HORIZON 2020

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

# Rencontres académiques Industrie

## saclay – 19/12/2016

# Rôle du PCN

## Informer

- Journées d'information
- Mise en ligne d'information
- Lettre du PCN

## Orienter

- Adéquation idée de projet
- Opportunités de financement

## Conseiller

- Relecture d'abstract
- Discussion autour d'idées de projets
- Relecture Instrument PME

# L'équipe du PCN Sécurité

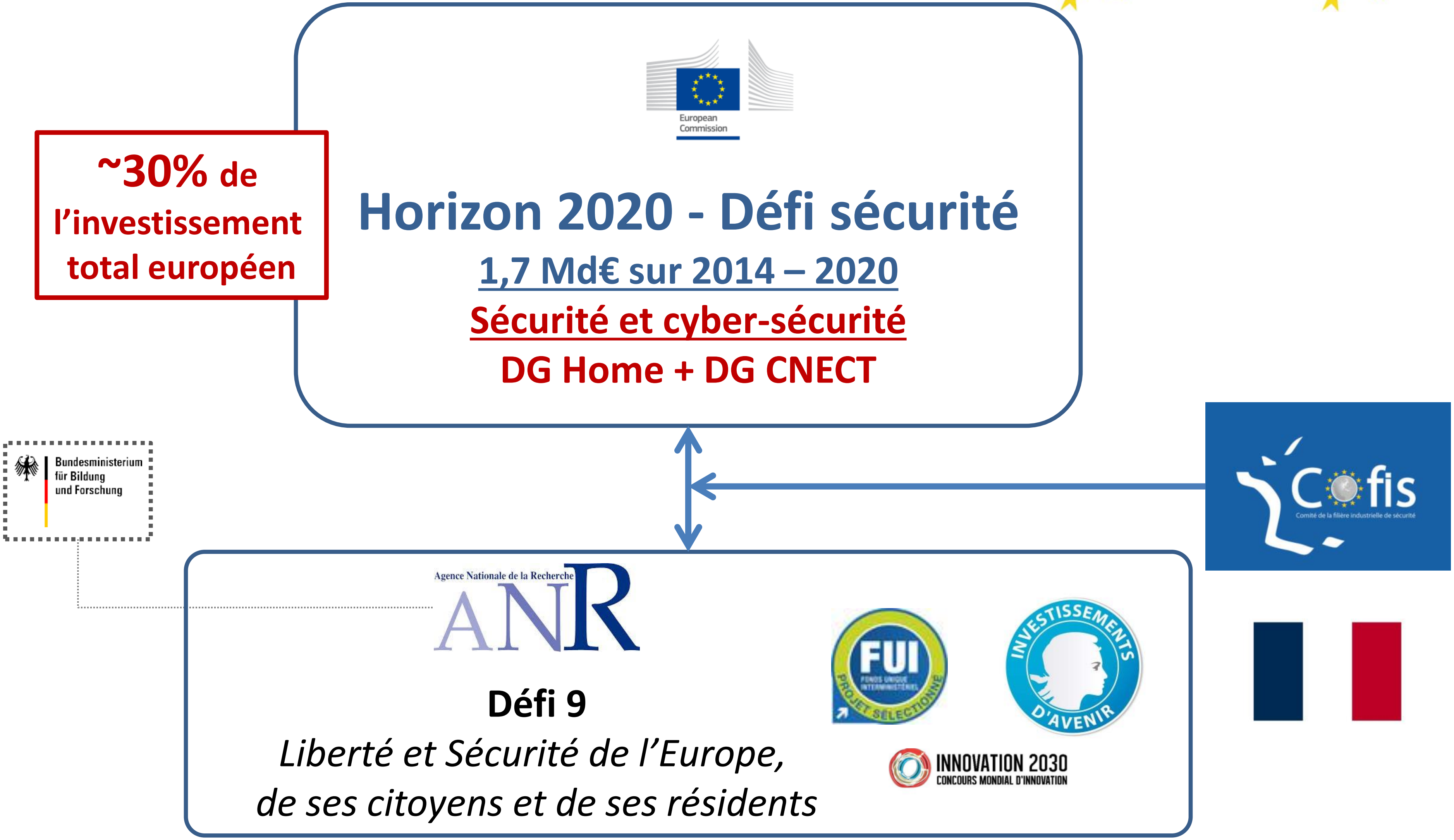
| | Prénom - NOM | Rôle | Etablissement |
|---|---|---|---|
| | Armand NACHEF | Coordinateur du PCN | CEA - Commissariat à l'Energie Atomique et aux Energies Alternatives |
| | Frédéric LAURENT | Représentant au Comité de Programme | Ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche |
| | François MURGADELLA | Représentant au Comité de Programme | SGDSN - Secrétariat Général de la Défense et de la sécurité Nationale |
| | Dominique SERAFIN | PCN | CEA - Commissariat à l'Energie Atomique et aux Energies Alternatives |
| | Isabelle de SUTTER | PCN | Systematic<br>Site Nano Innov |
| | Sébastien GIRAUD | PCN | Cluster SAFE |
| | Jean-Michel DUMAZ | PCN | Cluster SAFE |
| | Philippe MOGUEROU | PCN | Université de Rouen / CPU |

