HORIZON 2020

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

GTN Horizon 2020 « Défi sécurité » - Réunion 1

MESR – 05/03/14

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

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
ST(SI)²

Ordre du jour

- Programme de travail « Défi Sécurité »
  - Appels 2014
  - Programme de travail 2015
  - IPR
  - Calendrier du programme de travail 2016 – 2017
- Appel TIC/cyber
- Filière (CoFIS)
- Action préparatoire PSDC
- Point ANR – Défi Sécurité
- Lignes pilotes KET
- Actions du PCN: actions suite Retex
- AOB

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

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

SISSE

WP 2014-2015

Le Draft disponible sur Europa n'est pas à jour!

- Rappel du processus
  - Début des négociations en septembre 2013
  - Vote négatif en *shadow* comité le 18 novembre 2013 sur draft v1
  - Publication (malgré vote négatif) du draft v1 le 11 décembre 2013
  - Comité en format Experts, compromis CE - MS
    - Modifications sur OA (PRS Galiléo, Europol) => réintégration budget
    - Report de 4 sujets 'DG ENTR' (cf. partie IPR)
    - Alignement dates de clôture DS
    - *White sheet* sur appel DS 2015
  - Premier comité de programme
    - Accord informel du comité donné le 3 février 2014
  - Ouverture des 3 appels DG ENTR: 25 mars 2014
  - Clôture des 4 appels le 28 août 2014
  - Résultats attendus des 4 appels pour novembre 2014

Appel 2014 – DRS

- 9 sujets, 54,4 M€ (+ 7 M€ pour Instrument PME)
  - DRS-2-2014 *Tools for detection, traceability, triage and individual monitoring of victims after a mass CBRNE contamination and/or exposure* (IA, 5-12M€)
  - DRS-4-2014 *Feasibility study for strengthening capacity-building for health and security protection in case of large-scale pandemics - Phase 1 (Demo)* (CSA)
  - DRS-5-2014 *Situation awareness of Civil Protection decision-making solutions - preparing the ground for a PCP* (CSA)
  - DRS-7-2014 *Crises and disaster resilience - operationalizing resilience concepts* (R&I, 3-5 M€)
  - DRS-16-2014 *Improving the aviation security chain* (R&I, 3-5 M€)
  - DRS-17-2014/2015 *Urban critical infrastructure* (SME instrument)
  - DRS-19-2014 *Next generation emergency services* (R&I, 2-5 M€)
  - DRS-20-2014 *Improving protection of critical infrastructures from insider threats* (CSA)
  - DRS-21-2014 *Better understanding the links between culture, risk perception and disaster management* (CSA)

- **Topique PCP PMR transféré à 2015!**

Appel 2014 – FCT

- 8 sujets, 56,77 M€
  - FCT-5-2014 *Develop novel monitoring systems and miniaturised sensors to improve LEAs evidence-gathering abilities* (IA, 3-5 M€)
  - FCT-7-2014 *Pan European platform for serious gaming and training* (R&I, 4-6 M€)
  - FCT-8-2014 *Transnational cooperation among public end-users in security research stakeholders* (CSA)
  - FCT-10-2014 *Innovative solutions to counter security challenges connected with large urban environment* (R&I, 3-5 M€)
  - FCT-11-2014 *Countering the terrorist use of an explosive threat* (R&I, 3-5 M€)
  - FCT-12-2014 *Minimum intrusion tools for de-escalation during mass gatherings improving citizens' protection* (R&I)
  - FCT-13-2014 *Factors affecting (in-) security – Phase 1* (CSA)
  - FCT-14-2014 *Enhancing cooperation between law enforcement agencies and citizens-Community policing* (R&I, 2-5 M€)

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

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Appel 2014 – BES

- 3 sujets, 20,78 M€
  - BES-9-2014 *Technologies for inspections of large volume freight* (R&I, 5-12 M€)
  - BES-12-2014 *Enhancing the civilian conflict prevention and peace building capabilities of the EU* (CSA)
  - BES-14-2014: *Ethical Societal Dimension topic 1: Human factors in border control* (R&I, 2-5 M€)
- **3 sujets transférer en 2015 (IPR)**
  - **BES-1-2015 *Radar systems for the surveillance of coastal and pre-frontier areas and in support of search and rescue operations* (IA)**
  - **BES-3-2015 *Light optionally piloted vehicles (and sensors) for maritime surveillance* (IA)**
  - **BES-11-2015 *information management, systems and infrastructure for EU External actions* (CSA)**

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

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
STSI²

Appel 2014 – DS

- 3 sujets
  - DS 1-2014 *Privacy* – 19,04 M€
  - DS 2-2014 *Access control* – 18 M€
  - DS 6-2014 *Risk management and assurance models* – 10 M€

WP 2015

- Vote des Etats membres sur l'année 2014 du WP
- WP15
  - Inputs de *wording* reçus de: ANSSI, ISL, ONERA, Université de Rouen, ministères (+IMGS)
  - Modifications à la marge sur appels DRS, FCT et BES
  - Discussion sur IPR pour DRS18, BES1, BES3 et BES11 (cf. partie IPR)
  - Demandes Go6:
    - Ajout DS-X-2015: *Acceptance & acceptability of new digital technology*
    - Ajout DS-Y-2015: *Cybersecurity management tools*
    - Suppression DS: DS-4
- Calendrier prévisionnel
  - Deadline input MS: 7 mars 2014
  - Discussion avec MS: avril-mai 2014
  - Vote: juin 2014

IPR

- Rappel négociations RdP
  - Article 4
  - Article 49§2 (ex Art. 46§2-3)
- WP v. mi-novembre 2013, introduction de clauses additionnelles dans WP sur quatre sujets 2014 (sans alerte préalable du comité!)
  - DRS-18: PMR (PCP)
  - BES-1: radars OTH (IA)
  - BES-3: unmanned plateformes (IA)
  - BES-11: information management systems for civilian EU External actions (CSA)
- Compromis EC-MS: ok pour discussion mais report à 2015
- Constitution d'un groupe de travail dédié avec MS et industrie

