and secure digital identities;

22. STRESSES the need for the Network of Cybersecurity Competence Centres to be inclusive towards all Member States and their existing centres of excellence and competence and pay special attention to complementarity and with this in mind NOTES the planned European Cybersecurity and Research Centre, which should, as its key role, focus on ensuring complementarity and avoiding duplication within the Network of Cybersecurity Competence Centres

H2020 Work Programme 2018-2020

General Introduction:

"As recently highlighted, Europe urgently needs to reinforce its cybersecurity technology and industrial capacity. A special effort will therefore go to a pilot action for the development of a European network of cybersecurity Competence Centres. Due to its importance, the preparations for this activity will begin immediately, with a view to being launched as early as possible in 2018."

Cybersecurity Call in WP-LEIT-ICT 2018-2020

Topics:

SU-ICT-01-2018: Dynamic countering of cyber-attacks

SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems

SU-ICT-03-2018: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap

SU-ICT-04-2019: Quantum Key Distribution

SU-ICT-03-2018: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap

Type of action: Research and Innovation Action (RIA)

Budget: 50 MEUR

Opening: 1 February 2018

Deadline: 29 May 2018

Indicative EU contribution: up to 16 MEUR

Specific challenge

→ **Retain and develop essential capacities to secure the EU digital economy, infrastructures, society, and democracy.**

→ **Address the too little alignment of EU cybersecurity research, competences and investments which are spread across Europe.**

→ **Master relevant cybersecurity technologies from secure components to trustworthy interconnected IoT ecosystems and self-healing software.**

→ **Step up investment in technological advancements making the DSM more cyber-secure, and to overcome the fragmentation of EU research capacities.**

→ **Support and equip EU industries with latest technologies and skills to develop innovative security products and services, and protect vital assets against cyberattacks.**

Scope and conditions (1/7)

- **Scale up existing research for the benefit of the cybersecurity of DSM, with marketable solutions;**
- **Participants should propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub;**
- **Projects will help build and strengthen cybersecurity capacities across the EU and provide valuable input for the future set-up of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre;**
- **Proposals should: take into consideration relevant active digital ecosystems and public-private cooperation models; focus on solving technological and industrial**

Scope and conditions (2/7)

- **Support for consortia of competence centres in cybersecurity to engage in:**
  - **Common research, development and innovation (R&D&I) in next generation industrial and civilian cybersecurity technologies, applications and services, with focus on horizontal cybersecurity technologies and cybersecurity in critical sectors;**
  - **Strengthening cybersecurity capacities across the EU and closing cyber skills gap;**
  - **Supporting certification authorities with testing and validation labs equipped with state-of-the-art technologies and expertise;**
- **Proposal should bring together cybersecurity R&D&I centres in Europe to create synergies and scale up**

Scope and conditions (3/7)

- **Centres within the proposal should aim to collectively develop and implement a Cybersecurity Roadmap covering the call requirements and addressing multiple and complementary cybersecurity disciplines; results of cybersecurity cPPP's work, as well as relevant work of ENISA, Europol and other EU agencies and bodies should be sought out and taken into consideration;**
- **Roadmap should include: targets to be achieved with deliverables by the end of the project (3-4 years) as clear implementation milestones, ans priorities to be addressed in the future by the Cybersecurity Competence Network;**
- **To implement the Roadmap, partners are expected to set up a functional network of centres of expertise with a coordinating "competence centre" (one of the partners in**

Scope and conditions (4/7)

- Work includes **assessment** of various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria, including the EU mechanisms and rules, national and regional funding structures, as well as those offered by industry;
- A **governance structure** should be proposed, to be implemented, tested and validated in **demonstration cases** involving all network partners to showcase its performance and optimise the proposed governance structure;
- Projects will demonstrate the effectiveness of their selected governance structure by providing **collaborative solutions** to enhance cybersecurity capacities of the network and develop cyber skills;

Scope and conditions (5/7)

