



# HORIZON 2020

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

Les appels Sécurité de l'édition **provisoire**

**2016-2017**

du programme de travail  
Horizon 2020

**Armand Nacheff – CEA**

Présentation à la Cellule Mutualisée « Europe-Recherche »

Orléans

Le 25 juin 2015





2014-2020



# SÉCURITÉ DÉFI 7



MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE



# Rappel de l'architecture de Horizon 2020

## EXCELLENCE SCIENTIFIQUE

- Conseil européen de la recherche (E.R.C.)
- Actions Marie Skłodowska-Curie
- Technologies futures et émergentes (FET)
- Infrastructures de recherche

## PRIMAUTÉ INDUSTRIELLE

- TIC
- Technologies clés génériques (KET) :
  - microélectronique
  - photonique
  - nanotechnologies
  - matériaux avancés
  - systèmes de production
  - biotechnologies
- Espace
- Innovation dans les P.M.E.
- Accès au financement à risque

## DÉFIS SOCIÉTAUX

- Santé, bien-être, vieillissement
- Sécurité alimentaire, bioéconomie...
- Energies sûres, propres, efficaces
- Transports intelligents, verts, intégrés
- Climat, environnement, matières premières
- Sociétés inclusives et novatrices et capables de réflexion
- Sociétés sûres

• Diffusion de l'excellence et élargissement de la participation

• Science pour et avec la société

• Institut Européen d'Innovation et Technologie (I.E.T.)

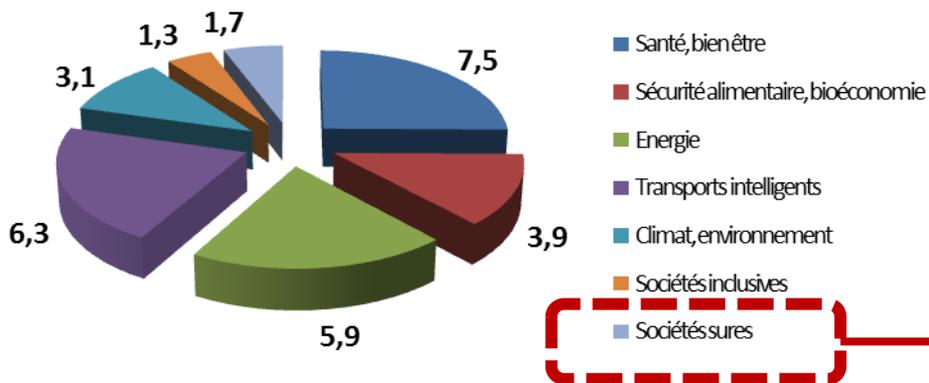
• Centre commun de recherche (Joint Research Center - J.R.C.)

E  
U  
R  
A  
T  
O  
M

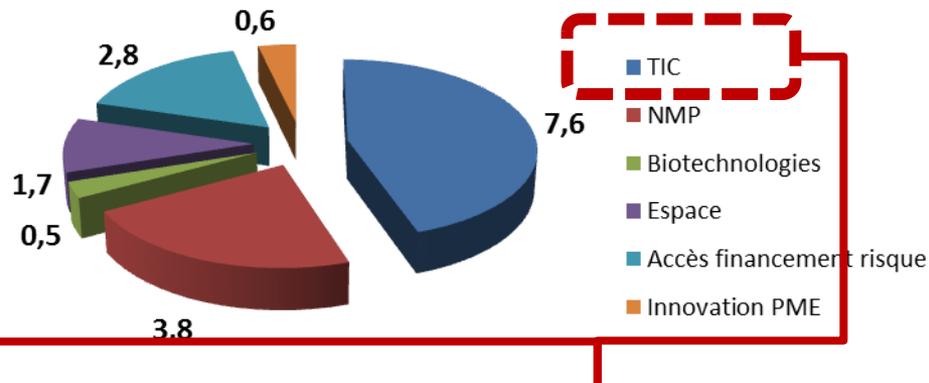


# H2020: Budget global (3)

## Défis sociétaux (Md€)



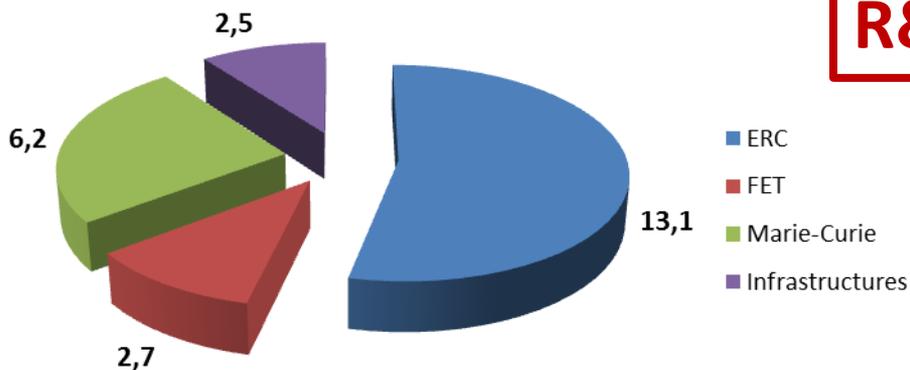
## Leadership Industriel (Md€)