IPR

- Art 4 §1
  - *[…]*
    In actions under the specific objective 'Secure societies - Protecting freedom and security of Europe and its citizens', the Commission shall upon request make available to Union institutions, bodies, offices or agencies or to Member States' national authorities any useful information in its possession concerning results generated by a participant in an action that has received Union funding. The Commission shall notify the participant of such communication. Where a Member State or Union institution, body, office or agency requests the communication of information, the Commission shall also notify such communication to all Member States
- Art. 49§2
  - *Regarding actions under the specific objective 'Secure societies - Protecting freedom and security of Europe and its citizens' set out in Part III of Annex I to Regulation (EU) No1291/2013, Union institutions, bodies, offices and agencies, aswell as Member States' national authorities, shall, for the purpose of developing, implementing and monitoring their policies or programmes in this area, enjoy the necessary access rights to the results of a participant that has received Union funding. Such access rights shall be limited to non-commercial and non-competitive use. Such access rights shall be granted on a royalty-free basis and upon bilateral agreement defining specific conditions aimed at ensuring that those rights will be used only for the intended purpose and that appropriate confidentiality obligations will be in place. Such access rights shall not extend to the participant's background. The requesting Member State, Union institution, body, office or agency shall notify all Member States of such requests. The Commission rules on security shall apply regarding classified information.*
- Art. 55§1
  - *In the case of actions involving security-related activities, the grant agreement may lay down specific provisions, in particular on pre-commercial public procurement, procurement of innovative solutions, changes to the consortium's composition, classified information, exploitation, dissemination, open access to research publications, transfers and licences of results*

IPR

- Points principaux du document CE
  - Rappel de l'historique
  - Plusieurs justifications avancées:
    - *Risk of lock-in situation* (monopole)
    - *Risk of EU tax-payers paying several times the same technology*
    - *Risk that EU money supports the design by a few countries of transnational and/or interoperable technical solution (that will then be « imposed » to other countries)*
  - Pistes avancées: PCP et PPI
- 'Problèmes' potentiels
  - RdP fixe des règles claires sur PCP et PPI
  - PCP: financement à 30% des MS impliqués (pourquoi ceux ne payant pas bénéficieraient-ils des mêmes conditions?!)
  - PPI: financement UE de 20%...
- Nombreux problèmes de fonds…

Document
rosoft Word 97 - 2

WP 2016-2017

- Début des discussions en comité: septembre 2014
- Calendrier général Horizon 2020:
  - Consultation du comité horizontal sur les priorités (ex *focus areas*) en juin 2014
  - Consultation des comités au second semestre 2014
  - Discussion sur le contenu au premier semestre 2015
  - Opinion des comités mi-2015

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

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
ST(SI)²

Programme Horizon 2020/LEIT ICT

- Composants et systèmes
- Calcul avancé
- Internet du futur
- Contenu et tech. Inform.
- Robotique
- KET
  µ-elect. et photonique
- FoF

<u>Activités horizontales</u>
IoT
SHS
Cyber
Coopération internationale

<u>Actions innovation</u>
Accès au finance
Politique d'innovation
Instrument PME: *Open innovative instrument scheme*

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

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
STSI²

ICT32-2014: *Cybersecurity, Trustworthy ICT*

- Cryptography (ICT32.a+b)
  - Research & Innovation Actions (small and large)
  - Coordination and Support Actions
- Security-by-design for end to end security (ICT32.a)
  - Research & Innovation Actions (small and large)

- Taille des projets attendus
  - Small contribution: 2-4 M€
  - Large contribution: 5-8 M€
- Appel ICT-2014-1
  - Clôture: 23 avril 2014
  - Budget: 37 M€ ICT32.a; 1 M€ ICT32.b

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

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
STSI²

Cryptographie

- *Research projects have to address the key challenges to guarantee the security for the lifespan of the application it supports, to stay ahead of the evolution of the ICT environment and keep pace with the performance increase of ICT technology.*
- Résultats attendus:
  - *net increase in performance; reduction in energy or power consumption; validation in realistic application scenarios; relevance to current trends (cloud, mobile, IoT,etc); methods for provable security against physical attacks; security certification.*
- Challenges
  - *Resource efficient, real-time and highly secure technology for 1. hardware based cryptography; or 2. homomorphic cryptography.*
  - *Distributed cryptography including functional cryptography;*
  - *Cryptographic tools for securely binding applications to software, firmware and hardware environments, with or without adaptation of primitives which are used;*
  - *Post-quantum cryptography for long-term security;*
  - *Quantum key distribution (QKD) systems and networks for long-term security-by-design (etc.) addressing: 1. low-bit-rate QKD with low cost components for shortdistance; 2. high-bit rate QKD systems, tolerant to noise and loss.*

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

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
STSI²

Security-by-design for end-to-end solutions

- *"Security-by-design paradigms have to be developed and tested, to provide end-to-end security, across all hardware and software layers of an ICT system and application and business services."*
- *Paradigms for complex environments:*
  - *Highly connected, complex and interoperable networks.*
  - *Multi-layer and multi-service systems, spanning multiple domains or jurisdictions*
- *Aiming at:*
  - *Platform-independent solutions for context-aware and selfadaptive security*
  - *Automated security policy governance for run-time verification, customisation and enforcement between operators or virtual entities,*
- *Important Considerations:*
  - *Interaction of Layers*
  - *Holistic Approach*
- *Special Attention to:*
  - *Open and dynamically reconfigurable environments*
  - *Reliance on other, potentially untrustworthy, providers Importance of*
- *Usability:*
  - *Deployment and implementation with usability in mind against improper use or misconfiguration for higher degrees of trust by users*

Sécurité/Privacy se retrouvent de manière transverse sur de nombreux objectifs de LEIT/TIC

- ICT 1 – 2014: *Smart Cyber-Physical Systems (privacy/security by design)*
- ICT 4 – 2015: *Customised and low power computing (security)*
- ICT 5 – 2014: *Smart Networks and novel Internet Architecture (security, trust, privacy)*
- ICT 7 – 2014: *Advanced Cloud Infrastructures and Services (security, privacy)*
- ICT 14 – 2014: *Advanced 5G Network Infrastructure for the Future Internet*
- ICT 22 – 2014: *Multimodal and Natural computer interaction (Robotics, security)*
- ICT 26 – 2014: *Photonics KET*
- ICT 30 – 2015: *Internet of Things and Platforms for Connected Smart Objects (security)*
- EUB 1 – 2015: *Cloud Computing, including security aspects (Joint Call with Brazil)*
- EUJ 4 – 2014: *Experimentation and development on federated Japan – EU testbeds (Joint Call with Japan)*

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

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
STSI²

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

La filière industrielle de la sécurité - CoFIS

GTN - MESR, le 5 mars 2014

SGDSN / PSE
Pôle « développement des technologies de sécurité »