# Le paysage des programmes
# Sécurité

# LE PAYSAGE FR/UE DE LA RECHERCHE EN SÉCURITÉ

TIC PCN - Horizon2020

Sécurité PCN - Horizon2020



European Commission

## Horizon 2020 - Défi sécurité

1,7 Md€ sur 2014 – 2020

**Sécurité et cyber-sécurité**

**DG Home + DG CNECT**

**~30% de l'investissement total européen**

Bundesministerium für Bildung und Forschung

Cofis
Comité de la filière industrielle de sécurité

Agence Nationale de la Recherche
ANR

**Défi 9**

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

FUI
FONDS UNIQUE INTERMINISTÉRIEL
PROJET SÉLECTIONNÉ

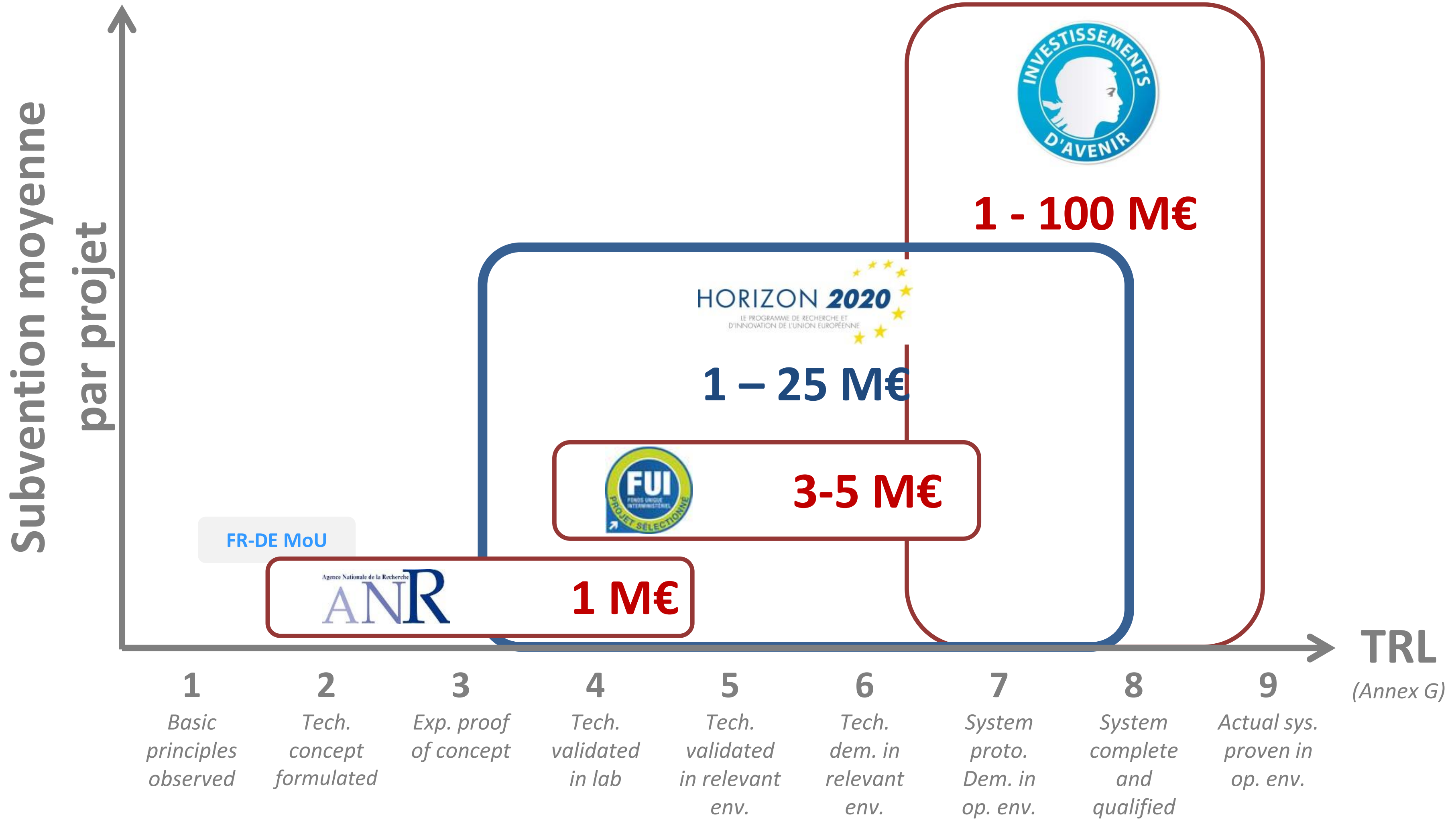
INVESTISSEMENTS D'AVENIR

INNOVATION 2030
CONCOURS MONDIAL D'INNOVATION

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

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

# Le panorama des soutiens nationaux et UE


Subvention moyenne par projet
INVESTISSEMENTS D'AVENIR
1 - 100 M€
HORIZON 2020
LE PROGRAMME DE RECHERCHE ET D'INNOVATION DE L'UNION EUROPÉENNE
1 – 25 M€
FUI
PROJET SÉLECTIONNÉ
3-5 M€
FR-DE MoU
Agence Nationale de la Recherche
ANR
1 M€
TRL
(Annex G)
1
Basic principles observed
2
Tech. concept formulated
3
Exp. proof of concept
4
Tech. validated in lab
5
Tech. validated in relevant env.
6
Tech. dem. in relevant env.
7
System proto. Dem. in op. env.
8
System complete and qualified
9
Actual sys. proven in op. env.

# Le programme Sécurité depuis 2007

European Commission

Security Research Projects
under the 7th Framework Programme for Research

EU Research for a Secure Society

May 2014

Catalogue
des projets

2007 – 2014
~ 450 projets
1,5 Md€
~200 M€ pour FR
>150 bénéficiaires FR dont ~50 PME

# Appels Sécurité
# En lien avec les TIC

# Orientations principales du WP16-17 (1)

## Une participation obligatoire des utilisateurs finaux (**en tant que partenaires**), dont les missions incluent :

- Les spécifications fonctionnelles et la validation de la solution (haut du cycle en V)
- La mise à disposition de composants de démonstrateurs (locaux, logiciels, systèmes, etc.)
- La quantification des impacts estimés pour améliorer la sécurité

## Orientation du programme vers des **pilotes** et des **missions de sécurité**

- Démonstrateurs avec des TRLs généralement élevés (atteignant le niveau 8)

## Prise en compte accrue de la **dimension sociétale**

- Les SHS doivent être complètement intégrées dans le projet
  - Sociologie des usagers
  - Mécanismes de l'innovation, etc.

