



HORIZON 2020

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

Appels 2019 H2020/Sécurité: Infrastructures critiques

Frédéric LAURENT (MESRI)

Paris – 18/03/19

Sommaire



1. Rappels H2020 et Sécurité
2. Topiques Infrastructures critiques 2019
3. Quelques conseils
4. Informations utiles

RAPPEL HORIZON 2020/SÉCURITÉ

Horizon 2020 en bref

Programmes (pérennes) de financement non-récurrent des équipes nationales de RDI entre 2014 et 2017 (en M€/an)



Part FR = 11% vs benchmarks:

- 15,9% (part FR dans budget H2020)
- 16,3% (part FR dans DIRD UE)
- 16,1% (part FR dans demande brevet OEB)

H20

Potentiellement: ~500 M€/an additionnel!

Horizon 2020: architecture



77,2 Md€ _{courant} pour 2014-20
dont ~1,9 Md€ pour la Sécurité (y compris cyber)

RDI

Défis sociétaux

- Santé, bien-être, vieillissement
- Sécurité aliment., bioéconomie
- Energies sûres, propres, efficaces
- Transports intell., verts, intégrés
- Climat, environnement, mat. 1^{ères}
- Sociétés inclusives et novatrices
- **Sociétés sûres**

Primauté industrielle

TIC
Technologies clés génériques:
microélectronique, photonique,
nanotechnologies, matériaux avancés,
systèmes de production, biotechnologies
Espace
Innovation dans les PME
Accès au financement à risque

*Recherche
fondamentale*

Excellence scientifique

Recherche exploratoire (ERC)
Technologies futures et émergentes (FET)
Infrastructures de recherche
Marie Curie