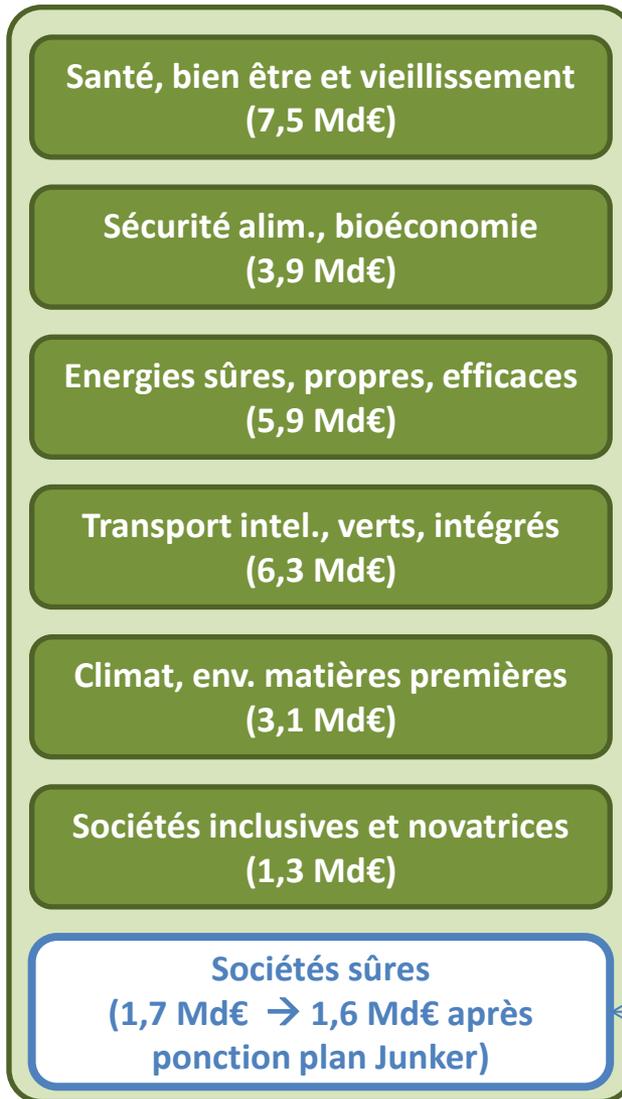
20M€/an en moyenne

**R&D Sécurité**

## Excellence scientifique (Md€)



# H2020: le pilier Défis sociétaux



Le cœur du soutien à  
la R&D Sécurité

29,7Md€



# Un programme de travail basé sur 4 appels sous la responsabilité de 2 DG

**Disaster  
Resilience  
(DRS)**

(compris €  
défi climat)

**Fight  
against  
crime and  
terrorism  
(FCT)**

**Border  
security &  
External  
security  
(BES)**

**Digital  
Security  
(DS)**

**DG HOME  
(+ DG RTD)**

**DG CNECT**

# Thèmes des 4 appels

## DRS

- Crisis mgmt
- Disaster resilience & climate change
- Critical infra. Protection (CIP)
- Com. & interoperability
- Ethical/societal dimension

## FCT

- Forensics
- LEA capabilities
- Urban security
- Ethical/societal dimension

## BES

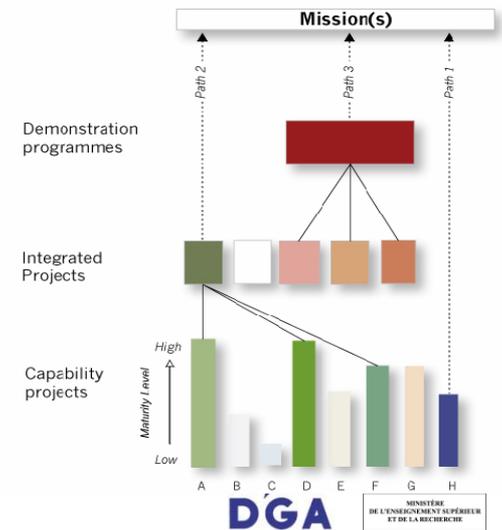
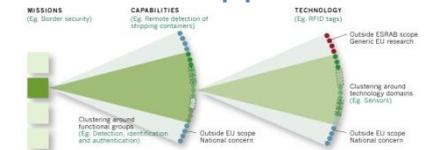
- Maritime border
- Crossing points
- Supply chain
- External sec.
- Ethical/societal dimension

## DS

- Cybersecurity
- Privacy
- Trust

# Quelques spécificités au défi 7

- ❑ Une approche « mission » et donc une implication élevée des utilisateurs finaux dans les projets
- ❑ Art. 16 Règlement H2020: le programme ne peut développer que des applications civiles, mais le développement de technologies duales est possible, voire encourager
- ❑ Une structuration toujours (plus ou moins) en ligne avec les préconisations du rapport European Security Research Advisory Board (ESRAB) de 2006 [http://ec.europa.eu/enterprise/policies/security/files/esrab\\_report\\_en.pdf](http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf)
- ❑ Une visibilité politique forte
  - Commission et agences / Etats-Membres / Parlement
- ❑ Impact sociétal
  - Privacy vs Security – enjeux normatifs et juridiques
- ❑ Pluridisciplinarité par essence
  - Dans les faits, un succès relatif vis-à-vis des SSH
- ❑ Transversalité
  - Transports, énergie, SI, santé, logistique...
  - Sécurité civile, opérateurs privés, agences européennes...
- ❑ Procédure de sécurité





# Les autres grandes directives du défi 7

## Treaty of Lisbon (13/12/2007)

<http://www.assemblee-nationale.fr/13/pdf/rap-info/i0439.pdf>

- Mise en place un système intégré de contrôle des frontières extérieures (art. 77)
- Prévention et lutte contre la traite d'êtres humains (art. 79)
- Renforcement des systèmes de prévention des catastrophes naturelles ou d'origine humaine (art. 196)
- Assistance et secours aux populations des pays tiers victimes de catastrophes, pour faire face aux besoins humanitaires (art. 214)
- Prévention de la menace terroriste sur le territoire des États membres (art. 222)

## Internal Security Strategy for the European Union (2010)

*Towards e European security model*

<http://www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=1083>

## EU Cyber Security Strategy (2013)

[http://eeas.europa.eu/policies/eu-cyber-security/cybsec\\_comm\\_en.pdf](http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf)

## European Agenda on Security (28/4/2015)

[http://europa.eu/rapid/press-release MEMO-15-4867\\_en.htm?locale=EN](http://europa.eu/rapid/press-release_MEMO-15-4867_en.htm?locale=EN)



# Programme de travail « Sociétés Sûres »

## Aspects d'implémentation

- ❑ Renforcer la coordination entre Agences Européennes : **FRONTEX, EUROPOL, ENISA, EMSA, etc.**
- ❑ Coordination plus étroite avec les activités de **l'EDA** (l'agence de la défense européennes) mais exclusivement sur les aspects civils

# Paysage FR/UE de la recherche en sécurité globale



## Programme Européen de Recherche en matière de Sécurité (PERS)



1,4 Md€ sur 2007 – 2013  
1,6 Md€ sur 2014 – 2020

'Coordination'  
via COFIS



Agence Nationale de la Recherche  
**ANR**

**Défi 9 (ex CSOSG)**  
Liberté et Sécurité de l'Europe,  
de ses citoyens et de ses résidents





# Programme de travail « Sociétés Sûres »

## Domaines spécifiques de missions

- Lutter contre la criminalité et le terrorisme (FCT)
- Protéger les frontières (BES)
- Considérer la politique de sécurité externe de l'UE (BES)
- Accroître la résilience de l'Europe aux catastrophes (DRS)
- Protéger les infrastructures critiques (CIP)
- Assurer la cyber sécurité (DS)
- Assurer la vie privée dans l'Internet et le renforcement de la dimension sociale (DS)



# Programme de travail « Sociétés Sûres »

## Les orientations principales

- ❑ Prise en compte accrue de la **dimension sociétale**
- ❑ Soutien à l'**industrie** de l'UE pour être **compétitive**
- ❑ Orientation du programme vers des **pilotes** et des **missions** de sécurité
- ❑ Renforcement de la participation des **utilisateurs finaux**