## **Soutien à l'industrie de l'UE pour être compétitive**

- Les business plans et les analyse économiques doivent être expliquées

# Orientations principales du WP16-17 (2)

## Une structure sur 3 appels principaux

- Protection des infrastructures critiques (DG CNECT + Home)
- Sécurité (DG Home)
- Digital security (DG CNECT)

## Budget:

- ~175 M€ en 2016
- ~197 M€ en 2017

## Les principaux changements par rapport au WP14-15:

- Un nombre de sujets plus limité (~33 vs. 55)
- **Des enveloppes réservées pour une majorité de sujets** (i.e. pas de compétition entre ces sujets)
- Des budgets par projet plus prescriptifs
- Des sujets plus resserrés ou au contraire très ouverts (et un texte globalement de meilleure qualité)
- **Une plus grande participation des utilisateurs finaux/practitioners attendue**
- Des règles *Special modalities* (fortement) assouplies et en nombre (très restreint)

# Thèmes des appels 2017

## CIP

~~Water Systems~~

——

~~Energy Infrastructure~~
~~(power plants and distribution)~~

——

~~Transport~~
~~Infrastructure and means of transportation~~

Communication Infrastructure

Health Services

Financial Services

## SEC-DRS

Broadband Comm. Systems

CBRN cluster

## SEC-GM

Clusters of practitioners

## SEC-FCT

Human Factor (with subtopics)
~~Crowd protection~~

Tools for forensic laboratories

Detection and data fusion (in sewage networks)

Prevention Investigation Mitigation (with subtopics)

## SEC-BES

Information system to EU external policy

Risk-based screening border crossing

Through-foliage detection

Big Data for customs

No gate crossing point solutions

## DS

Cryptography

Advanced threats

Privacy, data protection

## SME-Inst

Engaging SMEs in security R&D (SMEInst-13)

# Appel CIP – 2016-2017 (1)

**Sujet poussé notamment par FR**

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

**Budget total = 40M€**

# Appel CIP – 2016-2017 (2)

## Appel *Critical Infrastructure protection* (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
- ~8 M€/projet (soit 2 à 3 par an)
- Type d'action: IA
- Spécificités:
    - **1 seul projet par IC sur l'ensemble de la période 16-17**
    - **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.*

# DRS topics –2017

| Topic (Type of Action) | Budget (M€) | Deadline | Title |
|---|---|---|---|
| SEC-04-DRS-2017 (PCP) | 10.0 | 24 / 08 / 2017 | Broadband communication systems |
| SEC-05-DRS-2016-2017 (RIA) | 14.0 | 24 / 08 / 2017 | CBRN cluster |

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

*So far each EU Member States has adopted its own (broadband) radio-communication system for security forces (police, first responders, etc.).*

*The EU has funded a CSA (Call DRS-18-2015) for buyers of such systems to overcome this issue*

*Following the CSA requirements the topic may be updated*

- **Pre-Commercial Procurement (COFUND PCP)**
  *Pre-Commercial Procurement (PCP) is procurement of R&D services.*
  *The funding rate for PCP actions is limited to 90% of the total eligible costs*

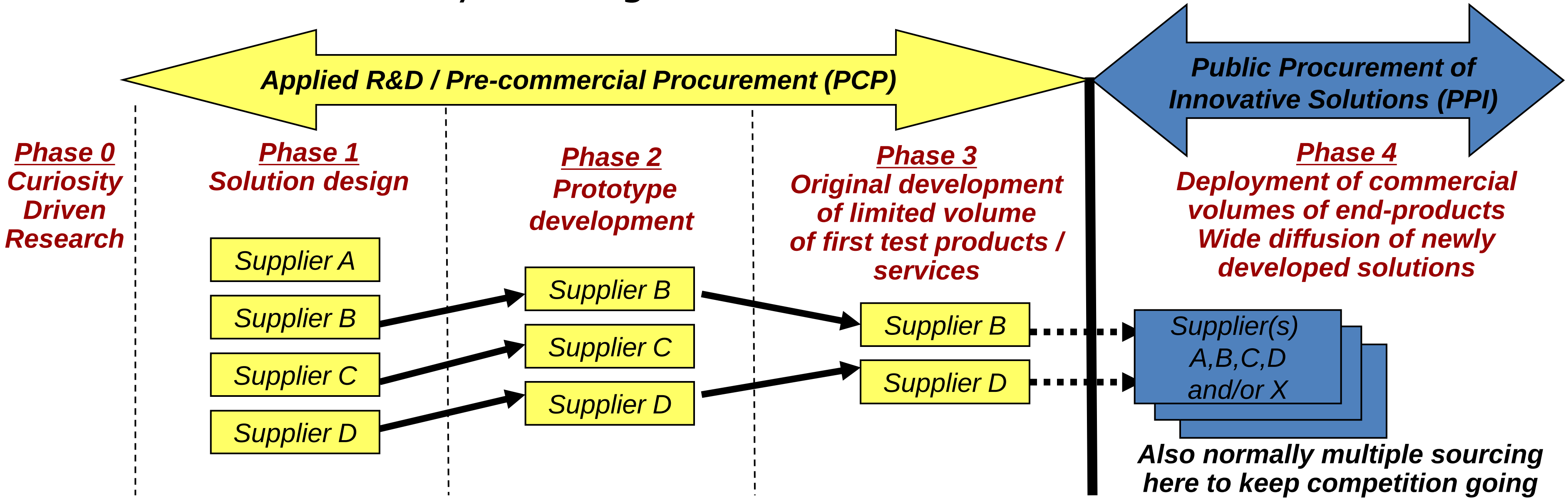
- Outcome TRL: **8**
- Budget: **10 M€ per project**
- Total budget: **10 M€** → 1 funded project