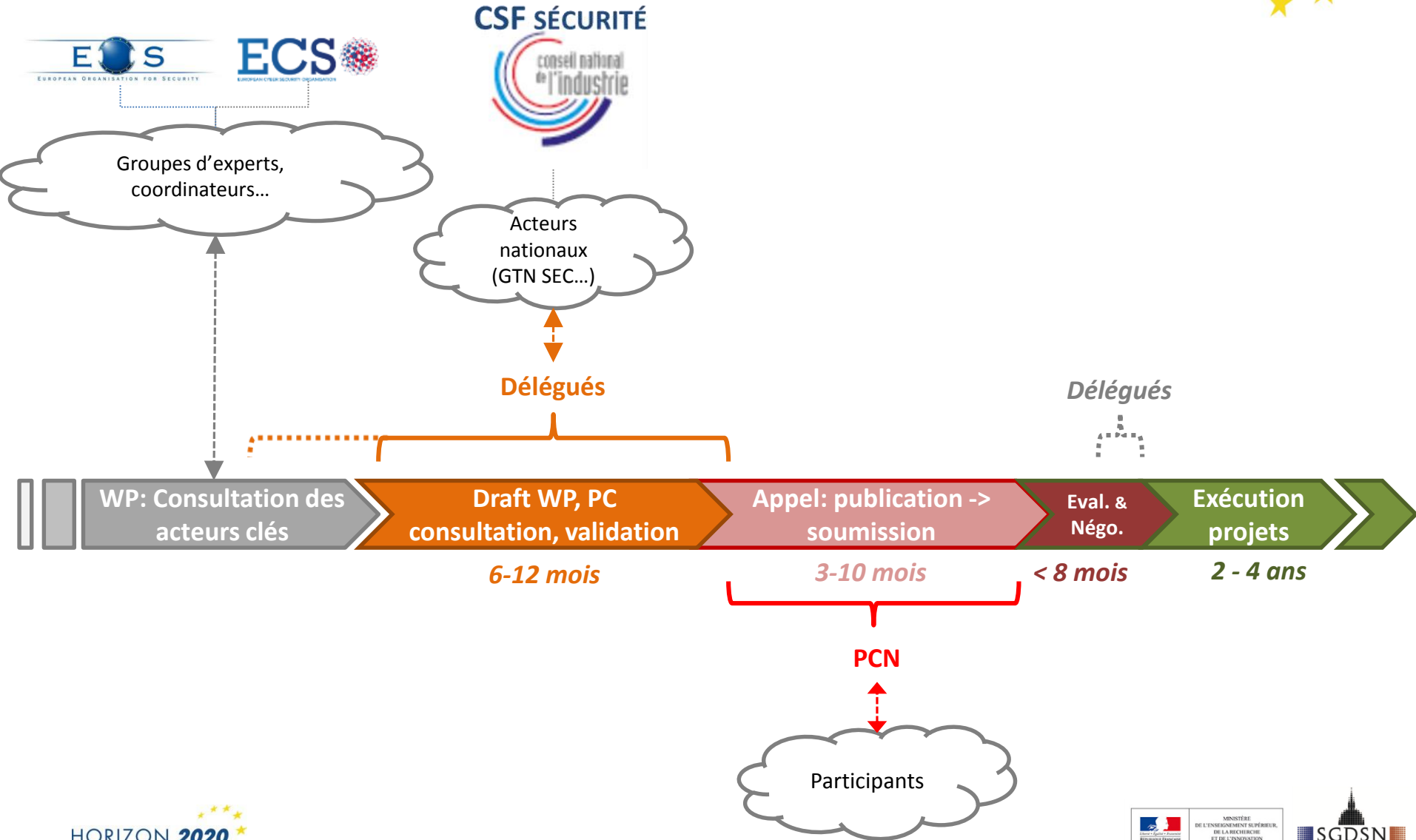
Euratom

Fission
Fusion

+ *Elargissement, Science et Société*

Institut EU
Innovation & Technologie
EIT / KIC

Mise en œuvre H2020: Le mécanisme des appels à propositions

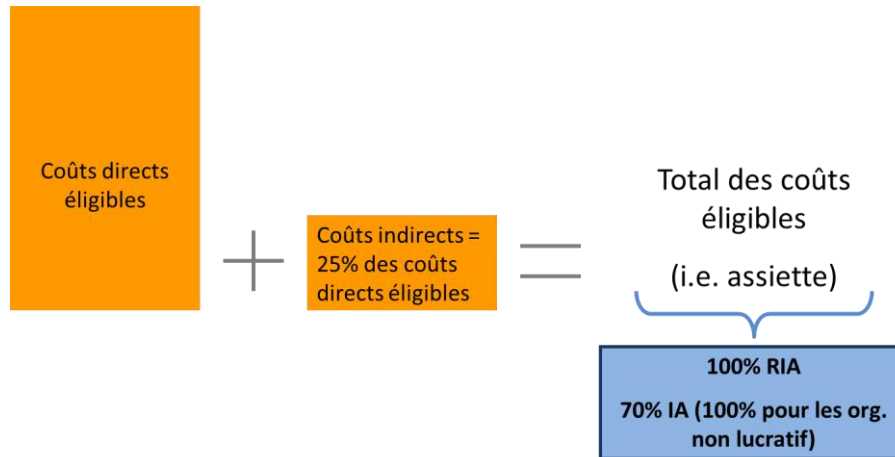


Horizon 2020: les règles de base



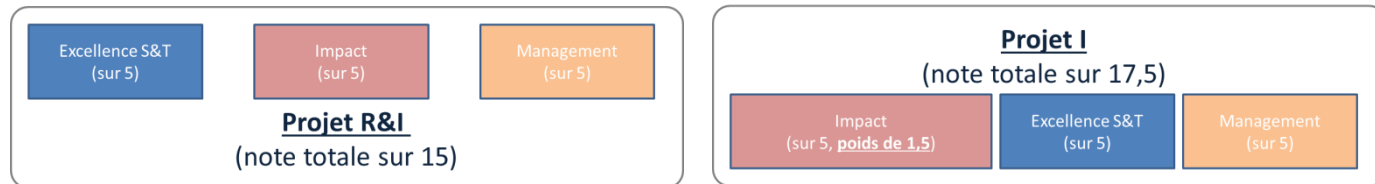
0. Des projets collaboratifs européens (min. 3 partenaires de 3 pays) en réponse à un appel (i.e. programme de travail)

1. Taux



A comparer aux taux nationaux !

2. Critères



3. Quelques autres « instruments » :

- PCP and PPI
- SME instrument, bourses (ERC, MSCA)
- *Fast Track to innovation (FTI)*

4. « time-to-grant » garanti!