# Performances FR dans **FP7 - Sécurité**

2007-2013



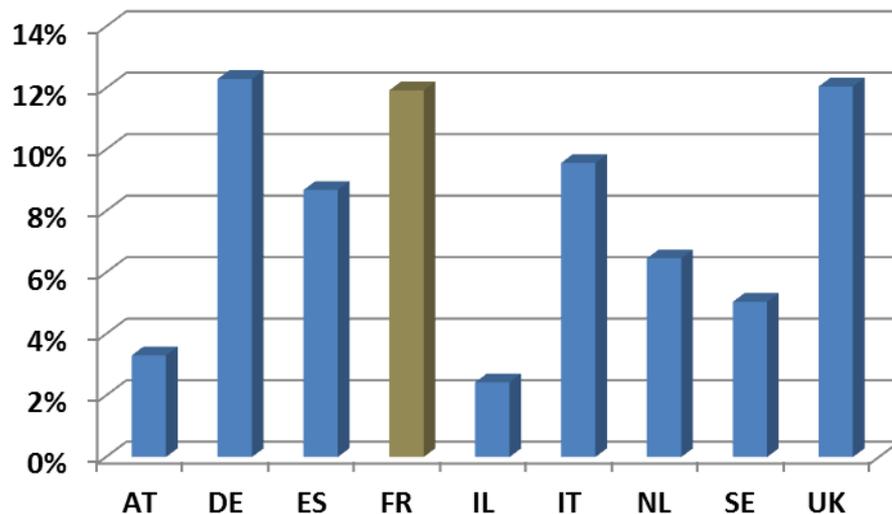


# 7<sup>ème</sup> PCRDT/PERS

## ☐ Budget PERS

- 1,4 Md€ distribués sur 7 ans avec une forte croissance du budget annuel

## ☐ France: troisième bénéficiaire avec 157 M€ capté (~30 M€/an depuis 2009)



### En absolu:

- DE: 162 M€
- UK: 159 M€
- FR: 157 M€
- IT: 126 M€
- ES: 115 M€

## ☐ 133 bénéficiaires français dont 39 PME

# Evolution de la part de la France dans le PERS avant SEC-2013



**FR (1<sup>er</sup>): 12,4%**

**FP7 2007-1 – 155 M€**  
propositions pour 1,05 Md€ demandés  
projets financés  
Un taux de succès moyen de ~14,6%

**FR (2<sup>ème</sup>): 12,9%**

**FP7 SEC-2007-1 – 20 M€**  
propositions pour 244 M€ demandés  
projets financés  
Un taux de succès moyen de ~9,2%

**FR (1<sup>er</sup>): 22,7%**

**FP7 2009-1 – 132,84 M€**  
propositions pour 719 M€ demandés  
22 projets financés  
Un taux de succès moyen de ~16,3%

**FR (2<sup>ème</sup>): 12,9%**

**FP7 SEC-2010-1 – 216,19 M€**  
propositions pour 820 M€ demandés  
projets financés  
Un taux de succès moyen de ~20,6%

**FR (3<sup>ème</sup>): 10,8%**

**FP7 2011-1 – 241,35 M€**  
propositions pour 1,07 Md€ demandés  
22 projets financés  
Un taux de succès moyen de ~17,5%

**FR (5<sup>ème</sup>): 8,3%**

**FP7 SEC-2012-1 – 241,7 M€**  
propositions pour 1,21 Md€ demandés  
56 projets retenus (liste principale)  
Un taux de succès moyen de ~19,5%

**FR (3<sup>ème</sup>): 9,4%**

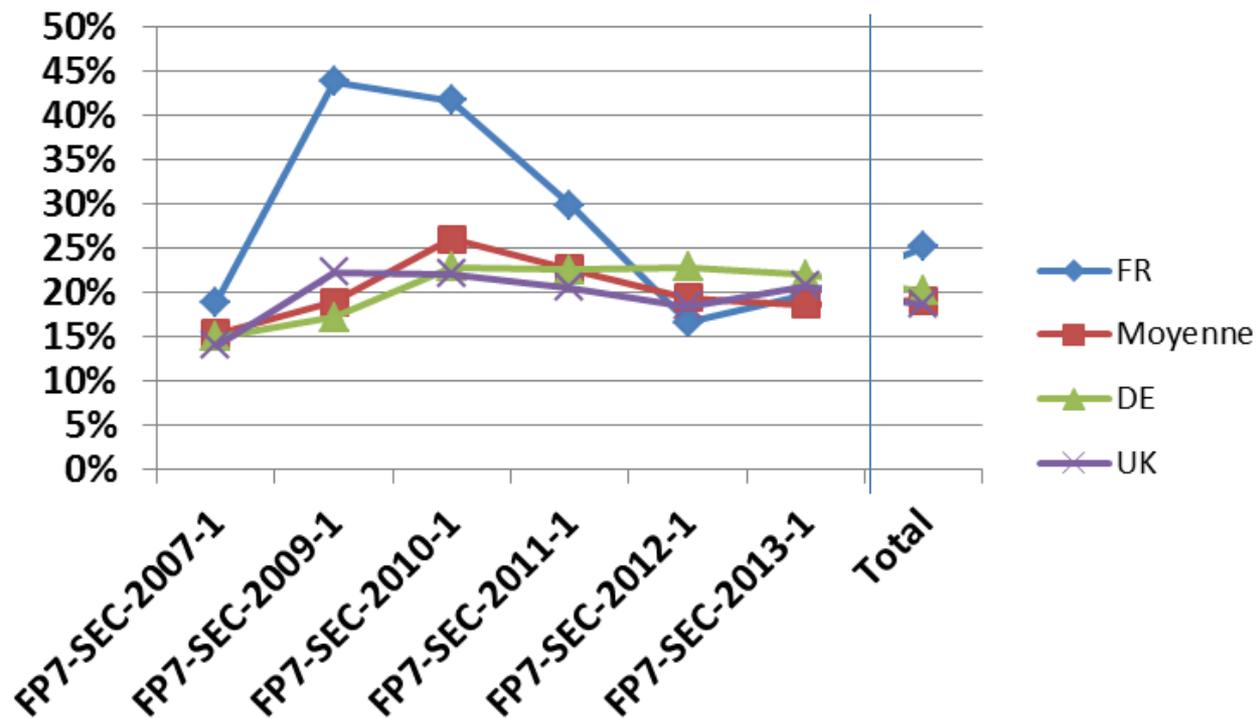
**FP7 2013-1 – 299,33 M€**  
propositions pour 1,6 Md€ demandés  
projets retenus (liste principale)  
Un taux de succès moyen de ~18,6%