- Must involve buyer organizations from at least **12** Member States or Associated Countries
- Grant beneficiaries will be subject to additional Intellectual Property Rights obligations
  - The PCP outcome must become available to EU MS national authorities not participating in the PCP for further procurement purposes

# Pre-Commercial Procurements

**PCP** to steer the development of solutions towards concrete public sector needs, whilst comparing alternative solution approaches from various vendors

**PPI** to act as launching customer / first buyer of innovative commercial end-solutions newly arriving on the market



Applied R&D / Pre-commercial Procurement (PCP)
Public Procurement of Innovative Solutions (PPI)
Phase 0
Curiosity Driven Research
Phase 1
Solution design
Phase 2
Prototype development
Phase 3
Original development of limited volume of first test products / services
Phase 4
Deployment of commercial volumes of end-products Wide diffusion of newly developed solutions
Supplier A
Supplier B
Supplier C
Supplier D
Supplier B
Supplier C
Supplier D
Supplier B
Supplier D
Supplier(s) A,B,C,D and/or X
Also normally multiple sourcing here to keep competition going

Objectives:

- Price/quality products that better fit public sector needs
- Earlier customer feedback for companies developing solutions
- Better take-up/Wider commercialisation of R&D results

# FCT topics –2017

SEC-FCT

| Topic (Type of Action) | Budget (M€) | Deadline | Title |
|---|---|---|---|
| SEC-07-FCT-2016-2017 (RIA) | 6 → ~7.0 | 24 / 08 / 2017 | Human Factor to mitigate terrorist acts |
| SEC-09-FCT-2017 (PCP) | 10.0 | 24 / 08 / 2017 | Tools and techniques for forensic laboratories |
| SEC-10-FCT-2017 (IA) | 16.0 | 24 / 08 / 2017 | Integration of detection capabilities and data fusion with utility providers’ |
| SEC-12-FCT-2016-2017 (RIA) | 10→ 14.0 | 24 / 08 / 2017 | Prevention, investigation, and risk mitigation |

# SEC-07-FCT-2016-2017:
# Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts

*Proposals should address only one of the following aspects:*

1. ~~*New methods for the protection of crowds during mass gatherings;*~~

**Couvert**

2. ***New methods to prevent, investigate and mitigate cybercriminal behaviours****;*
3. *New methods to prevent, investigate and mitigate corruption and financial crime to fight the infiltration of organised crime in the European Union (licit) economy;*
4. *New methods to prevent, investigate and mitigate high impact petty crimes;*
5. *New methods to prevent, investigate and mitigate high impact domestic violence*

- **Research and Innovation Action**
- Outcome TRL: **not provided but demonstrations are required**
- Budget: **3 M€ per project**
- Total budget: **17 M€** for SEC-06 and SEC-07 in 2016
  **12 M€** for SEC-07 and SEC-18 in 2017
  → Maximum 2 projects in 2017
- Maximum 1 funded project per sub topic

- Practitioners from various disciplines, including a minimum of **5 LEAs** from 5 EU Member States or Associated Countries
- Any proposal must include a workpackage for practical demonstrations

# SEC-09-FCT-2017: Toolkits integrating tools and techniques for forensic laboratories

*Heterogeneous, forensic tools are in use across Europe, making the exchange of information among forensic laboratories difficult. This limits the use of forensic data in cross-border investigations, and in foreign courts.*
*Forensic data need to be quickly available, at an acceptable cost, across borders.*

- **Pre-Commercial Procurement (COFUND PCP)**
  *Pre-Commercial Procurement (PCP) is procurement of R&D services.*
  *The funding rate for PCP actions is limited to 90% of the total eligible costs*

- Outcome TRL: **8**
- Budget: **10 M€ per projet**
- 1 funded project

- Forensic laboratories or institutes from a minimum of **5 EU Member States** or international organisations.
  Additional participation of laboratories from Associated Countries is encouraged
- Grant beneficiaries will be subject to the additional obligations aiming to ensure exploitation of the project results

# SEC-10-FCT-2017: Integration of detection capabilities and data fusion with utility providers' networks

*Deployment of detection systems in utility networks (e.g. to measure energy consumption, characteristics of used waters, air quality, etc.),*
*for instance for the detection of explosive precursors and illegal chemicals (drugs)*

- **Innovation Action**
- Outcome TRL: **7 to 8 for the sensors deployed**
  **6 for the information system and mobile platform**
- Budget: **8 M€ per project**
- Total budget: **16 M€** → 2 funded projects

- Coordination with activities of the EDA may be considered
- A minimum of 2 independent utility network operators; and a minimum of 3 Law enforcement agencies (LEA) in charge of counter-terrorism, or bomb squad units, from 3 different EU Members States
  Additional participation from LEAs from Associated Countries is encouraged
- Demonstrations must take place in at least 2 agglomerations: One of over 1000000 inhabitants, and another of between 100000 and 300000 inhabitants, located in 2 different Member States, and using different types of sewage systems

## SEC-12-FCT-2016-2017:
## Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism

*Organized crime and terrorist organizations are at the forefront of technological innovation in planning, executing and concealing their criminal activities*

*4 sub-topics*

1. *cyber-crime: virtual/crypto currencies des-anonymisation/tracing/impairing where they support underground markets in the darknet.*
2. *detection and neutralization of rogue/suspicious light drone/UAV flying over restricted areas, and involving as beneficiaries, where appropriate, the operators of infrastructure*
3. *video analysis in the context of legal investigation*
4. *Others, provided that it involves a sufficient number of LEAs*

- **Research and Innovation Action**
- Outcome TRL: **6**
- Budget: **5 M€ per project**
- Total budget: **27.25 M€** for SEC-08, SEC-11 and SEC-12, in 2016<br>**10 M€** in 2017

- Maximum 1 funded project per sub-topic

- A minimum of 3 Law enforcement agencies (LEA) from 3 EU Member States or Associated Countries for sub-topics 1, 2 and 3