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

Enjeux

- **Organiser l'expression du besoin**
  - connecter la filière avec la démarche nationale d'analyse du risque et de la menace,
  - structurer le dialogue interministériel,
  - mettre en réseaux les compétences.
- **Organiser le dialogue entre les acteurs publics et privés**
  - rassembler les acteurs dans un format adapté
  - se doter d'une feuille de route avec des objectifs sur CMT

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

Installation du CoFIS

- le 23 octobre 2013 par le PM
- une charte définissant l'organisation et les objectifs
- une feuille de route pour 2014

Schéma d'organisation

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

SGDSN

Comité de la filière industrielle de sécurité

Présidence Premier ministre

secrétariat conjoint SGDSN – DGCIS

membres de droits

collège des industriels

collège des utilisateurs et opérateurs non étatiques

collège des personnalités qualifiées

Groupe de pilotage

co-Présidence SGDSN-DGCIS

un vice-présidents issus du collège des industriels

un vice-président représentant des personnalités qualifiées

un représentant du MEDDE, du Ministère de l'Intérieur, du MESR et du Ministère de la défense

présidents et vice-présidents des sous-groupes

Sous-groupe

« prescripteurs de la sécurité »

Présidence SGDSN

Représentants des membres de droits

Sous-groupe

« expression des besoins »

Présidence représentant utilisateurs et opérateurs non étatiques

Représentants des membres de droits

Représentants du collège des utilisateurs et opérateurs non étatiques

Représentants du collège des industriels

Sous-groupe « export –normes – intelligence économique »

Présidence industrielle

Représentants des membres de droits
Représentants des trois collèges

Sous-groupe « recherche et innovation »
Présidence personnalité qualifiée

Représentants des membres de droits
Représentants des trois collèges

Sous-groupe

« financeurs de la recherche et de l'innovation »

Présidence DGCIS

Représentants des membres de droits

Pilotes des sous-groupes

Sous-Groupes	Participation des collèges	Président et Vice-président(s)
Prescripteurs de la sécurité	Représentant des membres de droit uniquement	Président - Préfet Evence RICHARD – secrétariat général de la défense et de la sécurité nationale – directeur de la sécurité de l'Etat
Expression du besoin	Représentants des membres de droit, du collège des utilisateurs et opérateurs non étatiques, du collège des industriels	Président – Préfet Patrick ESPAGNOL – EDF – directeur de la sécurité
		Vice-président - Général Bernard PAPALARDO – ministère de l'intérieur, directeur du service des technologies et des systèmes d'information de la sécurité intérieue
Stratégie export, normes et intelligence économique	Représentants des membres de droit et des trois collèges	Président - Jean-Pierre QUEMARD – CASSIDIAN – vice-président « sécurité et technologies »
		Vice-président – Thierry Campos – HGH – PDG
Recherche et innovation	Représentants des membres de droit et des trois collèges	Président – Michel Robert – université de Montpellier – président
		Vice-présidents – Philippe Dejean – MORPHO – directeur technique de la division « Technologies et Stratégies »
		Jean-Pierre Tual – pôle de compétitivité SYSTEMATIC – président du groupe de travail « confiance numérique et sécurité »
Financeurs de la recherche et de l'innovation	Représentants des membres de droit uniquement	Président – Benjamin GALLEZOT, ministère du redressement productif, directeur général de la compétitivité, de l'industrie et des services

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN

CoFIS 2014 : 7 priorités

- Connaitre la filière nationale, à travers une première cartographie des acteurs et du marché
- Exprimer le besoin, à travers un premier recensement des besoins de l'Etat et des opérateurs
- développer les solutions de demain, en soutenant le lancement de projets de démonstrateurs susceptibles d'incarner la filière
- Identifier les technologies de sécurité critiques
- soutenir les entreprises française à l'export, en favorisant l'émergence d'un club France
- Utiliser le levier européen, en proposant une stratégie nationale vis-à-vis des instruments européens
- mettre en réseau les acteurs, à travers la mise en place d'un portail « filière » et d'actions de sensibilisation

Equipes projets (1)

AXE	Actions	Pilote(s)
1. Connaitre la filière nationale	Lancer une étude de référence nationale, comprenant les éléments suivants : - élaboration d'une segmentation de référence pour l'analyse en profondeur du marché de la sécurité sur l'ensemble du champ visé ; - recensement des acteurs français, y compris dans le domaine de la recherche et du développement, et leur poids économique - réalisation d'une étude de marché à l'aide d'indicateurs stabilisés ; - analyse des forces et faiblesses, opportunités et menaces pour chaque segment du marché.	Etude sous financement DGCIS – SGDSN- DGPN/DGGN Comité de suivi : CICS, présidents et vice-présidents des différents sous-groupes
2. Exprimer le besoin	Définir une méthodologie de recueil du besoin s'appuyant sur une segmentation capacitaire du besoin	sous-groupe « expression du besoin »
	Recueillir et regrouper les besoins exprimés par grandes catégories, en distinguant les besoins génériques des besoins spécifiques et en prenant bien en compte les contraintes réglementaires et juridiques associées	
	Proposer des priorités à soumettre à la validation du CoFIS	sous-groupe « prescripteurs de la sécurité».
3. Développer les solutions de demain	Elaborer une cartographie des différents guichets d'aides publiques susceptibles de financer des projets de recherche et d'innovation dans le domaine de la sécurité	sous-groupe « financeurs de la recherche et de l'innovation », en coordination avec les « prescripteurs de la sécurité »
	Définir une dizaine de projets de démonstrateurs	sous-groupe « recherche et innovation », en coordination avec le sous-groupe expression du besoin
	Elaborer, pour chacun des démonstrateurs, un partage du plan de financement entre le public et le privé, qui pourra tenir compte du contexte commercial propre à chacun d'eux	
	Engager leur réalisation selon l'ordre de priorité déjà arrêté en commun par les membres de la filière »), tout en favorisant la mutualisation du développement des briques communes à plusieurs des projets retenus	sous-groupe « financeurs de la recherche et de l'innovation », en coordination avec le sous-groupe «prescripteurs de la sécurité »

Equipes projets (2)