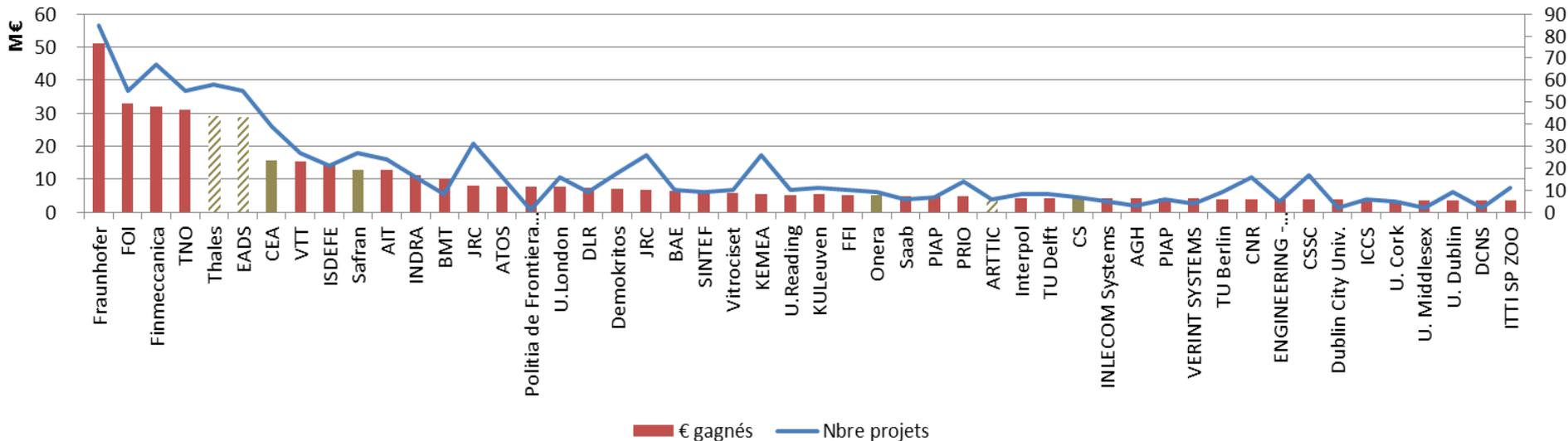
# Performances françaises dans le 7<sup>ième</sup> PCRDT (FP7)

Une baisse du retour FR causée par une dégradation du taux de succès (€)

(taux de succès coordination FR supérieur 28,2% vs. 18,5% DE vs. 18,8% UK)



# Grands bénéficiaires européens dans FP7



**Top 10** : 4 FR (Thalès, EADS, CEA, Safran)

**Top 20** : 4 FR

**Top 50** : 8 FR (Onera, ARTTIC, CS, DCNS)

**Une participation des universités FR  
(en particulier communauté SHS)  
insuffisante**

**Sur le 119 M€ alloués à l'activité SHS  
Retour FR: 7%**

**2 M € captés par les Universités  
3,4 M € par les Universités + CNRS**



2014-2020

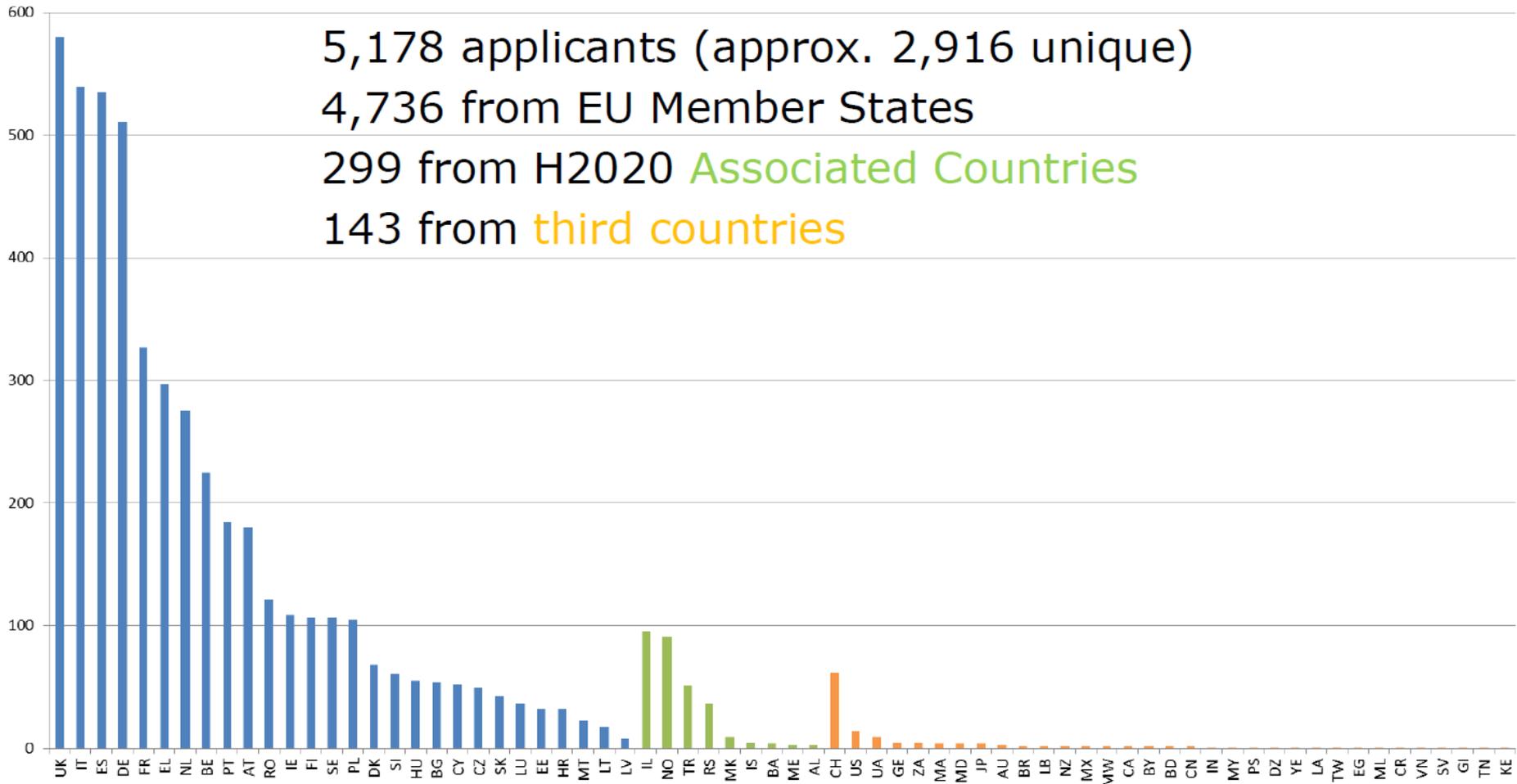


# SÉCURITÉ RÉSULTATS 2014



# Participation des organisations à H2020 défi 7 en 2014

5,178 applicants (approx. 2,916 unique)  
4,736 from EU Member States  
299 from H2020 **Associated Countries**  
143 from **third countries**