LE PAYSAGE FR/UE DE LA RECHERCHE EN SÉCURITÉ



>30% de l'investissement total européen

Horizon 2020 - Défi sécurité

~1,8 Md€ sur 2014 – 2020

Sécurité et cyber-sécurité

DG Home + DG CNECT

CSF SÉCURITÉ



Agence Nationale de la Recherche
ANR

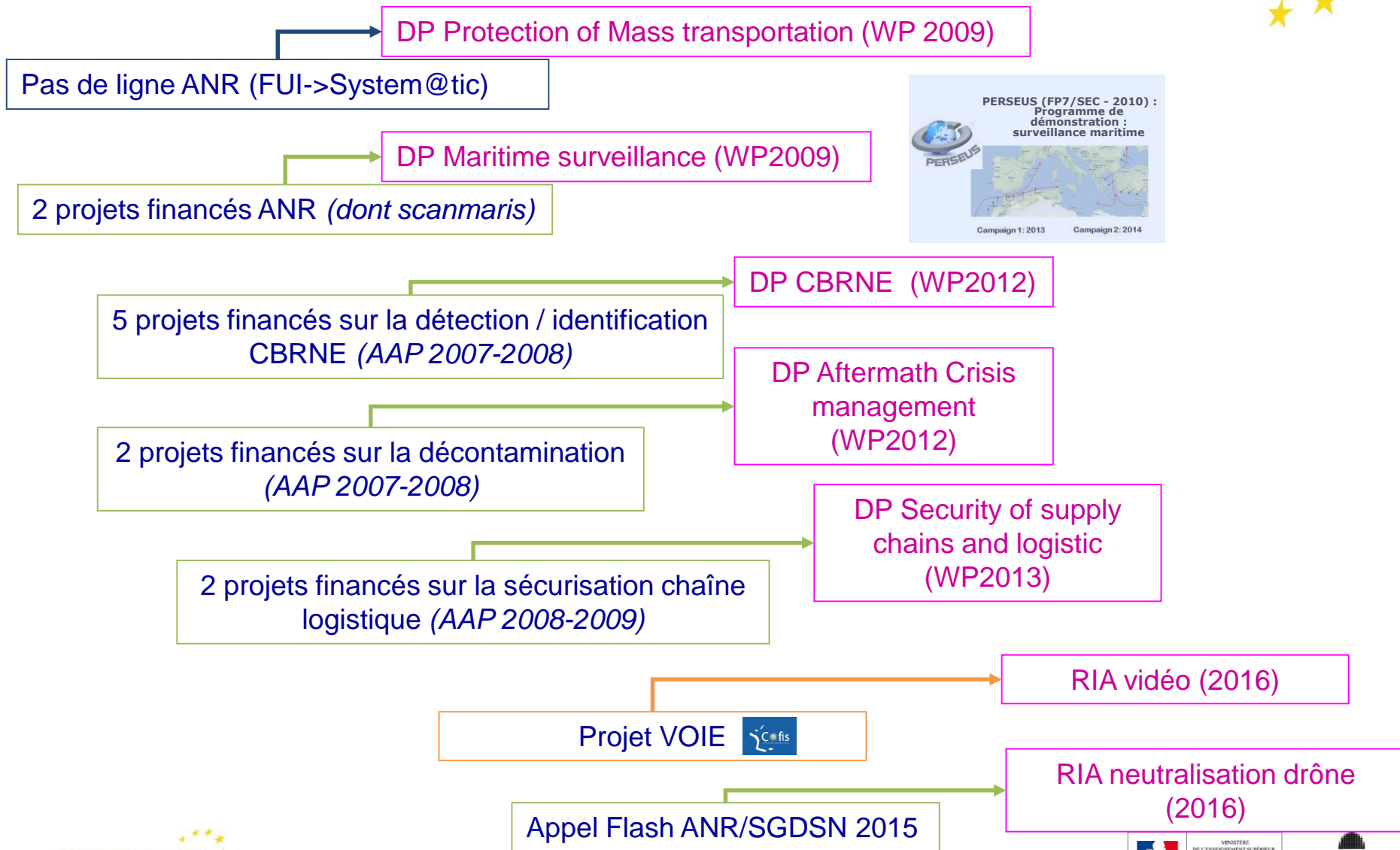
Défi 9

*Liberté et Sécurité de l'Europe,
de ses citoyens et de ses résidents*



Articulation Défi Sécurité & programmes nationaux Sécurité

PCN - Horizon2020



- ❑ Le 22 novembre 2018, le Premier ministre a labélisé la 18^{ème} filière du Conseil National de l'Industrie : la filière sécurité et cybersécurité.
- ❑ Le comité stratégique de filière (CSF) remplace les instances du CoFIS avec :
 - une nouvelle gouvernance
 - sous la présidence de l'industrie (président du CICS)
 - les pouvoirs publics resteront présents au sein du bureau et du comité plénier
 - Un contrat de filière avec des projets structurants et des activités transverses -> d'ici à l'été 2019
- ❑ Le CSF bénéficie des acquis du CoFIS et restera le lieu du dialogue public-privé au bénéfice de tous les acteurs de l'offre et de la demande.