- **Engage industrial communities and their cybersecurity research collaborators to: create synergies; collaboratively identify and analyse scalable cybersecurity industrial challenges in the selected sectors; and demonstrate their ability to collaborate in developing appropriate solutions to solve critical challenges through not less than 4 R&I demonstration cases;**
- **These demonstration cases (core part of the work to be done) will be based on a specific R&D roadmap to tackle selected industrial challenges and will implement it covering a complete range of activities, from R&I through testing, experimentation and validation to certification activities;**
- **A proposal must involve distinct cybersecurity R&D&I**

Scope and conditions (6/7)

- **Proposals should include a substantial representation of the most relevant R&D&I excellences centres in Europe, with a widespread European coverage and good geographical balance of activities as regards the scope of work; this will ensure the proposals meeting the policy goals of the initiative of supporting the establishment of the future Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre of the EU;**
- **A proposal should engage industrial communities/stakeholders from various (not less than 3) sectors that will be involved in the demonstration cases;**
- **Proposers are encouraged to involve relevant governmental bodies and authorities for monitoring and**

Scope and conditions (7/7)

- Projects under this topic are implemented as a programme through the use of complementary grants; respective options of Article 2, Article 31.6 and Article 41.4 of the Model Grant Agreement will be applied;
- Proposals shall foresee resources for clustering activities with other projects funded under this topic to identify synergies, best practices and kick-off the process of creating the network involving the sub-networks already created by awarded projects; this will contribute to the actual set-up of the Cybersecurity Competence Network and a European Cybersecurity Research and Competence Centre at a later stage;
- Beneficiaries nominated as project coordinators cannot, in this capacity, be awarded more than one grant from the EU budget; in case an applicant organisation appears as

Expected impact (1/2)

- **Cybersecurity solutions, products or services for the identified critical challenges, increasing DSM cybersecurity, in particular for sectors with stakeholders involved;**
- **Feasible, sustainable governance model for the Cybersecurity Competence Network, developed and tested through successful pilots addressing selected industrial challenges;**
- **Strengthening of MS' research and innovation competence, and cybersecurity capacities, also within their national cybersecurity ecosystems, to meet the increasing cybersecurity challenges;**
- **Synergies between experts from various cybersecurity domains;**

Expected impact (2/2)

- **Research and Development Programme with a common Research and Innovation Roadmap reflecting all different cybersecurity sectors and covering a wide range of activities from research to testing;**
- **Cybersecurity skills framework model developed, to be used as a reference by: education providers to develop appropriate curricula; employers, to help assess their cybersecurity workforce and improve job descriptions; citizens to reskill themselves;**
- **Establishment of foundations for pooling and streamlining the development and deployment of cybersecurity technology and strengthening industrial capabilities to secure EU's digital economy, society, democracy, space and infrastructures**

Cybersecurity Call - Planning

Topic	Instrument	Funding (MEUR)	Opening	Deadline
SU-ICT-01-2018	IA	40.00	15 Mar 2018	28 Aug 2018
SU-ICT-02-2020	RIA	47.00	25 July 2019	19 Nov 2019
SU-ICT-03-2018	RIA	50.00	1 Feb 2018	29 May 2018
SU-ICT-04-2019	IA	15.00	26 July 2018	14 Nov 2018

Useful links

H2020 Reference documents, including full version of the Work Programme 2018-2020 and the Annotated Model Grant Agreement:

https://ec.europa.eu/research/participants/portal/desktop/en/funding/reference_docs.html#h2020-legal-basis

NCP network:

http://ec.europa.eu/research/participants/portal/desktop/en/support/national_contact_points.html

Commentaires FR

- Soutien au principe du réseau européen
- Réserves sur l'approche (célérité, compétition, volume €, taille des consortia, adéquation entre objectifs et acteurs)
- Problèmes de la multiplication des réseaux en sus du cPPP et de l'ENISA

ACTUALITÉ COFIS

UNE POLITIQUE INDUSTRIELLE DE SÉCURITÉ AMBITIEUSE À HORIZON 2025 POUR LA FRANCE (1/2)

Quatre objectifs :

- Doubler le chiffre d'affaire de la filière.
- Créer 75000 nouveaux emplois qualifiés.
- Maintenir un taux de croissance à l'export supérieur au taux de croissance national.
- Couvrir l'intégralité des technologies identifiées comme critiques par des offres de solutions nationales ou européennes.