AXE	Actions	Pilote(s)
4. Identifier les technologies de sécurité critiques	Définir la notion de « criticité » s'appliquant aux technologies de sécurité	DGA
	Au regard de la segmentation du marché réalisée (axe 1) et des technologies de sécurité portées par les acteurs de la filière ou émergentes, distinguer celles qui pourraient être qualifiées de « critiques »;	DGA avec le soutien du sous-groupe « recherche et innovation »
	Analyser, avec les acteurs de la filière, l'opportunité et la faisabilité de la maîtrise de certaines de ces technologies au niveau national et/ou de leur portage au niveau européen en vue des développements	Sous-groupe « export, normes, intelligence économique »
5. soutenir les entreprises françaises à l'export	Elaborer un rapport sur les opportunités « export » de la filière française des industries de sécurité (marchés et technologies cibles)	Sous-groupe « export, normes, intelligence économique », avec soutien d'UBIFRANCE, ministère du commerce extérieur, D2IE, DCI
	Définir de manière concertée une liste de pays cibles prioritaires et un plan d'actions annuel porté par l'ensemble des opérateurs (ministères concernés, UBIFRANCE, groupements professionnels, etc.)	
	Valoriser l'excellence de l'offre française dans le cadre des déplacements ministériels dans les pays à forts débouchés	
	Participer sous bannière « filière française » à des manifestations internationales de renom	
	Sensibiliser des acteurs-relais : attachés à l'étranger en coordination avec leur structure siège (attachés de sécurité intérieure, de défense, services économiques), bureaux UBIFRANCE, réseau des chambres de commerce et d'industrie (CCI)	
	Mieux coordonner l'offre française sur les manifestations internationales organisées en France (par exemple Milipol)	
	Mettre en place une action ciblée d'aide au développement des capacités (« capacity building ») (un secteur sur un pays)	
6. utiliser le levier européen	Recenser les politiques européennes et instruments, et leur interconnexion	Copilotage ad hoc SGDSN-CICS
	Conduire une analyse « risques / opportunités » tant du point de vue de l'industrie que des pouvoirs publics, des différentes positions françaises envisageables	
	Elaborer un plan d'action concerté public/privé sur les trois prochaines années	
7. mettre en réseau les acteurs	Elaborer la stratégie de communication de la filière, à décliner en plan de communication sur 2014, avec comme action prioritaire la réalisation d'une plaquette de promotion de la filière, ainsi que l'identité visuelle de la filière	Equipe projet ad hoc, mixte public-privé : SGDSN, ANSSI, DGCIS, CICS, UBIFrance Porte-paroles – SGDSN-CICS
	Mettre en place un portail internet dans un premier temps réservé à la promotion et à la diffusion des activités de la filière	A déterminer
	Organiser un séminaire interministériel visant à présenter les objectifs et les modalités de mise en œuvre de la filière industrielle de sécurité aux administrations-prescriptrices	SGDSN/DGCIS

GTN et CoFIS (1/2)

De nombreuses adhérences avec les actions du CoFIS

- la plupart des membres du GTN sont représentés au sein du CoFIS
- les travaux du GTN bénéficieront de données d'entrée
  - Expression du besoin et priorités
- des interactions potentielles
  - Stratégie européenne et priorités R&I

GTN et CoFIS (2/2)

- le GTN est une enceinte qui garde toute sa pertinence
  - Forum d'échange et d'information spécialisé
  - concertation P&P
- Il est essentiel que des RDV réguliers se construisent
  - leur nature restent à préciser
  - vos suggestions sont les bienvenues
- Proposition :
  - les pilotes du groupe stratégie Europe du CoFIS participent et présentent l'avancée des travaux à la prochaine réunion en juin

La recherche

en Sécurité Globale à

l'Agence Nationale de la Recherche

GTN Sécurité – 5 mars 2014 – X. Dramard

Bilan du programme «Concepts, Systèmes et Outils pour la Sécurité Globale» de l'ANR

CSOSG 2006 - 2013

Retour CSOSG 2013

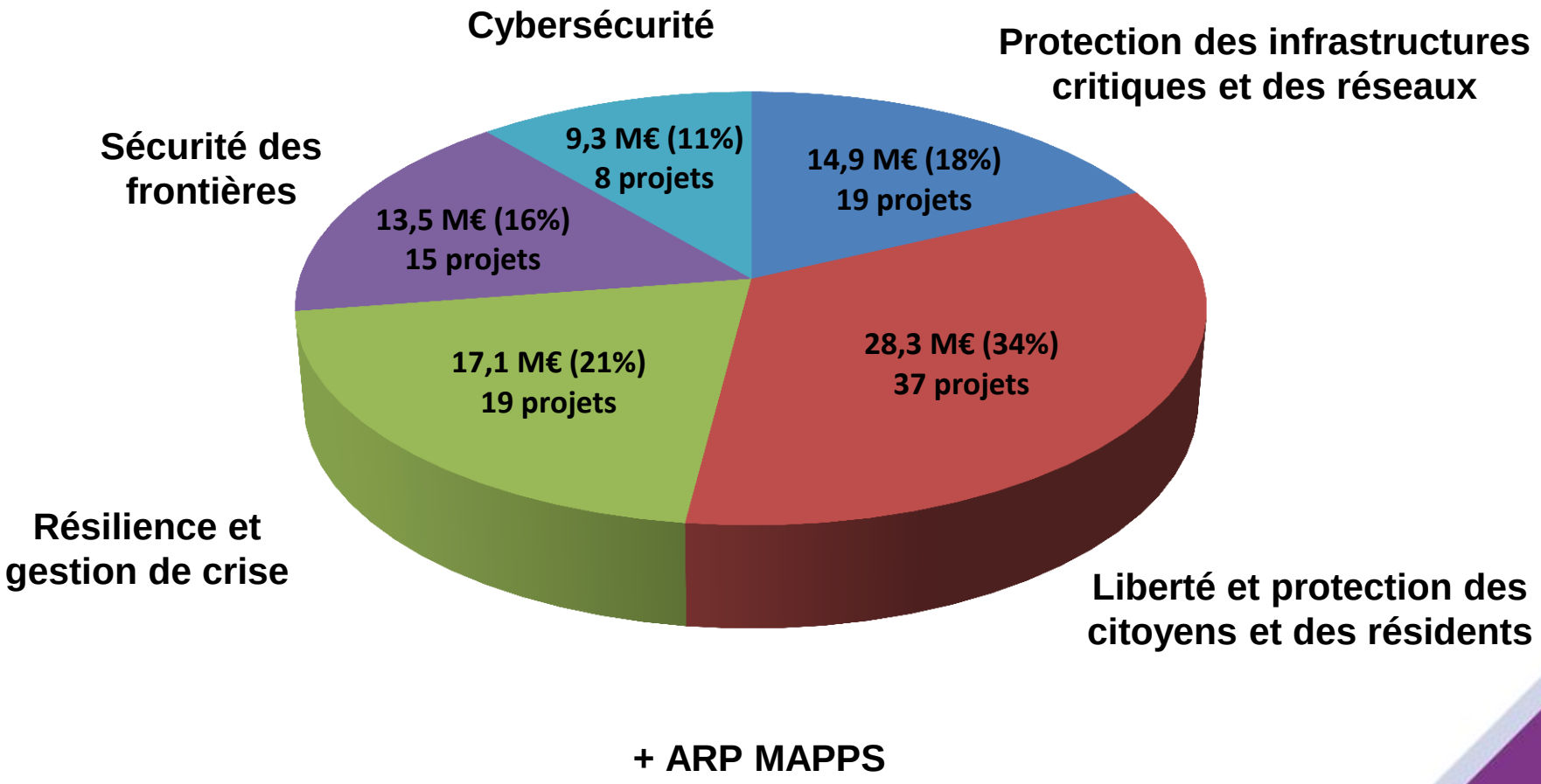
- Appel Franco-Français
- Partenariats: DGA et SGDSN
- Répondre aux priorités nationales et européennee en Sécurité Globale et préparer le futur HORIZON 2020
- Programmation:
  - Axe 1: Recherche de rupture en sécurité (ex « Axe transverse »)
  - Axe 2: Protéger le citoyen et les infrastructures
  - Axe 3: Résilience et gestion de crise
  - Axe 4: Lutter contre la cybercriminalité
- 7 projets financés
  - 33 partenaires français
    - 5,9 M€ d'aide pour un coût total de 20,3 M€
    - Démarrage des projets: Novembre 2013