Le programme Sécurité depuis 2007



Catalogue
des projets

2007 – 2018
~ 550 projets (collaboratifs)
➤ 2,2 Md€

~25 M€/an pour FR
~200 bénéficiaires FR dont ~65 PME

Appels 2018: éléments statistiques



□ Propositions

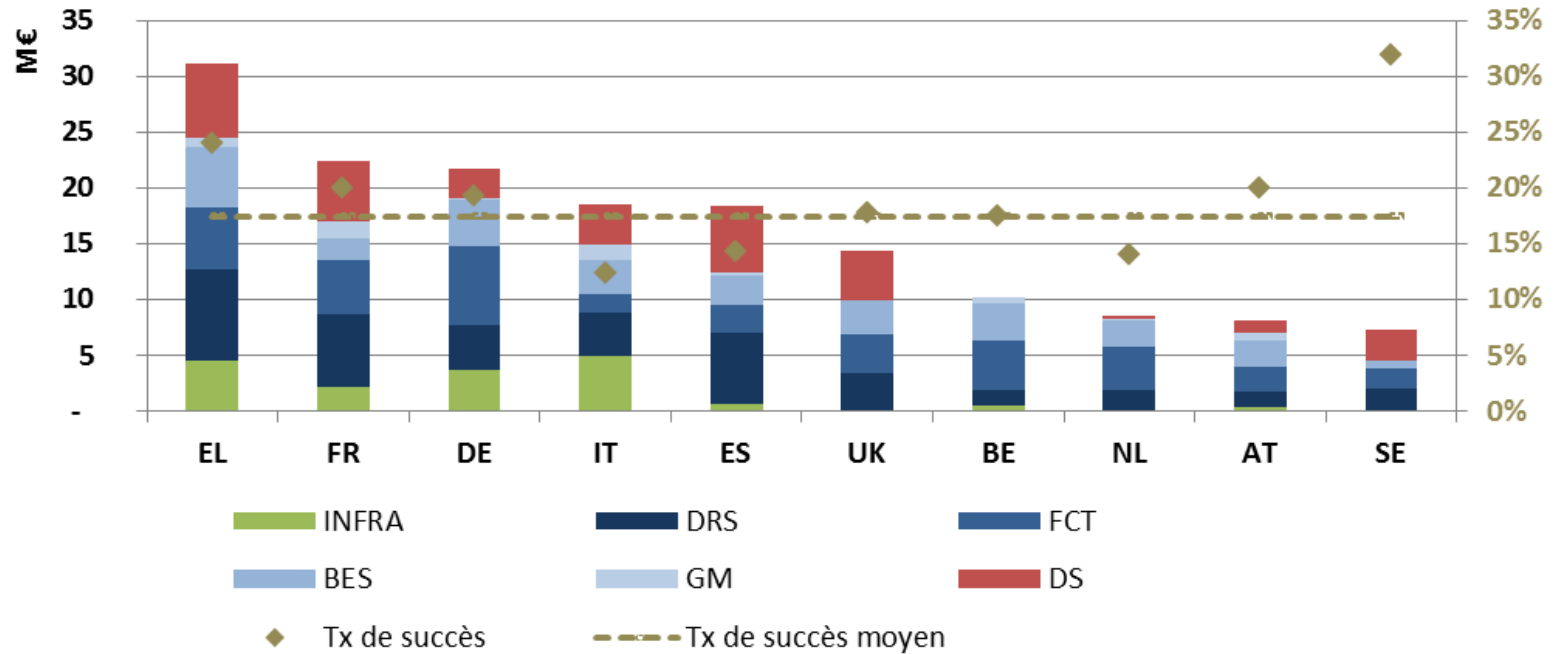
- 213 propositions éligibles dont 125 à participation FR (59%!)
 - dont 17 en coordination FR (9 RIA, 6 IA et 2 CSA)
- >3800 participations (252 FR) par ~1900 participants (123 FR)
- 1,3 Md€ demandés dont 112 M€ par FR (8,7%)

□ Projets

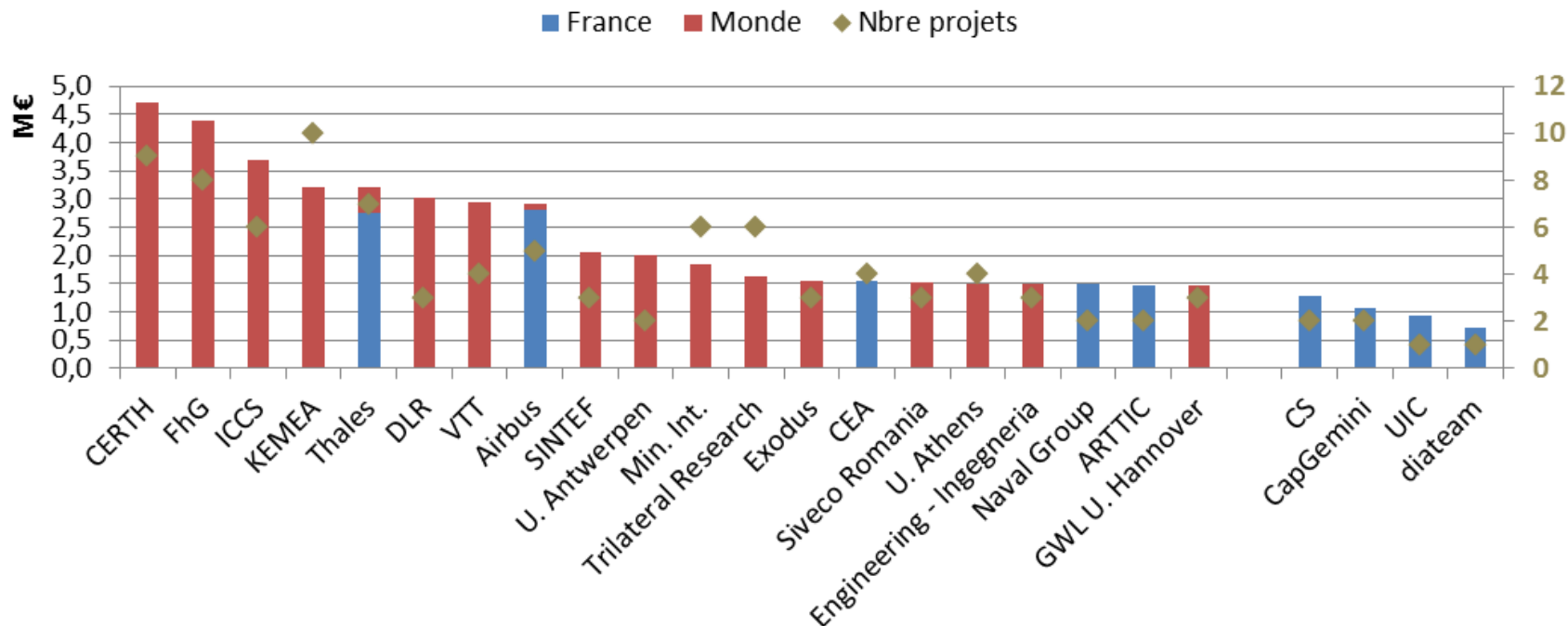
- 38 projets retenus dont 26 à participation FR (68%!)
 - dont 4 en coordination FR (2 RIA, 1 IA et 1 CSA)
- >700 participations (52 FR) par >500 bénéficiaires (32 FR)
- 225 M€ distribués dont 22,3 M€ pour FR (9,9%)
- Taux de succès moyen de 17% (FR: 20%)