UNE POLITIQUE INDUSTRIELLE DE SÉCURITÉ AMBITIEUSE À HORIZON 2025 POUR LA FRANCE (2/2)

Au moyen de cinq ambitions :

- la France sera reconnue comme le meilleur environnement, en Europe, pour l'accueil, la croissance et la consolidation des start-up (et des PME innovantes) de la sécurité ;
- la France sera un leader mondial dans le domaine des *safe cities* ;
- la France sera un leader mondial de la cybersécurité et de la sécurité de l'Internet des objets ;
- la qualité, la performance, la confiance et l'innovation des offres françaises sera reconnue internationalement. La marque « France » dans le domaine de la sécurité sera au moins aussi connue que celle des nations leaders du domaine;
- la France sera le moteur de la mise en place d'une autonomie européenne sur les segments clés de sécurité.

UNE VISION EUROPÉENNE

- Sécurisation de l'Espace Schengen
- la transformation numérique et l'interopérabilité des forces de sécurité»
- Protection des infrastructures critiques de transport et d'énergie
- Sécurisation de la ville « intelligente»

CICS
Conseil des Industries de la Confiance et de la Sécurité

L'OBSERVATOIRE

- **UN ENSEMBLE D'OUTILS POUR SUIVRE LA FILIÈRE SUR TOUT SON PÉRIMÈTRE DANS LE TEMPS**
  - ANALYSES DE MARCHÉ
  - RECENSEMENT DES ENTREPRISES
  - POSITIONNEMENT COMPÉTITIF
  - VISION PROSPECTIVE
  - SUIVI D'INDICATEURS
  - ACTUALISATION ANNUELLE DES DONNÉES ÉCONOMIQUES

- **UN PROJET DU COFIS**
  - LANCÉ SUR 4 ANS (2017-2021)
  - PORTÉ PAR LE CICS EN PARTENARIAT AVEC LE SGDSN, LA DGE, LA DMISC, LE GICAT ET MILIPOL

DGE
SGDSN
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR
GICAT

CICS
Conseil des Industries
de la Confiance et de la Sécurité

Cofis

LE PÉRIMÈTRE DE LA FILIÈRE

Milipol PARIS 2017

SECTEUR PRIVE

INDUSTRIES

PRODUITS PHYSIQUES

- Véhicules, plateformes
- Vêtements et équipements protecteurs
- Fournitures et armes, accessoires incendie
- Interdiction physique d'accès
- Equipements de sécurité incendie

5,6 Mds€

PRODUITS ELECTRONIQUES ET NUMERIQUES

- Identification, authentification
- Détection intrusion
- Détection, extinction incendie
- Détection produits dangereux, scanners
- Observation locale et surveillance large zone
- Suivi, traçage, localisation
- Communications
- Commande contrôle
- Renseignement
- Intégration

14,5 Mds€

PRODUITS ET SOLUTIONS DE CYBERSECURITE

- Gouvernance
- Gestion identités et accès
- Sécurité des données
- Sécurité des applications
- Sécurité des infrastructures
- Sécurité des produits et équipements

1,2 Mds€

SERVICES

SERVICES DE CYBERSECURITE

- Audit, planning, conseil
- Mise en œuvre
- Infogérence, exploitation
- Formation

3,1 Mds€

SERVICES PRIVES DE SECURITE

- Gardiennage, interventions sur alarme
- Transport de fonds
- Protection rapprochée
- Sûreté aéroportuaire
- Surveillance et télésurveillance
- Enquêtes privées
- Conseil en sécurité
- Formation en sécurité

10,5 Mds€

SECTEUR PUBLIC

SERVICES PUBLICS DE SECURITE

- Forces de maintien de l'ordre (police, police de l'air et des frontières, gendarmerie)
- Gardes côtes, sécurité maritime
- Douanes
- Militaires (en mission de sécurité)
- Sécurité civile
- Sapeurs-pompiers
- Justice et Administration pénitentiaire
- Polices municipales