# Soumission de dossiers en 2014 à H2020-défi 7

- 453 Proposals received
- 6 proposals found ineligible (3 declared out of scope by the evaluators)
- 3 proposals were found inadmissible
- 2 proposals were transferred between topics on request of the coordinator (wrong submission)

Call	Proposals	Topics	MEUR	Prop/MEUR
<b>BES</b>	26	3	20,78	1,3
<b>DRS*</b>	173	10	73,4	2,4
<b>FCT</b>	146	8	56,77	2,6
<b>DS</b>	108	3	47,04	2,3
<b>Total</b>	<b>453</b>	<b>25</b>	<b>197,99</b>	<b>2,3</b>

\***DRS:** all except topic DRS-17 (managed by EASME separately)

# H2020 défi 7

## Résultats 2014 par topiques

	Below threshold	Above threshold below budget	Within call budget	Total
BES-09-2014	9	1	1	11
BES-12-2014	3	4	1	8
BES-14-2014	5	0	1	6
DRS-02-2014	10	3	1	14
DRS-04-2014	3	1	1	5
DRS-05-2014	7	2	0	9
DRS-07-2014	30	15	3	48
DRS-08-2014	0	0	1	1
DRS-09-2015	20	17	3	40
DRS-16-2014	8	4	1	13
DRS-19-2014	7	4	2	13
DRS-20-2014	1	0	0	1
DRS-21-2014	15	7	4	26
DS-01-2014	25	19	5	49
DS-02-2014	16	12	3	31
DS-06-2014	16	8	2	26
FCT-05-2014	7	4	2	13
FCT-07-2014	13	13	3	29
FCT-08-2014	0	1	0	1
FCT-10-2014	22	14	1	37
FCT-11-2014	1	4	0	5
FCT-12-2014	4	8	0	12
FCT-13-2014	8	7	1	16
FCT-14-2014	14	11	5	30
<b>Total</b>	<b>244</b>	<b>159</b>	<b>41</b>	<b>444</b>