- A minimum of 5 LEA from 5 EU Member States or Associated Countries for 4 (Others)

- Proposals on detection technologies are excluded from this topic

- Any proposal must include a workpackage for field demonstrations

# BES topics –2017

SEC-BES

| Topic (Type of Action) | | Budget (M €) | Deadline | Title |
|---|---|---|---|---|
| SEC-13-BES-2017 | (PCP) | 10.0 | 24 / 08 / 2017 | Information System for the EU external policy |
| SEC-15-BES-2017 | (IA) | 8.0 | 24 / 08 / 2017 | Risk-based screening at border crossing |
| SEC-16-BES-2017 | (RIA) | 8.0 | 24 / 08 / 2017 | Through-foliage detection |
| SEC-17-BES-2017 | (RIA) | 10.0 | 24 / 08 / 2017 | Big data and data analytics for customs |
| SEC-18-BES-2017 | (RIA) | 6.0 → ~7.0 | 24 / 08 / 2017 | Acceptance of "no gate crossing point solutions" |

# SEC-13-BES-2017: Next generation of information systems to support EU external policies

*Development of a cost-effective common Situational Awareness, Information Exchange and Operation Control Platform, to support the Common Security and Defence Policy civilians' missions*

- **Pre-Commercial Procurement (COFUND PCP)**
  *Pre-Commercial Procurement (PCP) is procurement of R&D services.*
  *The funding rate for PCP actions is limited to 90% of the total eligible costs*

- Outcome TRL: **8**
- Budget: **10 M€ per project**
- Total budget: **10 M€** → 1 projet

- Coordination with European Defence Agency (EDA)

- A minimum of 3 potential users/buyers of such information systems from 3 different EU Member States
- Beneficiaries will be subject to additional obligations aiming to ensure exploitation of the results

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

*Maintaining the current level of border checks is becoming increasingly expensive given the ever growing volumes of people and goods on the move.*
*Thorough checks could be limited to fewer individual goods and people pre-selected further to a preliminary risk-based screening of the flows*

- **Innovation Action**
- Outcome TRL: **7**
- Budget: **8 M€ per project**
- Total budget: **8 M€** → 1 funded project

- Collaboration with the International Air Transport Association (IATA), the air transport industry and stakeholders in other fields of transport safety (e.g. maritime, rail) may lead to the development of new solutions

- At least 3 border guard authorities or custom authorities from 3 EU or Schengen Member States

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

*For the traveler it would be ideal to cross borders without being slowed down.*

*In the next 10 years, technologies will become available. Some are to be deployed in the vicinity of border crossing points, others can be mobile and used to check travellers data along his/her journey.*

*Privacy becomes a main issue. Thus, the societal and political acceptance of technologies is required.*

- **Research and Innovation Action**
- Outcome TRL: **non spécifié**
- Budget: **3 M€ per project**
- Total budget: **6 M€** → 2 funded projects

- At least 3 border guard authorities or custom authorities from 3 EU or Schengen Member States

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

*Detecting, locating, tracking or identifying persons and vehicles crossing the border in forested regions. is extremely difficult given that technologies for surveillance through harsh unstructured environments are currently not effective.*
*The increasing risk of irregular flows and immigration across the border with, for instance, Turkey, Ukraine, Belarus, Russia or Brazil makes the issue even more acute than in the past.*

- **Research and Innovation Action**
- Outcome TRL: **5 or 6**
- Budget: **8 M€ per project**
- Total budget: **8 M€** → 1 funded project

- Coordination with European Defence Agency (EDA)
- At least 3 border guard authorities from 3 EU Member States or Associated Countries

# SEC-17-BES-2017:
# Architectures and organizations, big data and data analytics for customs risk management of the international goods supply chain trade movements

*Improving customs risk management and supply chain security.*
*A need for customs to acquire quality data on supply chain movements, to exploit them for risk assessment purposes, and to make checks more efficient*

- **Research and Innovation Action**
- Outcome TRL: **not provided**
- Budget: **5 M€ per project**
- Total budget: **10 M€** → 2 funded projects

- At least 3 border guard or custom authorities from 3 EU or Schengen Member States or Associated Countries

# Appels cybersécurité

# Eléments statistiques
# sur les appels « cybersécurité »

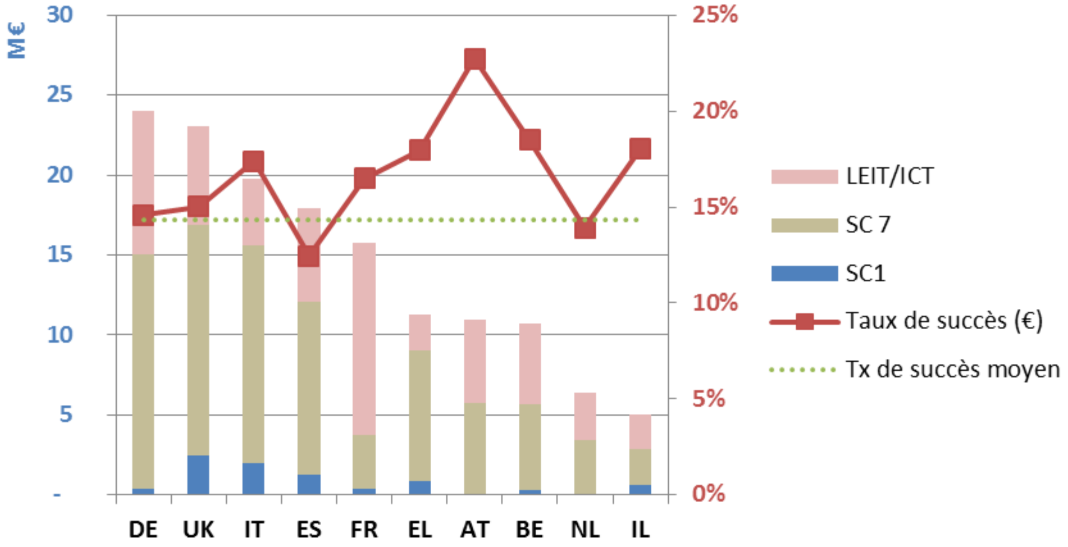
15 à 20 projets soutenus par an

>70 M€/an sur les questions cyber depuis 2014

Un taux de succès global de 14,3%

Un résultat FR très contrasté:

- 19,3% sur LEIT/ICT (assurance models, certification, security-by-design, crypto.)
- 3,3% sur SC7 (privacy, access control, assurance models, cybersec. management, trust eservices) => tendance confirmée en 2016 (au mieux un projet R&T!)