CICS
Conseil des Industries
de la Confiance et de la Sécurité

L'ACTIVITÉ DE LA FILIÈRE EN FRANCE EN 2016

	CA millions €		Croissance annuelle 2013-2016
	2013	2016	
Produits physiques	5 330	5 605	1,7%
Produits élec. et num.	12 428	14 450	5,1%
Cyber-sécurité	3 150	4 300	10,9%
Services privés de sécurité	8 969	10 466	5,3%
Total marchand	29 877	34 821	5,2%
Services publics de sécurité	29 000		
Total filière sécurité	58 877		

Source : DECISION ETUDES & CONSEIL

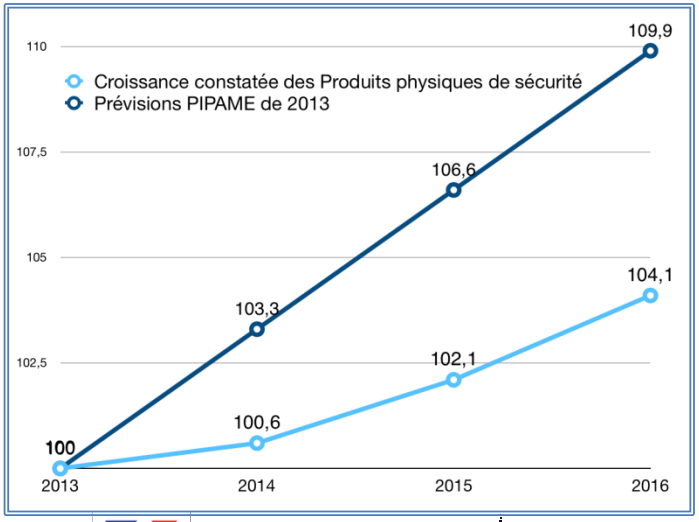
MINISTÈRE DE L'INTÉRIEUR

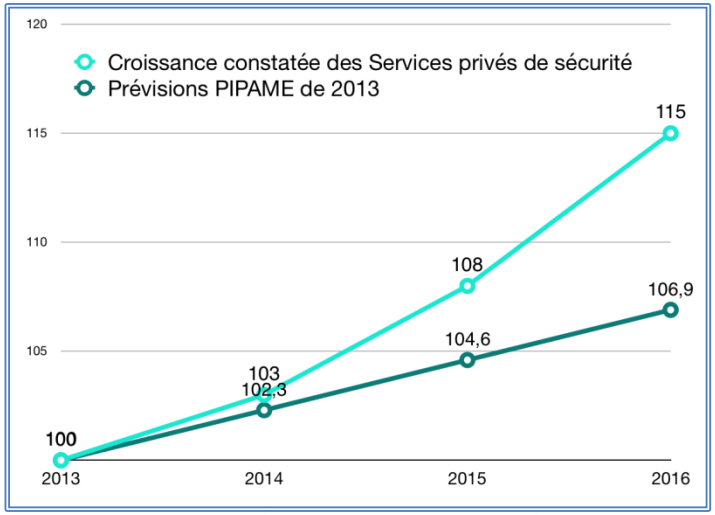
CICS
Conseil des Industries de la Confiance et de la Sécurité

FOCUS ANNUEL ET ÉCARTS PAR RAPPORT AUX PRÉVISIONS

	Croiss 2014	Croiss 2015	Croiss 2016	Moyenne observée 2013-2016	Prévision (étude PIPAME)
Produits physiques	0,6%	1,5%	2,0%	1,7%	3,3%
Produits élect. & num.	2,5%	6,0%	7,0%	5,1%	6,0%
Cybersécurité	7,0%	14,0%	12,0%	10,9%	10,4%
Services privés de sécurité	3,0%	5,0%	7,0%	5,3%	2,3%
Total marchand	**2,8%**	**5,8%**	**6,8%**	**5,2%**	**5,1%**