Concurrence plus forte sur sujet IC:
Taux de succès de 14% sur INFRA

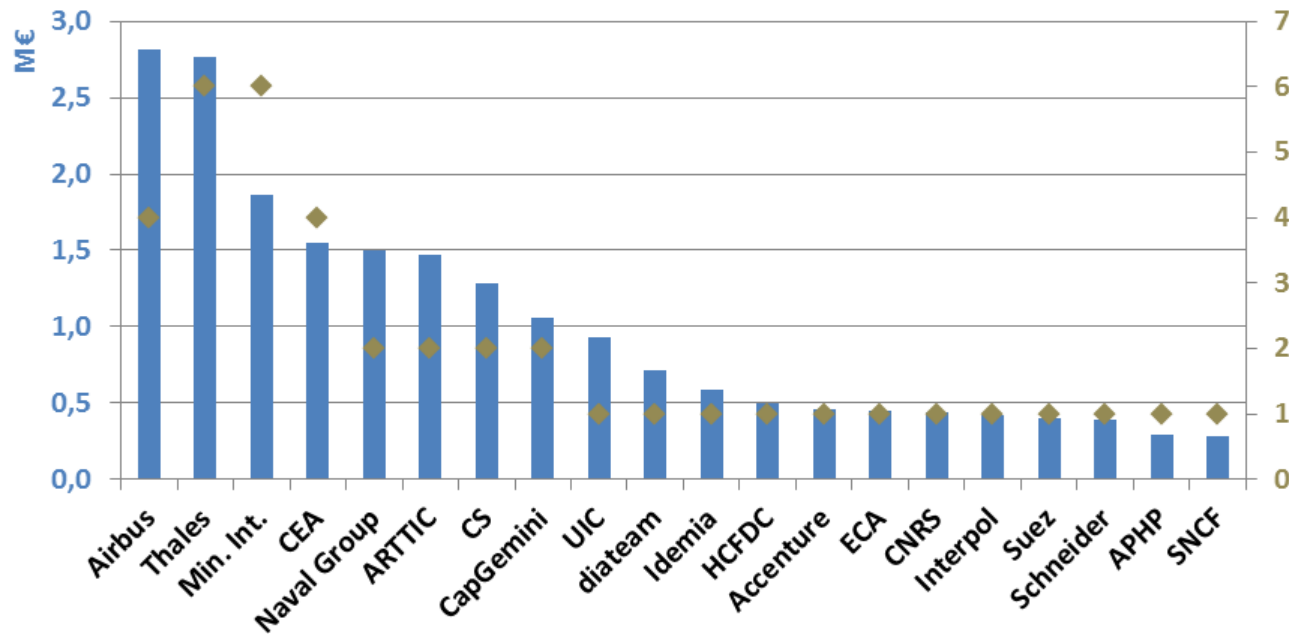
Analyse pays



Grands bénéficiaires (monde + FR)