20,5 M€

Deadline: 25/04/17

# DS-06-2017: Cryptography (RIA)

- *In line with technological developments and emerging threats, the improvement of performance and efficiency of cryptographic solutions is a persistent need across ICT.*

- Nine thematic research challenges, including:
  - Ultra-lightweight, High speed, Implementation, Authenticated encrypted tokens

- TRL de sortie entre 3 et 5
- Increase trust in ICT and online services
- Protect the European Fundamental Rights of citizens

  Privacy, Data Protection

**Taille projets : 3-5 M€**

# DS-06-2017 (2/2) Cryptography

Proposals may address **one or more** of the areas/challenges below

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

18 M€

Deadline: 24/08/17

# DS-07-2017: Addressing Advanced Cyber Security Threats and Threat Actors

- Situational Awareness (RIA);
  - Detect and quickly and effectively respond to sophisticated cyber-attacks;
  - Interdisciplinary research to counter threat actors and their methods;
  - Assess and address the impact to fundamental rights, data protection and privacy in particular;
- Simulation Environments, Training (IA);
  - Prepare those tasked with defending high-risk organisations;
  - Realistic environments; Tools for producing both benign and malicious system events;
  - May also address crisis management and decision making processes in relation to obligations stemming from applicable legal frameworks

**Taille projets : 2-3 M€ (RIA) ; 4-5 M€ (IA)**

18 M€

Deadline: 24/08/17

# DS-08-2017: Privacy, Data Protection, Digital Identities (IA)

- Privacy-enhancing Technologies (PET)
- General Data Protection Regulation in practice
- Secure digital identities
- Support for Fundamental Rights in Digital Society.
- Increased Trust and Confidence in the Digital Single Market
- Increase in the use of privacy-by-design principles in ICT systems and services

Taille projets : 2-3 M€

# Autres appels en lien avec sécurité

RIA

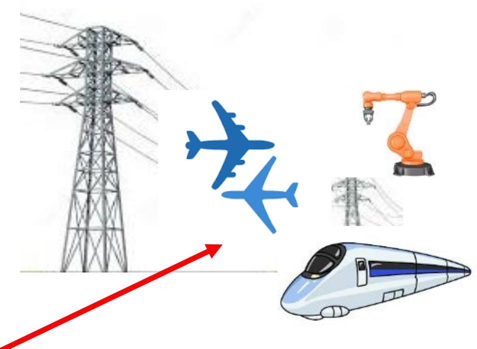
Deadline
25 April 2017

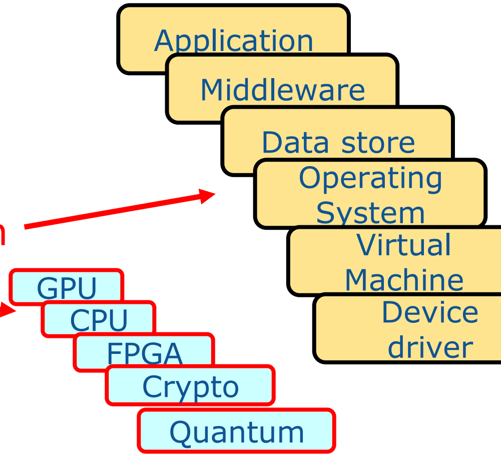
Budget
20 M€

# ICT 5 - Customised and low energy computing

## What we ask for (RIA)

## Programming environments and toolboxes for low energy and highly parallel computing





- optimised for specific application domains
- ideally covering complete software stack from runtime to application
- supporting multicore and heterogeneous architectures
- supporting non-functional requirements: time criticality, power, reliability, security, etc…
- reuse and extension of existing solutions is OK