Programme CSOSG "Concepts, Systèmes et Outils pour la Sécurité Globale" 2006-2013

- **99 projets, réunissant 500 partenaires**
  - 43 projets labelisés par 18 pôles différents
  - Une participation public/privé équilibrée:
    - Partenaires: Public 57,7% / Privé 42,3%
    - Volume d'aide : Public 53,2% / Privé 46,8%
- **83 M€ d'aide pour 187 M€ de coût total**
- **Co-financements**
  - DGA (depuis 2006)
  - SGDSN (depuis 2013)
  - MinInt/STSI^2 (de 2007 à 2011)
- **Coopération franco-allemande**
  - Depuis 2009: MoU avec le BMBF (Ministère fédéral allemand de l'éducation et de la recherche)

Federal Ministry of Education and Research

Thèmes des projets CSOSG 2006-2013



+ ARP MAPPS

Présent et avenir de la recherche en Sécurité Globale à l'ANR

Plan d'action 2014 et Défi Sociétal «Liberté et sécurité de l'Europe, de ses citoyens et de ses résidents»

2013-2014 : Une année de transition pour l'ensemble de l'ANR

- Contexte de cette transition:
  - Prise en compte des attentes des Assises de la Recherche
  - En cohérence avec l'agenda stratégique « France-Europe 2020 »
  - Mobilisation des Alliances (Allenvi, Allistene, Ancre, Athena, Aviesan) et du CNRS
  - Prise en compte des partenaires -publics et privés- de l'Agence

- Grands principes:
  - Simplification de la procédure d'appel à projets
  - Dans le respect des fondamentaux:
    - mise en œuvre des standards internationaux
    - sélection compétitive
    - évaluation par les pairs
    - équité de traitement

Concrètement: un changement de paradigme pour le financement sur projets à l'ANR

- Changement de calendrier de programmation
  - 1 appel à projets « générique » par an:
    - Regroupe l'ensemble des actions de l'ANR

- Changement de processus de sélection
  - En 2 temps:
    - Etape 1: pré-proposition (5 pages)
    - Etape 2: proposition complète (30 pages)

-> Un document annuel unique: le « Plan d'Action 2014 »

Le Plan d'Action 2014

- Dans le cadre de l'exercice budgétaire 2014
- S'adresse à l'ensemble des communautés scientifiques, du public et du privé (dont PME et TPE)

- Est constitué d'un AAP unique générique…
  - Se substitue aux AAP des éditions précédentes
  - Rassemble l'ensemble des actions de l'ANR pour 2014
  - Dont les actions liées aux 9 grands « Défis Sociétaux »
  - Décrit les « instruments » à disposition des candidats
    - Projets collaboratifs, PPP, Challenge = ancien « défi » (mise en compétition), Réseaux et JC-JC
  - Expose les modalités d'évaluation (2 temps)

- … Et d'un nombre très limité d'AAP complémentaires
  - dont bilatéraux avec d'autres agences, programme Astrid, etc.

Les 9 grands Défis Sociétaux du PA2014

1. Gestion sobre des ressources et adaptation au changement climatique
2. Une énergie propre, sûre et efficace
3. Stimuler le renouveau industriel
4. Santé et bien-être
5. Sécurité alimentaire et défi démographique
6. Mobilité et systèmes urbains durables
7. Société de l'information et de la communication
8. Sociétés innovantes, intégrantes et adaptatives
9. **Liberté et sécurité de l'Europe, de ses citoyens et de ses résidents**

Défi 9: Liberté et sécurité de l'Europe, de ses citoyens et de ses résidents

-> Défi dans la continuité du programme CSOSG

- Objectifs du Défi:
  - Solutions pour la sécurité des citoyens et résidents français et européens
    - En complémentarité avec H2020
    - En cohérence avec la création d'une filière industrielle de sécurité, et avec les priorités nationales et européennes
    - Dans le respect de l'éthique et de la vie privée
  - Fédérer la communauté de recherche et innovation en sécurité globale
- Moyens d'atteindre ces objectifs
  - La pluridisciplinarité
    - Efficacité d'un système de sécurité: conditionnée par interdépendance entre les technologies, les modes d'organisation et l'humain
    - Toutes les disciplines scientifiques peuvent être concernées (dont SHS)
  - Les Partenariats Publics-Privés
    - Académiques, Entreprises, Utilisateurs (réponse à un réel besoin)
    - Non obligatoire dans le cadre du PA 2014 (autres instruments éligibles)

Les 5 grands axes thématiques du Défi 9

- Axe 1: Protection des infrastructures critiques et réseaux
  - Appel à projets dédié (hors appel générique du PA2014)
  - Bilatéral Franco-Allemand (ANR-BMBF)
  - Publié le 22 janv. 2014
- Axe 2: Liberté et protection des citoyens et des résidents
- Axe 3: Résilience et gestion de crise
- Axe 4: Sécurité des frontières
- Axe 5: Cybersécurité
  - Axe en interface avec le Défi 7 « Société de l'information et de la com° »