Grands bénéficiaires FR

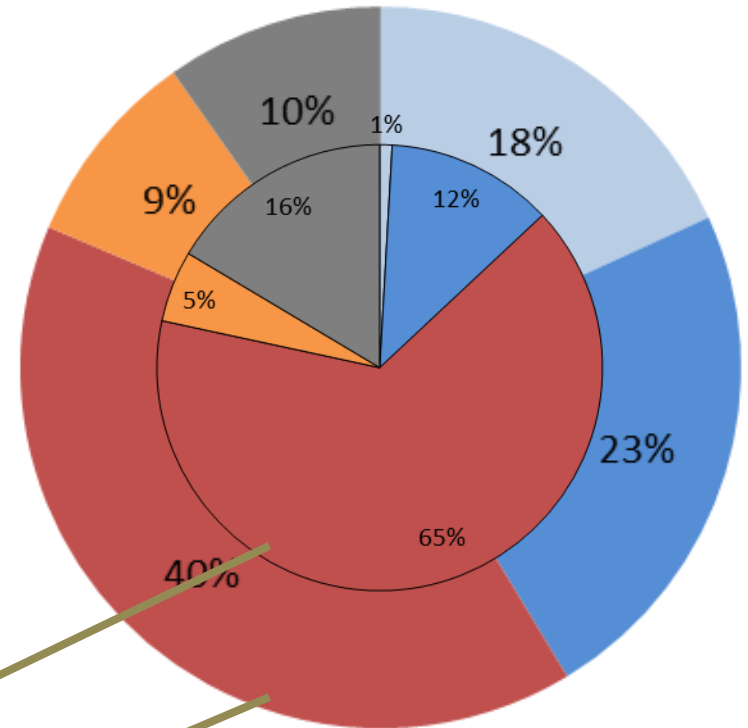
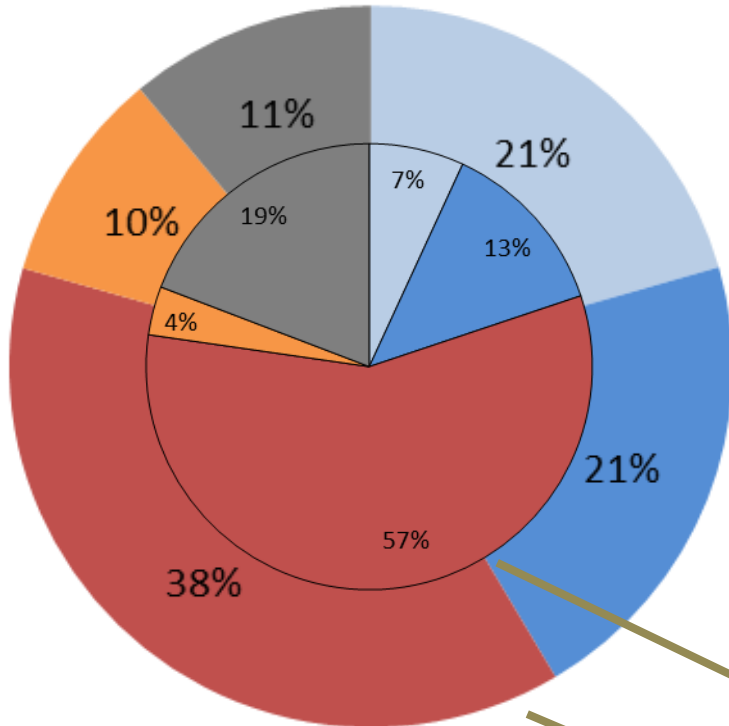