# Horizon 2020

## Résultats de l'appel « Sociétés Sûres » 2014

❑ 404 propositions soumises

❑ Demande totale de 1,681 Md €

❑ 2550 proposants individuels

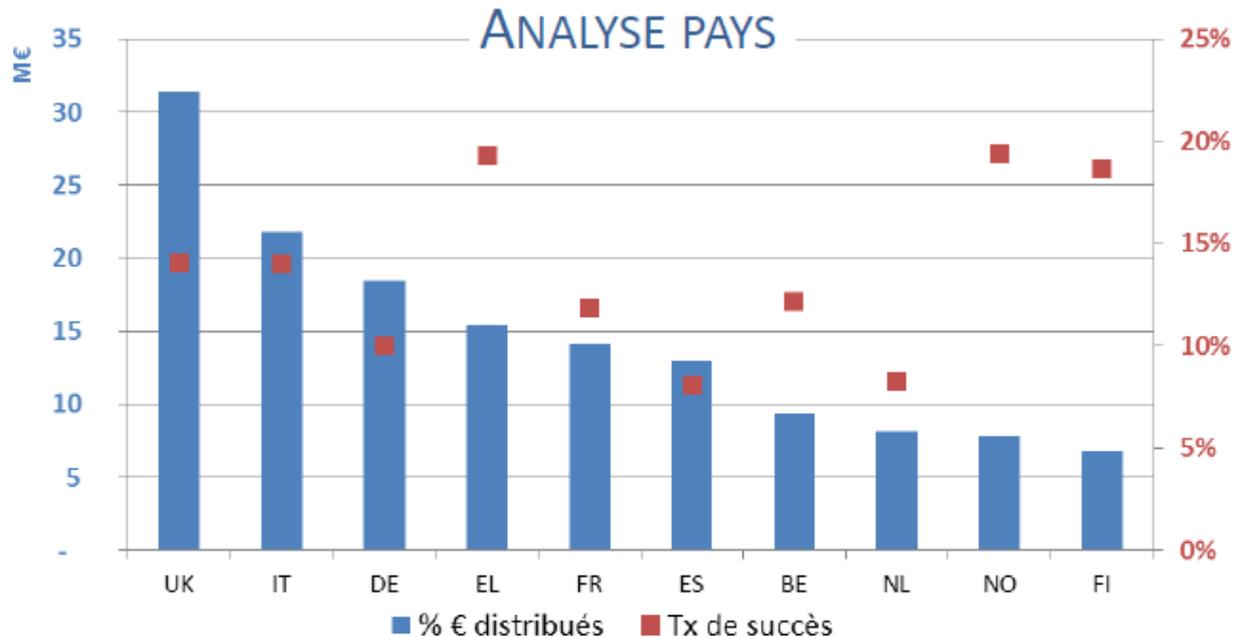
❑ Taux de succès moyen

→ 38 + 8 projets retenus

→ 193 M € de subvention

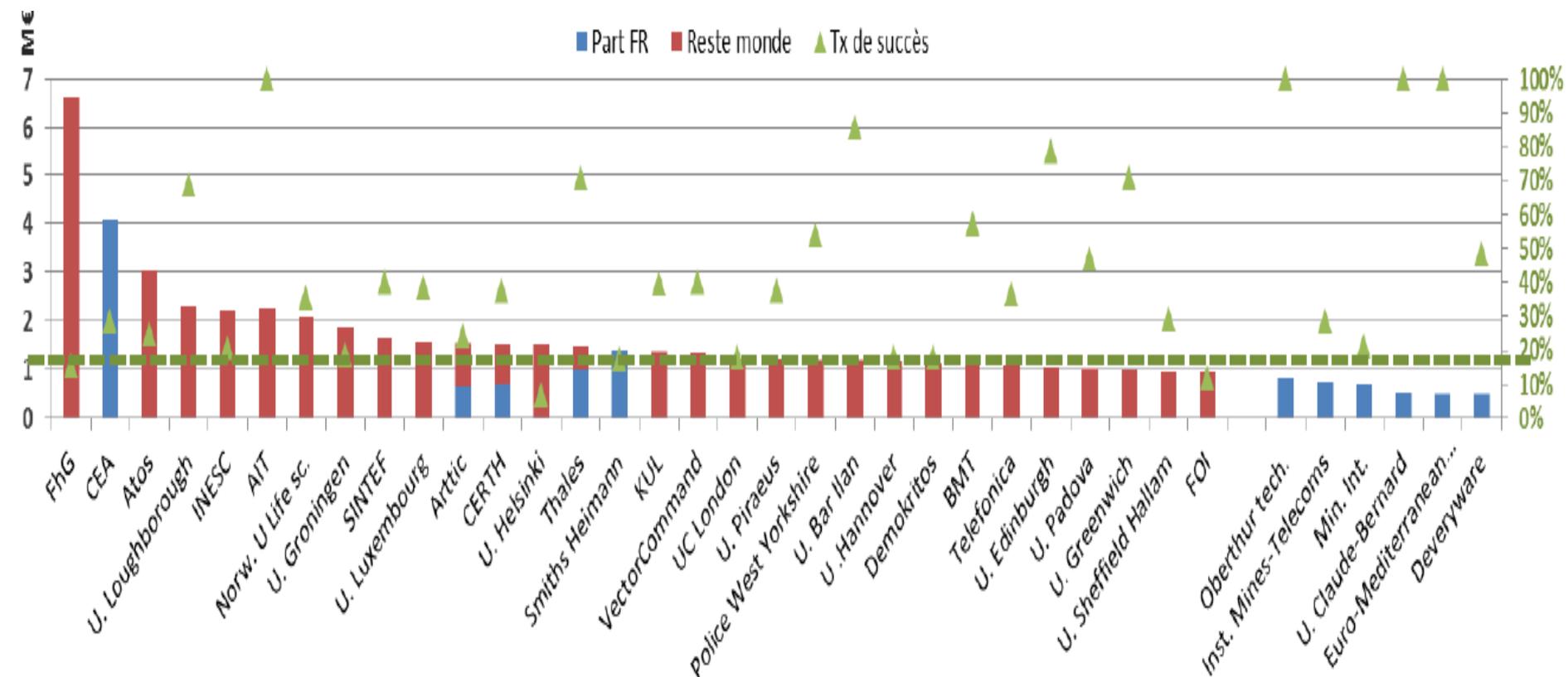
→ 453 bénéficiaires

→ 11,5%



# Horizon 2020 – Appel « Sociétés Sûres » 2014

## Résultats par organisme

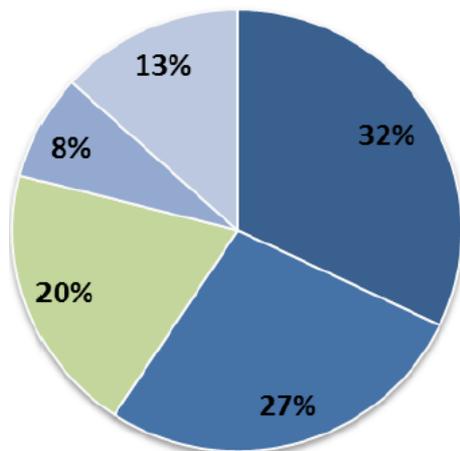


# Typologie des participants et bénéficiaires FR

## ☐ France

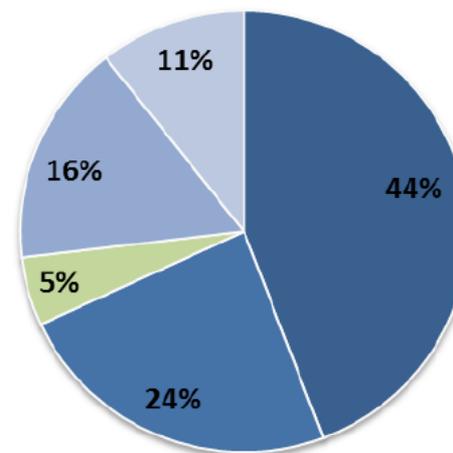
- 7,1% de la demande totale
- 7,3% des financements captés
- 161 participants dans 152 propositions
- 22 bénéficiaires dans 17 projets

### Proposants



■ Lab. Publics  
■ IND  
■ PME  
■ End-user  
■ Autre

### Bénéficiaires





2014-2020



SÉCURITÉ  
2015



# Un WP basé sur 4 appels

Une date de clôture unique: 27 août 2015

## DRS

- Crisis mgmt
- Disaster resilience & climate change
- Critical infra. protection
- Com. & interoperability
- Ethical/societal dimension

69,13 M€  
(+28 M€)

## FCT

- Forensics
- LEA capabilities
- Urban security
- Ethical/societal dimension

42,16 M€

## BES

- Maritime border
- Crossing points
- Supply chain
- External sec.
- Ethical/societal dimension

42,17 M€

## DS

- Cybersecurity
- Privacy, Trust

50,21 M€



# Horizon 2020 – Appel 2015 « Sociétés Sûres »

☐ Date limite de soumission pour « Sociétés Sûres »

Le **27/08/2015**

à **17h** (heure locale de Bruxelles)



2014-2020



# SÉCURITÉ PROGRAMME DE TRAVAIL 2016-2017





# Les grandes lignes du **draft** du programme de travail 2016-17 Défis sociétaux

## ❑ Une structure sur 3 appels principaux

- Protection des infrastructures critiques
- Sécurité
- Sécurité numérique

CIP (DG CNECT + Home)  
FCT, BES, DRS (DG Home)  
DS  
et topiques du défi1 (DG CNECT)

## ❑ Budget 2016-17:

- Brut:
- Après taxes (FTI, Juncker...) et contribution Etats Associés :

~437 M€ dont 108 M€ pour DG CNECT

~**370 M€** (vs ~332 M€ 2014-15)



# Principaux changements

## WP 16-17 par rapport au WP14-15

- ❑ Un nombre de sujets plus limité (~30 vs. 55)
  - 5 DS
  - 1 CIP en 2016 et 2017
  - 5 DRS
  - 7 FCT
  - 8 BES
  - 3 GM
  -
- ❑ Des enveloppes réservées pour une majorité de sujet
  - pas de compétition entre ces sujets
  - des budgets par projet plus prescriptifs
- ❑ Une plus grande participation attendue des utilisateurs finaux / *practitioners*
  - TRLs jusqu'à 8 !