Calendrier de l'appel générique mis à jour

Pré-proposition

30 juillet 2013	mise en ligne du plan d'action 2014
septembre 2013	ouverture du site de soumission
23 octobre 2013	clôture de la réception des pré-propositions

→ **70 PP reçues**

Proposition détaillée

Début mars 2014 information de l'ANR vers les porteurs

Envois à partir du 7 mars

Non retenu

Retenu

8 à 10 semaines

Début mai 2014	fin de la période de soumission des projets détaillés
Mi juillet 2014	publication des résultats de la sélection
juillet - décembre	phase de contractualisation

→ **Début Juillet 2014: Publication du Plan d'Action 2015**

Informations

Site web de l'ANR:

http://www.agence-nationale-recherche.fr

-> Informations sur le Plan d'Action 2014
(puis PA 2015: publié en juillet 2014)

-> FAQ

-> Résultats 2014 (soumissions et 1ère étape)

AGENCE NATIONALE DE LA RECHERCHE
ANR

Federal Ministry
of Education
and Research

Franco-German Call on Protection of Critical Infrastructures

Continuing a successful partnership

Basis:

Memorandum of Understanding of 2009

Current funding:

9 projects with 67 partners, for an overall volume of EUR 41 million

MAPPS tool

- Strengthen the FR/GE partnership (for bilateral and European projects) by:
  - Improving the mutual knowledge
  - Mapping of French and German research projects, technologies, actors involved in security research

  -> Booklet

  -> Web platform (database, access to information, registration, exchange)

Preparing the continuation

National calls on protection of critical infrastructures

Germany: Calls regarding traffic (2007) and supply (2008) infrastructures

France: Important topic in all calls of the last years

4th Franco-German Research Forum

Agreement on the choice of topic for a new joint call

Joint Working Group “Protection of Critical Infrastructures”

Analysis of the state of the art as well as end users’ needs

Recommendations to ANR and BMBF

Franco-German coordinated call on protection of critical infrastructures

Publication of the coordinated calls: 22nd January 2014

ANR: "Franco-German call on Protection of Critical Infrastructures"

BMBF: Franco-German cooperation in the area of "Civil Security - Protection of Critical Infrastructures"

Thematic priorities

1. Energy and water infrastructures
2. Transport infrastructures
3. Interdependencies between critical infrastructures
4. Cross-cutting social and economic aspects of protecting critical infrastructures

1: Energy and water infrastructures

- New risks and solutions for increasing the resilience of energy and water supply
- Solutions for the physical protection of critical infrastructures
- Concepts and solutions for crisis management in the case of cross-border large scale power failures
- Solutions for providing citizens, the economy and authorities with energy and water in case of breakdown of major infrastructures

2: Transport infrastructures

- Methods and tools to assess and improve the resilience of all kinds of transport infrastructures
- Solutions for enhancing the availability of transportation for people and goods in case of crisis

3: Interdependencies between critical infrastructures

This priority concerns energy, water, transport infrastructures as well as other critical infrastructures (health care, communication, etc.)

- Multi-sector analysis of risks and threats for co-located or interdependent infrastructures
- Analysis of interdependencies between critical infrastructures and concepts for managing it (cascading effects)
- Innovative concepts for the operation of critical infrastructures to allow a basic functioning in case of breakdown of a connected infrastructure

4: Cross-cutting social and economic aspects of protecting critical infrastructures

- Crisis and risk communication to the public in case of failure or attack on a critical infrastructure
- Solutions, concepts and best practices for effective cooperation and communication between all actors in case of critical infrastructures failure
- Definition of security models and metrics to analyze the cost/benefit of security investments from the economic and societal perspective
- Methods and concepts for evaluation and standardization of security tools

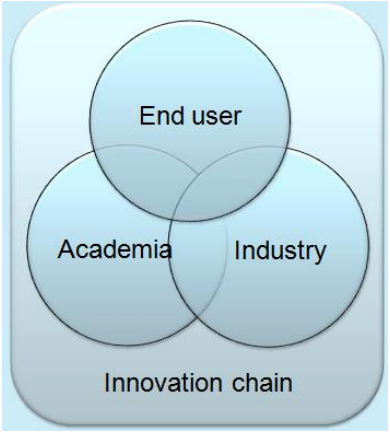
These issues can be addressed either in dedicated projects or as part of projects corresponding to thematic priorities 1, 2 or 3

Proposals

- Proposals have to:
  - Show particular relevance for both France and Germany:
    - fit in with the joint call thematic priorities
    - be based on relevant scenarii (ex.: cross-border event)
    - compare and take account of national specificities
  - Lead to an increase of the security
    - without limiting privacy and personal rights of citizens
  - Address topics that are different from, or complementary with projects that could be funded at European level (H2020 - WP “Secure Societies”)
  - Achieve world-class scientific and technical results
  - Respect the project timescale range (max. 36 months)

Franco-German Consortium

- A Franco-German consortium is understood as:
  - a joint team of French and German partners
  - with complementary skills
  - working together in one common project
  - creating a joint output



- A Franco-German consortium is composed of:
  - One unique Spokesperson for the FR-GE consortium
  - A French part, and a German part, each one consisting of:
    - One national coordinator
    - Partners from academia and industry, and end-users
      - Exception: Projects exclusively addressing cross-cutting societal and economic aspects

- Multidisciplinarity
  - Quality of a security system:
    - Depends on the quality of interaction between technologies, the human factor, and the organization (system and its environment)
  - All relevant areas of research and technology have to be involved
    - Natural sciences, engineering, SSH, law, economics, psychology etc.