Typologie

Projets

■ HES
 ■ REC
 ■ PRC
 ■ Public Body
 ■ Other

Propositions

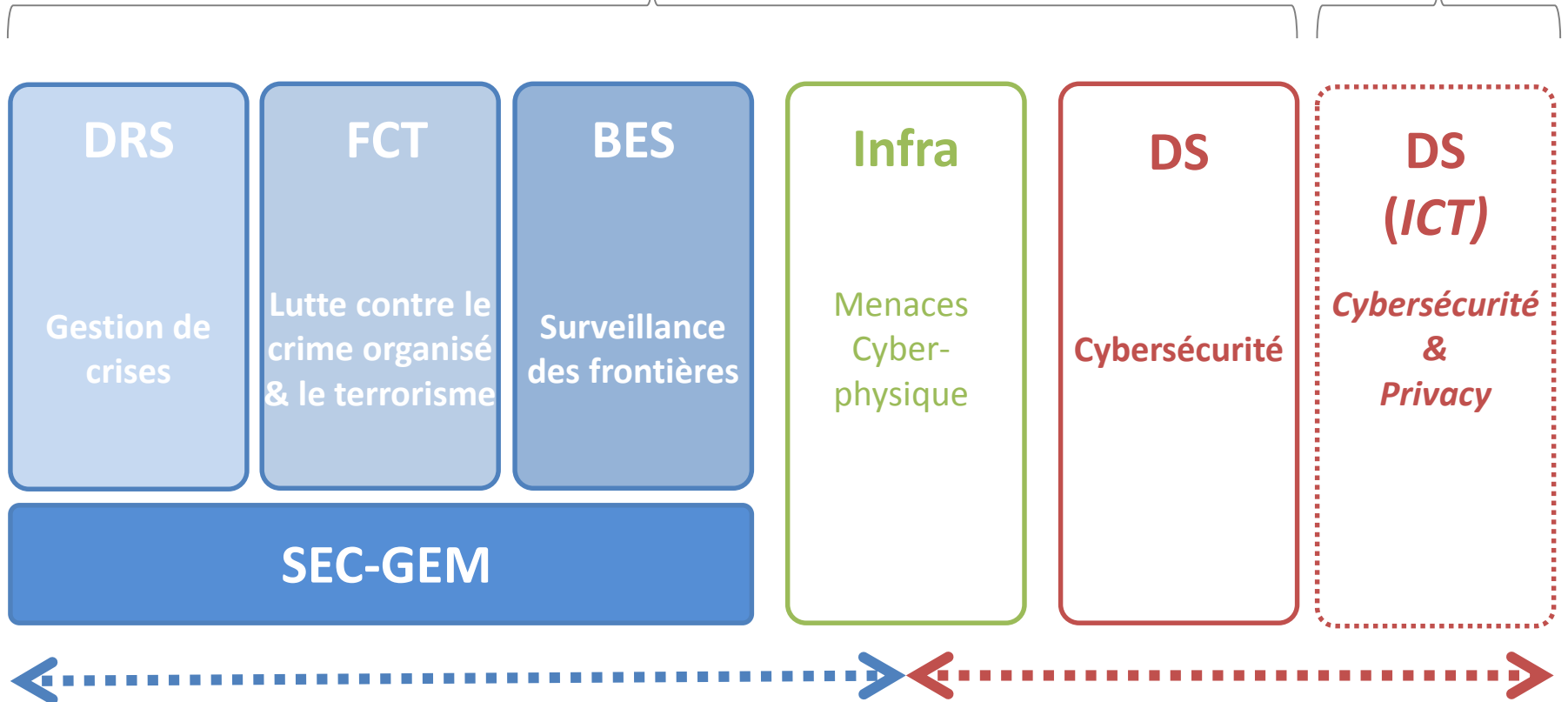


France

Monde

Structure du programme de travail 2018 - 2019/20

WP Sécurité

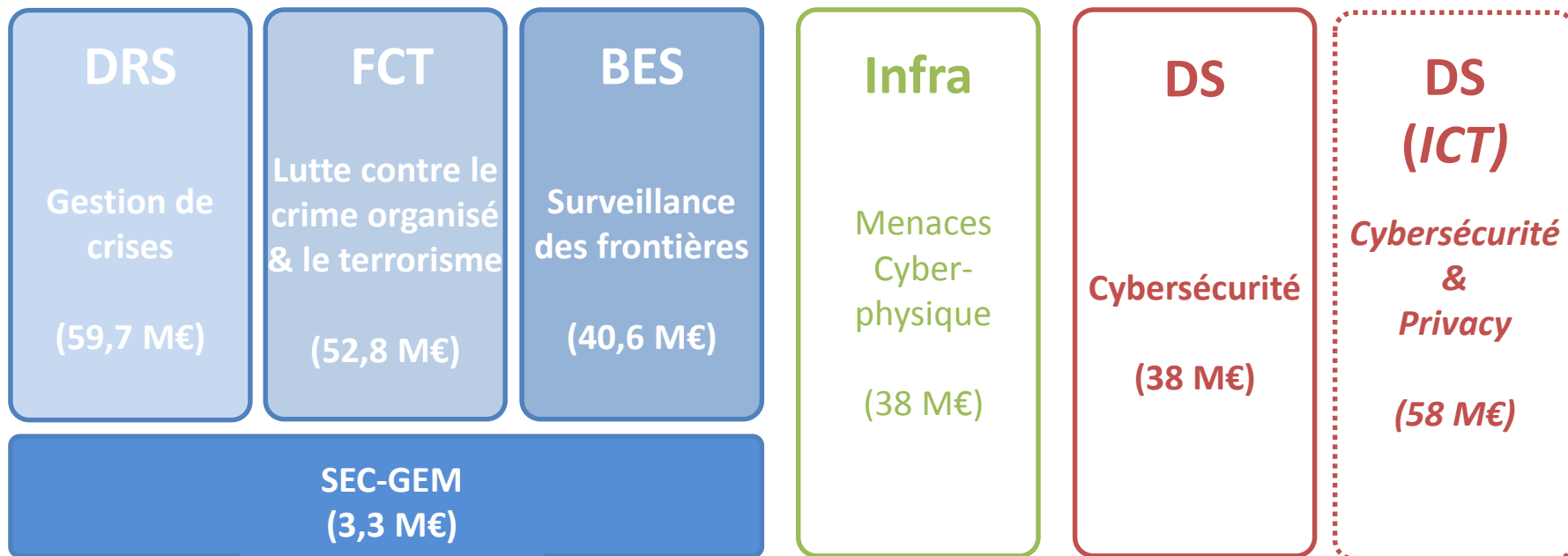


Inputs: EM + CE
Gestion: CE/DG Home
(Incl. Cybercrime)

Inputs: cPPP Cyber
Gestion: CE/DG CNECT

Budget 2019

Attention:
Modifications
post MaJ



Les sujets IC en 2019 (en bref)

- SU-INFRA01-2018-2019-2020: *Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe*
 - SU-INFRA02-2019: *Security for smart and safe cities, including for public spaces*
-
- SU-DS05-2018-2019: *Critical sectors: Privacy & accountability*