**Suggested EU contribution: 4 to 6 million (not binding!)**

**37 M€**

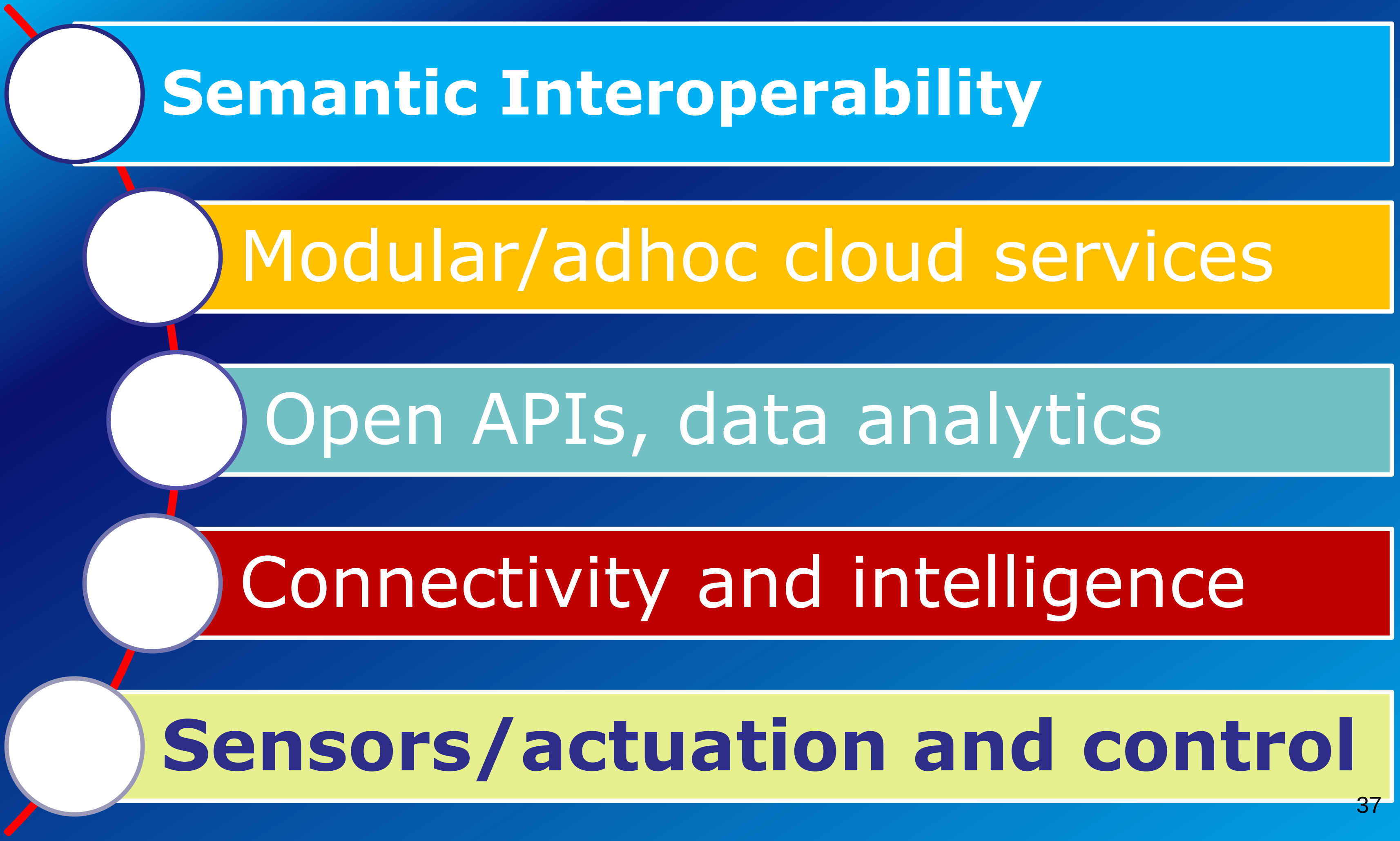
**3-5 M€ /projet**

# RIA IoT-03-2017: R&I on IoT integration and platforms

## Scope:

- **Architectures, concepts, methods and tools**
  for open IoT platforms integrating evolving sensing, actuating, energy harvesting, networking and interface technologies.
  - **Platforms** providing connectivity and intelligence, actuation and control features, linkage to modular and ad-hoc cloud services, data analytics and open APIs as well as semantic interoperability across use cases and conflict resolution.
  - Platforms should be compatible with existing international developments addressing object identity management, discovery services, virtualisation of objects, devices and infrastructures and trusted IoT approaches.
- **IoT Security and Privacy**
  advanced concepts for end-to-end security in highly distributed, heterogeneous and dynamic IoT environments. Approaches include identification and authentication, data protection and prevention against cyber-attacks at the device and system levels.
- **Other proposal characteristics**: To include two or more usage scenarios, verification and testing, and identify the added value of the proposed approach specific to IoT in comparison to generic solutions.

## Specific Platform Considerations



- Semantic Interoperability
- Modular/adhoc cloud services
- Open APIs, data analytics
- Connectivity and intelligence
- Sensors/actuation and control

# Le cPPP Cyber

# SIGNATURE CEREMONY – July 5, 2016

## Commissioner Oettinger

46 ORGANISATIONS
14 DIFFERENT COUNTRIES
MORE THAN 300 TWEETS
180 TWITTER FOLLOWERS
1,610 WEBSITE VIEWS

2

“Cybersecurity needs trust and confidence We have to invest in cybersecurity. This means financial investment, technological investment and human investment”

“This PPP is the beginning of a  team work”

“It is our ambition to stabilise cybersecurity in our digital infrastructure and to leverage upon our industries to develop a European culture of cybersecurity”

“Cybersecurity is a shared responsibility we need your economic and technical competence”

“We are expecting from your side advise on what should be done from our side“

# Budget

- Commission contribution to the cPPP for R&I initiatives (from H2020 budget): **€450 mln for the 2017-2020 calls (4 years)**
- **Leverage factor = 3**

  The cPPP should demonstrate that the €450mln will trigger investments linked to R&I for 3*450= € 1350mln in the next (typically) 10 years
- Contributions are expected from private investments (users/operators, suppliers, RTOs/Universities, national R&I funds, other EU funds: regional / structural, capital venture, insurances, etc.) and public funding

# Cybersecurity: a different cPPP

- Cybersecurity: a transversal issue, pervasive in all sector (economic, societal, …): large number of stakeholders, of interests, of constraints…
- Security: a national prerogative. Stronger participation of representatives from the national administrations, also at decision making level (not just a "mirror group")
- Interest from national Public Administrations:  Representatives to the two PCs + Ministries (Interior, Economy, etc.) + Regulatory Bodies + Public users