Application and selection of proposals

- Application:
  - 1 document for the whole FR-GE consortium
  - Max. 35 pages, in English
  - 100% common (template available from ANR and VDI TZ)
  - But submitted to both ANR and VDI TZ, in parallel, following national procedures
  - Submission deadline : **5th of May, 2014**
- Funding of FR-GE projects:
  - French teams
    - apply in accordance with ANR rules
    - are funded by ANR
  - German teams
    - apply in accordance with BMBF rules
    - are funded by BMBF
- Evaluation:
  - Eligible proposals are evaluated jointly by BMBF and ANR
  - Using common criteria

Information and support

	France	Germany
Text of the call + Submission	http://www.agence-nationale-recherche.fr/FR-ALL-2014-Protec-Infra-Critiques	http://www.bmbf.de/foerderungen/23241.php www.SIFO.de
Apply as an expert to evaluate proposals		
Support	**Scientific and technic questions** Karine Delmouly +33 (0)1 73 54 82 38 karine.delmouly@agencerecherche.fr **Administrative questions** Cécile Goujon +33 (0)1 78 09 80 53 Cecile.goujon@agencerecherche.fr	VDI Technologiezentrum Christian Krug (VDI) +49/2 11/62 14 – 452 krug_c@vdi.de Steffen Muhle (VDI) +49/2 11/62 14 – 3 75 muhle@vdi.de

DANKE
THANK YOU
MERCI

HORIZON 2020

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

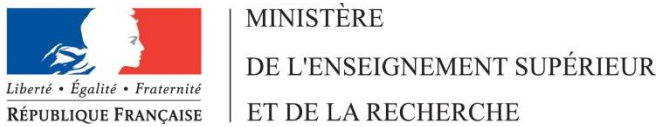
Françoise SIMONET
Coordinatrice PCN Sécurité
francoise.simonet@cea.fr

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

CEA: Françoise Simonet
MESR: Frédéric Laurent
CICS: Philippe Dejean
Université de Rouen: Philippe Moguérou
Pôle Risques: Sébastien Giraud, Jean Michel Dumaz, Alice Letessier (communication)
Pôle System@tic: Jean Pierre Tual, Isabelle de Sutter



Le Point de Contact National **Sécurité** est en charge du défi "**Sécurité**".

Vos contacts PCN Sécurité :

Prénom - NOM	Rôle	Etablissement	Téléphone	Mél.
 Françoise SIMONET	Coordinatrice du PCN	CEA - Commissariat à l'Energie atomique et aux énergies alternatives	33 1 69 26 75 74 33 6 85 80 48 22	Contact
 Frédéric LAURENT	Représentant au Comité de Programme	Ministère de l'Enseignement Supérieur et de la Recherche	33 1 55 55 88 81	Contact
 Philippe DEJEAN	PCN	CISC / MORPHO	33 1 58 11 87 09	Contact
 Sébastien GIRAUD	PCN	Pôle Risques	33 6 23 32 34 69	Contact
Philippe MOGUEROU	PCN	Université de Rouen / CPU	33 2 35 14 60 33	Contact
Jean-Pierre TUAL	PCN	Pôle SYSTEM@TIC / GEMALTO	33 1 55 01 61 60 33 6 80 18 77 93	Contact

Sommaire

1. Cahier des charges du PCN
2. Organisation et animation du consortium
3. Information et sensibilisation
4. Assistance, conseil et formation des porteurs de projets
5. Orientation et coopération avec d'autres réseaux
6. Divers

Cahier des charges du PCN

Cahier des Charges (FR)

Volet 1 Information et sensibilisation de la communauté de recherche et d'innovation

Constituer le réseau de diffusion des acteurs de son domaine et établir les listes de diffusion correspondantes (établissements, laboratoires, agences, entreprises, ministères, associations professionnelles, pôles de compétitivité etc.)

Diffuser l'information et la documentation générale et spécifique au domaine d'Horizon 2020 dont il a la responsabilité, notamment sur les règles de participation, sur les possibilités et les conditions de soumission des propositions, ainsi que sur les budgets des projets, en alimentant notamment la rubrique dont il a la responsabilité sur le site www.horizon2020.gouv.fr.

Elaborer un plan d'information et de communication en liaison avec le MESR, ou le cas échéant, les alliances, décliné sur tout le territoire, en lien avec les acteurs régionaux de l'accompagnement au PCRD.

Développer son réseau au niveau européen, national et régional

Promouvoir les nouveautés d'Horizon 2020

Afin de réaliser ces actions, le PCN :

-utilisera obligatoirement la charte éditoriale multi-support réalisée et diffusée par le MESR dans toutes ses actions d'information et de communication ;

-appuiera le Représentant au Comité de Programme dans l'analyse des résultats de la participation

Cahier des Charges (FR)

Volet 2 : Assistance, conseil et formation des porteurs de projets

Aider les chercheurs et les organisations, en particulier les nouveaux acteurs et les PME, en vue d'accroître leur participation à Horizon 2020 :

•Conseiller et orienter le porteurs de projet dans l'élaboration de leur proposition (conseil sur la constitution du consortium ; relecture critique etc.) ;

•Orienter les chercheurs, organisations et porteurs de projets potentiels vers l'interlocuteur ad hoc, susceptible de les accompagner dans le montage et la gestion de leur propositions en s'appuyant sur la base de contacts fournie par le MESR (ex. ingénieur projet européen de l'établissement de rattachement ; dispositif régional d'accompagnement) ;

•Les informer sur les outils existants, notamment le nouveau site horizon 2020.gouv.fr

•Animer l'extranet « Client » et promouvoir sa valeur ajoutée

•Appuyer les Représentants aux Comités de Programme (RCP) dans la remontée d'information / le retour de terrain en vue de contribuer à la position française défendue dans les comités de programme et les assister dans l'animation du Groupe Thématique National correspondant (GTN).

Aider à la recherche de partenaires

Conseiller les chercheurs et les organisations sur les procédures administratives, les règles de participation et les enjeux

Organiser des formations ou intervenir dans le cadre des formations à horizon 2020

Cahier des Charges (FR)

Volet 3 : Orientation vers d'autres services support aux porteurs de projet

Le PCN doit être en mesure d' orienter les porteurs de projet vers d'autres sources de financement, européennes ou nationales, qui seraient plus adaptées à leurs besoins, et vers les services support dédiés à l'accompagnement de ces programmes et les mieux à même de les accompagner dans le montage de leur proposition et la gestion de leur projet.

Sensibiliser aux opportunités de financement offertes par des mesures externalisées (les initiatives au titre de l'article 185, les Initiatives Technologiques Conjointes (art. 187), les Communautés de la connaissance et de l'innovation de l'Institut Européen de Technologie, les initiatives de programmation conjointes) liées au domaine dont il a la charge.