- ❑ Titre: *Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe*
- ❑ Challenge:
 - *Forecast, assess physical and cyber risks, prevent, detect, response, mitigate consequences, and achieve fast recovery (including novel installation designs)*
 - *Proposals should: physical threats and incidents; cyber threats and incidents; the cascading risks*
- ❑ Mots clés: *sécurité et résilience des installations existantes et futures; neighbouring populations and the environment, cost-effective and automated*
- ❑ 8 Secteurs: *water systems; energy infrastructure (power plants and distribution, oil rigs); transport infrastructure (airports, ports, railways, urban multimodal nodes); communication infrastructures and ground segments of space systems; health services; financial services; e-commerce and the postal infrastructure; sensitive industrial sites and plants*

Type	Output TRL	Durée Projet	Budget/proj. (M€)	Budget total (2019)	Conditions d'éligibilité
IA	7	< 24 mois	7-8	24 M€	Min. 2 opérateurs part. PME

Scope

SU-INFRA01-2018-2019-2020

Prevention, detection, response and mitigation of combined physical and cyber threats to CI in Europe

- **Scope of proposals:**

- Forecast, assessment of physical and cyber risks, prevention, detection, response, mitigation of consequences and fast recovery after incidents.
- Objective: Resilience of all functions, and of neighbouring population/envirom.

- **Proposals should:**

- Assess in detail all aspects of interdependent physical and cyber threats and incidents;
- Demonstrate the accuracy of risk assessment approaches;
- Develop real-time evidence-based security management of threats
- Provide scenarios and recommendations for policy planning, engagement of civil society and investment measures

Les projets financés en 2016-17



Scalable multidimensional situation awareness solution for protecting European ports

- 14 partenaires
- 36 mois
- Sub. CE: 6,9 M€



RESilience enhancement and risk control platform for communication infrastructure Operators

- 19 partenaires
- 36 mois
- Sub. CE: 8 M€



STOP-IT

Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats

- 23 partenaires
- 48 mois
- Sub. CE: 8,3 M€



Defending the European Energy Infrastructures

- 18 partenaires
- 36 mois
- Sub. CE: 6,8 M€



Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures

- 22 partenaires
- 36 mois
- Sub. CE: 7,8 M€



Integrated cyber-physical security for health services

SAFeguard of Critical health infrastructure

- 21 partenaires
- 36 mois
- Sub. CE: 8 M€



3 projets en 2018: réseaux de gaz, aéroports, sites Seveso



SU-INFRA02-2019-2020: Safe cities/Soft targets



- ❑ Titre: *Security for smart and safe cities, including for public spaces*

- ❑ Challenges:
 - Multiplication des menaces (e.g. terrorisme “low-cost”)
 - Mieux utiliser le potentiel des smart cities
 - Sécuriser la smart-cities vs. menaces cyber

- ❑ Mots clés: intégration et démonstrations!

- ❑ Les projets doivent contribuer à la mise en oeuvre du plan d’action “protection of public spaces” (COM(2017) 172 final).

Type	Output TRL	Durée Projet	Budget/proj. (M€)	Budget total (2019)	Conditions d'éligibilité
IA	7	< 24 mois	8	16 M€	Min. 2 villes & IND

- ❑ Titre: *Digital security, privacy, data protection and accountability in critical sectors*
- ❑ 2 sujets en 2019:
 - *Digital security, privacy and personal data protection in **multimodal transport***
 - *Digital security, privacy and personal data protection in **healthcare ecosystem***
- ❑ Scope: *[...] proposals should treat generic aspects for at least two of them, by identifying common threats and attacks, and by developing proof of concepts for managing cybersecurity and privacy risks. In addition, proposals should treat specific aspects for one of the three critical sectors/domains mentioned as sub-topics, i.e. transport, healthcare and finance [...]*

Type	Output TRL	Durée Projet	Budget/proj. (M€)	Budget total (2019)	Conditions d'éligibilité
IA	7	N/A	5 (transport) 3-4 (santé)	10 M€	PME encouragées

SU-DS05-2018-2019: Scope for sub-topics - Tackle on at least two of the following items:

Transport:

- (1): Secure access management for citizens to all types of vehicles.**
- (2): Assurance and protection in multimodal transport, addressing interconnected threats and propagated vulnerabilities.**
- (3): Standardization (allow quick adoption of best practices).**

Healthcare:

- (1) Develop dynamic vulnerability data basis; build dynamic taxonomies.**
- (2) Deliver dynamic, evidence-based, sophisticated security, privacy and personal data protection risk assessment frameworks & tools.**
- (3): Provide collaborative privacy-aware tools, advise and provide best/good practices about incident handling.**

Sites à consulter



<http://www.horizon2020.gouv.fr>



Participant Portal H2020

Liens utiles

INFORMATION

[Site français H2020 TIC](#)

[Digital Europe](#) - EUROPA

PROJET

[Portail du participant](#)

[Projet de programme de travail TIC 2016-2017](#)

RECHERCHE DE PARTENAIRE

[IDEAL-IST](#) plateforme d'idée de projet TIC

[CORDIS](#)

RESULTATS

[CORDIS](#)