# DS

Les numérotations des topiques peuvent encore changer





# DS1 – 2016 Cyber Sécurité pour les

**A) PME's, B) administrations publiques locales , C) Particuliers**

## ❑ Challenge

- 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

## ❑ Scope

- 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

## ❑ Expected Impact

- Augmentation de la compétitivité et de l'efficacité des produits européens de cyber sécurité des TIC
- Augmentation de la résilience des organismes

## ❑ Action d'Innovation (IA)

❑ **3-4 M€, TRL 5-7, budget de 20 M€**



# DS2 – 2016 *L'économie de la cyber sécurité*

## □ Challenge

- Les échecs en cyber sécurité doivent être compris des points de vue technique, sociétal, institutionnel et économique.
- Les menaces ne sont pas adéquatement couvertes par les structures institutionnelles ou par des cadres d'incitations (financières ou réglementaires, positives ou négatives)

## □ Scope

- 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
- les propositions doivent couvrir un des deux volets:
  - A. Cadre des coûts-avantages de la cyber sécurité (investissement optimal en sécurité)
  - B. Incitations et modèles d'affaires

## □ Expected Impact

- Amélioration de la compréhension sociétale des défaillances de la sécurité de l'information
- Amélioration de l'investissement fondée sur les risques, dans la sécurité de l'information.
- Résilience sociétale accrue
- Progrès au delà de l'état de l'art dans les modèles de l'économie de la sécurité de l'information

□ **Action de Recherche et d'Innovation (RIA) : 1-2 M€, TRL 3-5, budget de 4 M€**



# DS3 - 2016 *Coopération de l'UE et dialogues internationaux sur la cyber sécurité et sur la recherche et l'innovation dans le domaine de la vie privée*

## Challenge

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

## Scope : 3 sous-sujets:

- I. Les synergies entre H2020 et les activités de l'UE et des clusters
- II. Le dialogue international avec le Japon
- III. Le dialogue international avec les USA

## Expected impacts

- Identifier et hiérarchiser les sujets de R & I dans l'UE.
- Favoriser et promouvoir les activités européennes en cyber sécurité
- Augmenter la visibilité internationale des activités de l'UE en cyber sécurité
- Identifier des approches communes européennes et internationales pour relever les défis de la cyber sécurité de points de vue R & I, institutionnel et gouvernance.

## Action de Coordination et de Support (CSA)

## 1 M € pour (I), 0,5 M € pour (II) et 0,5 M € pour (III)

# DS4 – 2017 (A)

## Protection avancée contre les menaces cyber sécurité et leurs acteurs

### Challenge

- 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.

### Scope : A) RIA – Appréciation de la situation

- développement de nouvelles 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 médico-légales**
- garanti des droits fondamentaux, de la protection des données et de la vie privée, pendant la conception et développement des solutions

### Expected Impact

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

### A. “Appréciation de la situation” : RIA, 2-3 M€ / projet, TRL 3-5, budget de 10 M

# DS4 – 2017 (B)

## Protection avancée contre les menaces cyber sécurité et leurs acteurs

- ❑ Scope : **B)** IA - 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
  - Les propositions doivent répondre aux besoins spécifiques de l'utilisateur final publique et / ou privé
- ❑ Expected Impact
  - Préparation des personnes chargées de défendre les systèmes des TIC contre les menaces avancées dans des scénarios à haut risque
- ❑ **B)** Environnements de simulation et Formation  
**IA: 4-5 M€ / projet, TRL 5-7, budget de 10 M€**

### C) CSA

## Protection de la vie privée et des données et identités numériques

### □ Challenge :

- *Des données personnelles des utilisateurs sont souvent divulgués aux services. Par exemple, les mots recherchés sur des moteurs de recherche peuvent laisser des traces sensibles.*
- *La mise en œuvre du draft sur la régulation générale 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.*

# DS5 – 2017 (bis)

## Protection de la vie privée et des données et identités numériques

- ☐ Scope : 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 auditable 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



# SMEInst-XX -2016-2017

- SMEInst-XX -2016-2017: *Innovative European SMEs in cybersecurity*

**9 M€**



# Autres Appels liés à DS



## □ Partie LEIT/ICT:

- DS1 – 2016:  
*Assurance and Certification for Trustworthy and Secure ICT systems, services and components*
  - RIA: 3-4 M€, budget de 13,5 M€
  - IA: 3-4 M€, budget de 9 M€
  - CSA: 1 M€
- DS2 – 2017:  
*Cryptography*
  - RIA: 3-5 M€, budget réservé de 17 M€
  - 1 CSA de 0,5 M€

deadline  
**12 avril 2016?**

## □ Partie SC1

- PM 17 – 2016:  
*Increasing digital security of health related data on a systemic level*
  - RIA

Attention deadline  
**16 février 2016**



# CIP

Les numérotations des topiques peuvent encore changer

# Critical Infrastructure Protection (CIP)

☐ CIP 1 – 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.*

- TRL à l'issue des projets : **7**
- Budget total de l'action : **20 M€/an**
- Budget par projets : **~8 M€/projet** (soit 2 à 3 par an)
- Type d'action: **IA**
  
- 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:
  - *Water Systems,*
  - *Energy Infrastructure (power plants and distribution),*
  - *Transport Infrastructure and means of transportation.*
  - *Communication Infrastructure,*
  - *Health Services,*
  - *Financial Services.*

Sujet Protection du transport aérien éligible



# DRS

Les numérotations des topiques peuvent encore changer



# Disaster-Resilience: safeguarding and securing society (DRS) (1)

## □ DRS 1-2016: *Integrated tools for response planning and scenario building*

- **IA, 8 M€, TRL 7-8, max. 2 projets,**
- participation obligatoire des end-users suivants :
  - **firefighting units,**
  - **medical emergency services,**
  - **police departments,**
  - **civil protection units,**
  - **control command centres**

## □ DRS 2-2016: *CSA on situational awareness systems to support civil protection preparation and operational decision making*

- **CSA, 1,5 M€, TRL 6-8, max. 1 projet,**
- Règles additionnelles de propriété intellectuelle



# Disaster-Resilience: safeguarding and securing society (DRS) (2)

- ❑ DRS 3-2016: *Validation of biological toxins measurements after an incident: Development of tools and procedures for quality control*
  - **IA, 8 M€, max. 1 projet,**
  - au moins 3 labos de contrôle
  
- ❑ DRS 4-2017: *PCP for broadband communication systems*
  - **PCP, 10 M€, max. 1 projet, TRL 8,**
  - un seul projet réunissant **entre 8 et 12 Etats Membres,**
  - Règles additionnelles de propriété intellectuelle
  
- ❑ DRS 5-2016: *CBRN cluster*
  - **2016: CSA de 1,5 M€** sur une durée minimale de 3 ans
  - **2017: RIA, TRL4-8, projets de ~3,5 M€, max. 4 projets, coordination PME**



# FCT

Les numérotations des topiques peuvent encore changer



# FCT 1-2016 (1)

## ☐ FCT 1-2016: *Developing a comprehensive approach to violent radicalization in the EU from early understanding to improving protection*

### ▪ Challenge :

*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 aux défis de lutte contre l'extrémisme violent.*

*Les groupes terroristes utilisent les dernières avancées des technologies pour diffuser la propagande et alimenter les comportements radicaux, cependant les techniques traditionnelles d'application de la loi restent insuffisantes pour faire face à ces nouvelles tendances de radicalisation violente.*

*Les sociétés démocratiques sont attachées à la liberté de pensée - même la pensée radicale - tout en protégeant la société des actions illégales des groupes et individus radicalisés et violents.*

# FCT 1-2016 (2)

## ☐ Scope

**Traitement holistique et multidisciplinaire** pour la prévention et la lutte contre la radicalisation.

Les facteurs constituant un processus de radicalisation violente sont nombreux :

1) familial, 2) social, 3) socio-économique, 4) psychologique, 5) religieuse, 6) idéologique, 7) historique, 8) culturel, 9) politique, basés sur des propagandes, des medias sociaux ou sur Internet.