Sensibiliser aux autres programmes européens de recherche et développement technologique dans le domaine de la recherche et de l'innovation, tels que COSME, EUREKA, COST, ainsi que la R&D dans les fonds structurels et les politiques extérieures de l'UE

Afin d'accompagner le réseau dans la mise en œuvre de cette mission, la coordination nationale du réseau des PCN organisera

- Un travail « collectif » et régulier avec le réseau Entreprise Europe (EEN)
- La mise en place de réunions rassemblant les deux réseaux ;
- Des formations sur les autres services de soutien européen ;
- La mise à jour d'une base de données de contact en région.

Organisation et animation du consortium

1 Organisation et animation du consortium

- **Analyser la participation**
  - Compléments au rapport de stage MESR sur le FP7 (ex: changement de règles en 2010?)
  - Analyse de la participation à l'appel sécurité 2014-2015
- **Liste de diffusion des acteurs Sécurité H2020**
  - Liste GTN, MESR
  - Liste des pôles, Liste CICS
  - Liste universités
  - .etc.
- **Suivre les autres appels européens**
  - Autres topics d'H2020 (MG-8-2 2014, COMPET6, FET PROACT 2 et 3 .etc.)
  - AED
  - DG HOME

Information et sensibilisation

2 Information et sensibilisation

✯ Journée d'information

- Journée System@tic à Paris/Ubifrance le 21 /01/2014
- Journée d'information le 20/03/2014 à Toulouse
- Infoday à Bruxelles le 1ier avril 2014

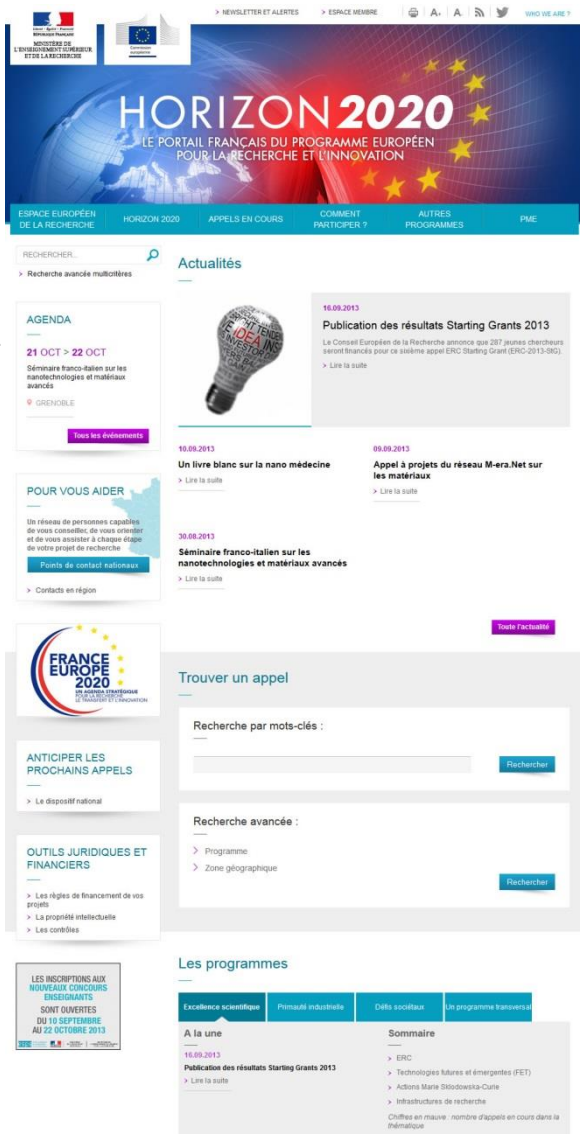
✯ Faire la promotion des lauréats

✯ Etoile de l'Europe: projet SECUREAU

✯ Support de communication: Plaquette, booklet Success stories, intérêt des acteurs pour l'appel à projets 2015 (ex: SERENITY)

✯ Réaliser de la documentation H2020 Sécurité

2 Site http://www.horizon2020.gouv.fr



Agenda

PCN

GTN, RCP

Outils juridiques et financiers

Menu de navigation

Zone « Actualités »

Zone « Trouver un appel »

Zone « Les programmes »

Page web Sécurité

Accueil > Horizon 2020 > Défis sociétaux > Sécurité

DES SOCIÉTÉS SÛRES - PROTÉGER LA LIBERTÉ ET LA SÉCURITÉ DE L'EUROPE ET DE SES CITOYENS

Actualités

21.01.2014

Publication des interventions de la journée sécurité numérique à Bruxelles

L'Unité Trust and Security de la D.G. CONNECT organisait le 15 janvier 2014 à Bruxelles la journée d'information sur les aspects sécurité numérique du programme Horizon...

> Lire la suite

20.01.2014

13.12.2013

LE DÉFI SÉCURITÉ

> Présentation

LE POINT DE CONTACT NATIONAL

> Présentation et contacts

HORIZON 20

2

✯ Evènements, salons pour rencontrer les participants potentiels à Horizon 2020

- EUROSATORY 16-20 juin 2014 (Stand Pôle Risques)
- MWC (Mobile World Congress) en mars 2015
- Congrès des sapeurs pompiers (SDIS) à Avignon en octobre 2014
- IT security expo à Nuremberg le 7-9 octobre 2014
- RU France - Allemagne (avec les FhG) sur les risques industriels à Aix le 13 novembre 2014
- ..autres..

Assistance, conseil et formation des porteurs de projets

3 Assistance, conseil et formation des porteurs de projets

- **Aide à la formation de consortiums**
  - Cluster
  - Equipe France
  - ANR France-Allemagne
  - Cartographie sur Cordis
- **Brokerage events européens**
  - SMIIG le 23-24 janvier 2014 à Bruxelles

- **Rencontrer les porteurs de projets, les participants à des consortiums**
  - L'EU veut se recentrer sur la programmation,
  - Exécution d'H2020 entre autres via les PCNs

Orientation et coopération avec d'autres réseaux

4 Orientations et coopération avec d'autres réseaux

- **Réunion des PCN**
  - PCN Sécurité à Bruxelles le 28 février 2014
  - PCN français le 28 mars 2014 au MESR
- **Participer au réseau des PCN (SEREN3)**
  - Partenaires associés
  - SEREN 3 cordonné par APRE (Italie)
- **Lien avec les autres réseaux**
  - SSH
  - PCN ICT
  - 3S Risques Sécurité Sureté en PACA

AOB

- Agenda
  - 01/04/14 - Bruxelles: Journée d'information sur les 4 appels du défi sécurité, y compris *brokerage event*
- Agenda GTN Sécurité pour 2014
  - 18 juin 14h
  - 24 septembre 14h
  - 3 décembre 14h