Source : DECISION ETUDES & CONSEIL





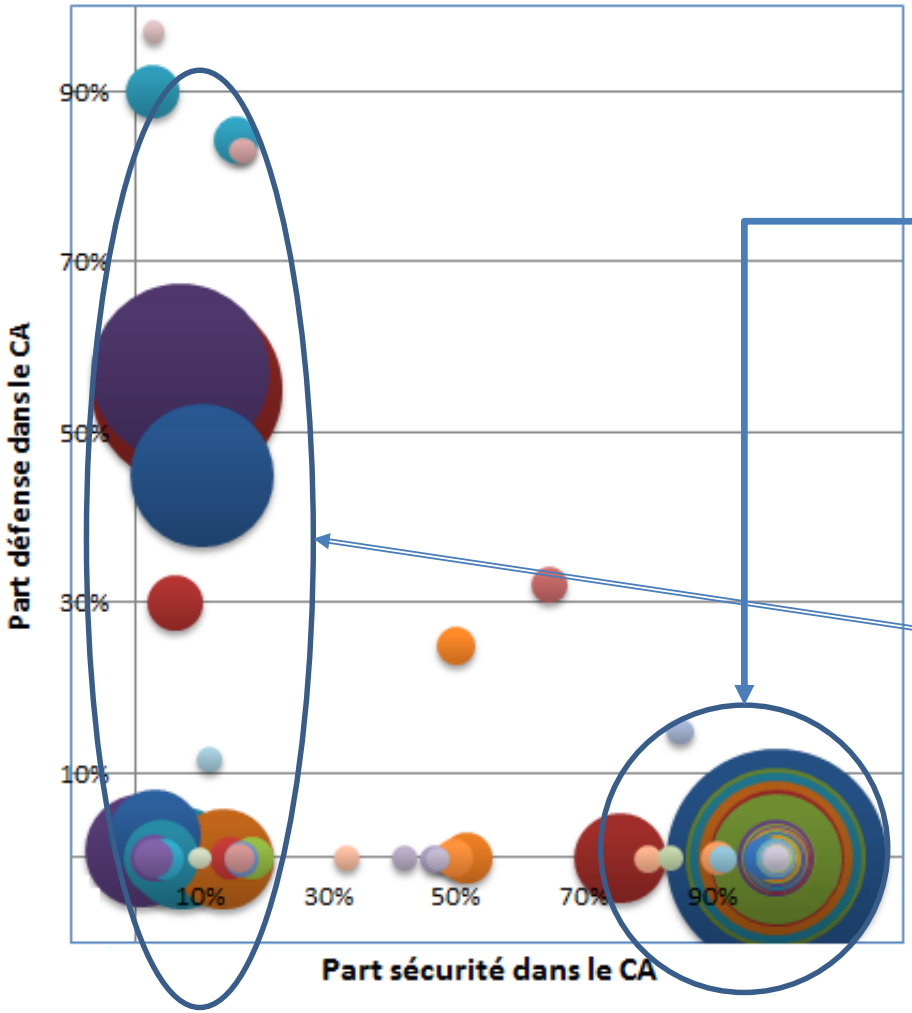
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES
DGE
SGDSN
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR
GICAT

CICS
Conseil des Industries de la Confiance et de la Sécurité

Cofis

UN SECTEUR INDUSTRIEL À PART ENTIÈRE

Milipol PARIS 2017



MAJORITÉ DE L'ACTIVITÉ RÉALISÉE PAR 60% DE « PURE PLAYERS » (ACTIVITÉ SÉCURITÉ > 90%)

DES GRANDS ACTEURS DE LA DÉFENSE OU DU CIVIL (AVEC UNE ACTIVITÉ SÉCURITÉ < 30% MAIS STRUCTURANTE)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES
DGE

SGDSN

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

GICAT

La filière et les JO « Paris 2024 »

- Un événement superlatif
  - 2,5 à 3 millions de visiteurs
  - 300 à 400 000 accréditations
  - 17 000 athlètes
  - 3 mois avec évènements associés
- Des enjeux de sécurité majeurs
  - Risques et menaces très étendus (terrorisme, sanitaire,…)
  - Plus de 100 000 agents (dont 45 000 publics)
  - Sécurité stades, fanzones, villages olympiques, hôtels, transports,…
  - Plus de 3000 km de voies réservées dynamiques à sécuriser
- Des attentes fortes = opportunité d'accélérateur et de vitrine
  - Limiter le volume des forces publiques et privées grâce à la technologie
  - Sécurité transparente, de bout en bout
  - Système d'information du public sécurisé et contribuant à la sécurité

TECHNOLOGIES CRITIQUES (1/3)

Une **technologie critique de sécurité** est une technologie **essentielle et sensible** pour la mise en œuvre de missions de sécurité **sur laquelle pèsent des risques de maitrise** (nombre de fournisseurs très restreints, rentabilité insuffisante, risque de prise de contrôle capitalistique, perte de savoir-faire, absence de technologies alternatives ou de contournement possible etc.).