**Comprendre comment les réseaux et les groupes agissent pour radicaliser des individus.**

Les individus radicalisés, s'organisent de différentes manières:

1) centralisées et hiérarchisées; 2) en réseaux; 3) par petits groupes basés en Europe ou à l'étranger; 4) des cellules; 5) acteurs isolés opérant de façon imprévisible et moins contrainte.

une meilleure compréhension des causes et des processus peut conduire à des solutions innovantes, pour contrer des actions violentes prises par des individus radicalisés.

- politiques pour prévenir l'extrémisme violent;
- contre-communication diffusés soit en ligne (YouTube, forums spéciaux, Twitter, etc.) ou hors ligne (dans la salle de classe par exemple),

**Alors que sociétal Défi 6 se concentre principalement sur l'étude du phénomène de radicalisation, les propositions sur ce topique devraient se concentrer sur l'élaboration de recommandations**

**politiques et de solutions pratiques à mettre en œuvre par les utilisateurs finaux de sécurité.**

☐ RIA, 3 M€/projet,

☐ Agences repressives (LEA) d'au moins 5 Etats Membres

# Fight against crime and terrorism (FCT) (1)

- FCT 2-2016-2017: *Human Factor for Prevention, Investigation, and Mitigation of criminal and terrorist acts*
  - **RIA, 3 M€/projet, 5 sous-topiques,**
  - **Police Technique et Scientifique (forensics lab) d'au moins 5 Etats Membres**
  - **max. 2 projets en 2017**
  
- FCT 4-2017: *PCP of toolkits integrating tools and techniques for forensic laboratories*
  - **PCP, 10 M€, TRL 8, max. 1 projet,**
  - **Agences repressives (LEA) d'au moins 5 Etats Membres**
  
- FCT 5-2017: *Integration of detection capabilities and data fusion with **utility providers' networks***
  - **IA, 8 M€/projet, max. 2 projets,**
  - **TRL 7-8 sur les capteurs et TRL 6 sur les systèmes d'information et de contrôle et plateforme mobile,**
  - **au moins 2 opérateurs et 3 unités de contreterrorismes ou démineurs de 3 Etats Membres,**
  - **démonstration dans au moins 2 villes de 2 EM utilisant des syst. égoûts différents**



# Fight against crime and terrorism (FCT) (2)

- FCT 3-2016: *Forensics techniques on: a) trace qualification, and b) broadened use of DNA*
  - **RIA, 5 M€/projet, TRL 5,**
  - implication de **PST (forensic lab)** d'au moins 5 EM
- FCT 6-2016: *Detection techniques on explosives: Countering the use of an explosive threat, across the timeline of a plot*
  - **RIA, 5 M€/projet, max. 1 projet,**
  - lien avec EDA,
  - au moins **3 unités anti-terroristes** de 3 EM
- FCT 7-2016-7: *Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism*
  - 1: cyber-crime: virtual/crypto currencies des-anonymisation/tracing/impairing... (Deep Web)
  - 2: Light drone/UAV
  - : Video analysis
  - 4: Autres
  - **RIA, 5 M€/projet, TRL7, max. 2 projets en 2017**
  - au moins **3 Agences Repressives (LEA)** de 3 EM (1,2,3) ou 5 LEA de 5 EM (4),
  - pas de technologies de détection
  - démonstration obligatoires,



# BES

Les numérotations des topiques peuvent encore changer



# Border Security & External security (BES) (1)

- ❑ BES-1-2017: *PCP of next generation of information systems to support EU external policies*
  - **PCP, 10 M€, max. 1 projet, TRL8,**
  - liens avec EDA, au moins 3 **end-users** de 3 EM
  
- ❑ BES-2-2016: *Towards cost reduction in land border security applications*
  - **RIA, 5 M€/projet, max. 2 projets, TRL 6,**
  - liens avec EDA, 3 **end-users** de 3 EM
  
- ❑ BES-3-2017: *Risk-based screening at border crossing*
  - **IA, 8 M€/projet, 1 projet, TRL 7,**
  - 3 **end-users** de 3 EM
  
- ❑ BES-4-2017: *Through-foliage detection, including in the outermost regions of the EU*
  - **RIA, 8 M€/projet, max. 1 projet, TRL 5-6,**
  - liens avec EDA, 3 **end-users** de 3 EM



# Border Security & External security (BES) (2)

- ❑ **BES-5-2017: Architectures organization, data analysis and risk assessment for ensuring security in the supply chain**
  - **RIA, 5 M€/projet,**
  - 3 end-users de 3 EM
  
- ❑ **BES-6-2017: Acceptance of "no gate crossing point solution"**
  - **RIA, 3 M€/projet, max. 2 projets,**
  - 3 end-users de 3 EM
  
- ❑ **BES-7-2016: Data fusion for maritime security applications**
  - **IA, 8 M€/projet, TRL 7,**
  - liens EDA,
  - 3 end-users de 3 EM et 3 industriels indépendants de 3 EM
  
- ❑ **BES-8-2016: Autonomous surveillance with enhanced command and control systems for the surveillance of borders in a 3D environment**
  - *Autonomous surveillance*
  - *Enhanced command and control systems for the surveillance of borders in a 3D environment*
  - *Autonomous surveillance*
  - **IA, 8 M€/projet, TRL 6-7,**
  - end-users de 5 EM



# GM

Les numérotations des topiques peuvent encore changer

# General Matters (GM)

- ☐ GM 1-2016 and 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 méditerranéenne, 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, 2 x 14 M€**
    - **end-users d'au moins 8 EM**
  
- ☐ GM 2-2016 and 2017: *SME Instrument*
  - Engaging SMEs in security research and development
  - **19,5 M€**
  
- ☐ GM 3-2016 : *Fast Track for Innovation*
  - **FTI**