La définition prise ici pour le terme technologie est extensive : il peut s'agir au cas par cas de composants, de procédés, de sous-système, voire de systèmes entiers, de compétences académiques, etc.

TECHNOLOGIES CRITIQUES (2/3)

- Gouvernance : Pilotage par l'Etat (SGDSN et ministères).
- Trois phases de travail
  - Identification des technologies critiques de sécurité.
  - Recensement des entreprises en particulier des PME entrant dans la chaine de valeurs des technologies critiques identifiées.
  - Définition des plans d'actions à mettre en œuvre pour soutenir les technologies critiques retenues, au plan national ou européen.

TECHNOLOGIES CRITIQUES (3/3)

- Analyse guidée par la segmentation CoFIS et les ruptures technologiques identifiées
- 2 critères pour les technologies actuelles
  - Caractère essentiel et sensible des technologies
  - Risques concrets pesant sur la maitrise nationale
- 27 technologies identifiées comme critiques.
- Exemples :
  - Cyber : sondes d'analyse et sondes souveraines de détection.
  - Systèmes complets de contrôle d’accès logique et physique.
  - Système radio privé offrant des communications de groupe sécurisées.
- Des entreprises identifiées sur ces segments

TECHNOLOGIES DE RUPTURE (1/2)

Une technologie de rupture pour la sécurité sera une technologie qui devrait être indispensable pour les missions de sécurité avec un impact fort sur le marché de la sécurité à horizon 2025.

Certaines de ces technologies pourront s'avérer critiques et nécessiteront des plans d'actions afin de favoriser leur développement.

TECHNOLOGIES DE RUPTURE (2/2)

- Des technologies de rupture à horizon 2025
  - Un futur document de prospective, en cours d'élaboration, sera publié par le CoFIS.
  - Une dizaine de domaines de rupture sont identifiés et documentés comme :
    - ✓ La Blockchain pour la sécurité
    - ✓ Les objets connectés
    - ✓ Le Big-Data pour la sécurité
    - ✓ L'identification/ authentification
  - Les composants de confiance et l'intelligence artificielle comme socle de nombreux domaines de rupture sont potentiellement critiques.

DIVERS

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Commissariat Général à l'Investissement

INVESTISSEMENTS D'AVENIR

PIA3 – Concours d'innovation

CONCOURS INNOVATION

- Dans le cadre des investissements d'avenir, la première vague des appels à projets du concours de l'innovation a été publiée. La thématique « Sécurité et cybersécurité » est à l'honneur avec un focus sur la sur **la protection des environnements urbains.**
- Le « Concours d'innovation » (CI), financé par le Programme d'investissements d'avenir (PIA), vise à soutenir des projets innovants portés par des start-ups et des PME (selon le droit européen1), et à favoriser l'émergence accélérée d'entreprises leaders dans leur domaine, pouvant prétendre à une envergure mondiale. Il sélectionne, dans le cadre d'une procédure favorisant la compétition, des projets d'innovation au potentiel particulièrement fort pour l'économie française. Il permet de cofinancer des projets de recherche, développement et innovation, dont les coûts totaux se situent entre 600 k€ et 5 M€, et contribue à accélérer le développement et la mise sur le marché de solutionset technologies innovantes.
- Les projets soutenus dans le cadre de ce Concours sont portés par une entreprise unique et sont non collaboratifs.
- La date de clôture est fixée au 13 mars 2018 à 12h00 (midi).

- Toutes les informations sur http://www.bpifrance.fr/A-la-une/Appels-a-projet-concours/Appel-a-projets-Concours-d-innovation-38041

Calendrier

- 23-24/01 – FIC: session pitchs H2020
- 01-02/02 – SMIGs 2018
- Infoday REA: Bruxelles, date à définir (mars?)
- Brokerage ES-FR: Madrid, 20 février