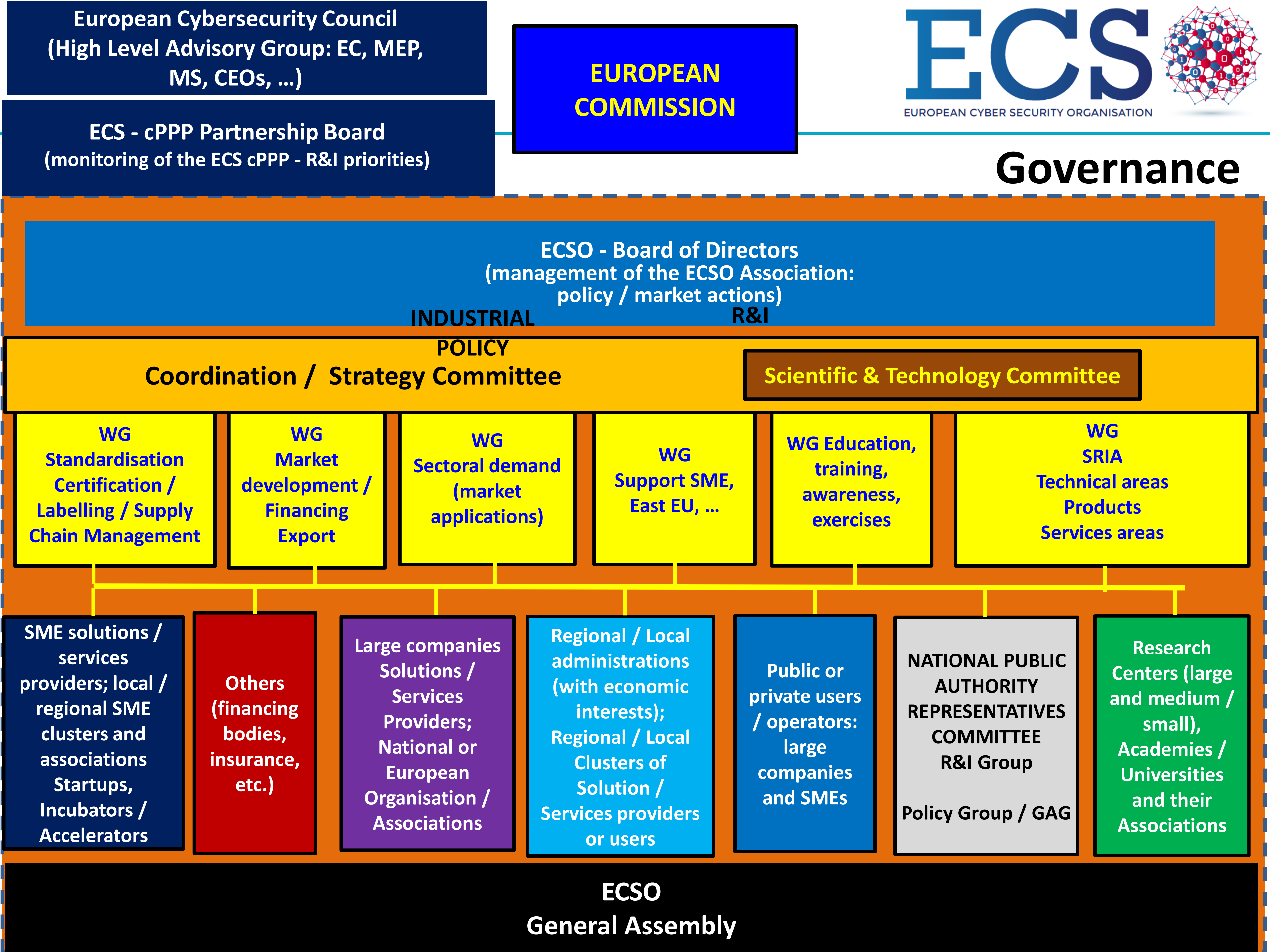
- cPPP: leveraging upon H2020 rules
- Open to any entity eligible under H2020 (EU MS + EEA / EFTA countries)

- **The cPPP will focus on R&I, developing a SRIA and supporting its implementation in the H2020 Work Programme**

- **The ECSO Association will tackle other industry policy aspects for the market and the industrial / economic development**
- **ECSO will support the development of the European cybersecurity industry and EU trusted solutions, including cooperation with Third Countries.**

# Governance

ECS
EUROPEAN CYBER SECURITY ORGANISATION



European Cybersecurity Council
(High Level Advisory Group: EC, MEP, MS, CEOs, …)

ECS - cPPP Partnership Board
(monitoring of the ECS cPPP - R&I priorities)

EUROPEAN COMMISSION

ECSO - Board of Directors
(management of the ECSO Association: policy / market actions)

INDUSTRIAL POLICY

R&I

Coordination / Strategy Committee

Scientific & Technology Committee

WG Standardisation Certification / Labelling / Supply Chain Management

WG Market development / Financing Export

WG Sectoral demand (market applications)

WG Support SME, East EU, …

WG Education, training, awareness, exercises

WG SRIA Technical areas Products Services areas

SME solutions / services providers; local / regional SME clusters and associations Startups, Incubators / Accelerators

Others (financing bodies, insurance, etc.)

Large companies Solutions / Services Providers; National or European Organisation / Associations

Regional / Local administrations (with economic interests); Regional / Local Clusters of Solution / Services providers or users

Public or private users / operators: large companies and SMEs

NATIONAL PUBLIC AUTHORITY REPRESENTATIVES COMMITTEE
R&I Group

Policy Group / GAG

Research Centers (large and medium / small), Academies / Universities and their Associations

ECSO
General Assembly

# ECSO Membership (152 from 23 countries)

**To be admitted as a Member, the party should be:**

a) Legal Entity established at least in an EU Member State, an EEA / EFTA country or an associated country (called: "ECSO Countries")

b) A public body from an ECSO Country.

**CATEGORIES OF MEMBERS**

a) Large companies : cybersecurity solutions / services providers;

b) National and European Organisation / Associations (gathering large companies and SMEs) representing interests at national or European / International level.

c) SME solutions / services providers directly represented; Associations composed only by SME, Startups, Incubators, Accelerators.

d) Users / Operators (where cybersecurity technology / solutions / services provision is not one their business activities): National public administrations or private companies (large or SMEs) directly represented.

e) Regional / Local public administrations (with economic interests); Regional / Local Clusters of public / private Legal Entities with local economic / ecosystem development interests.

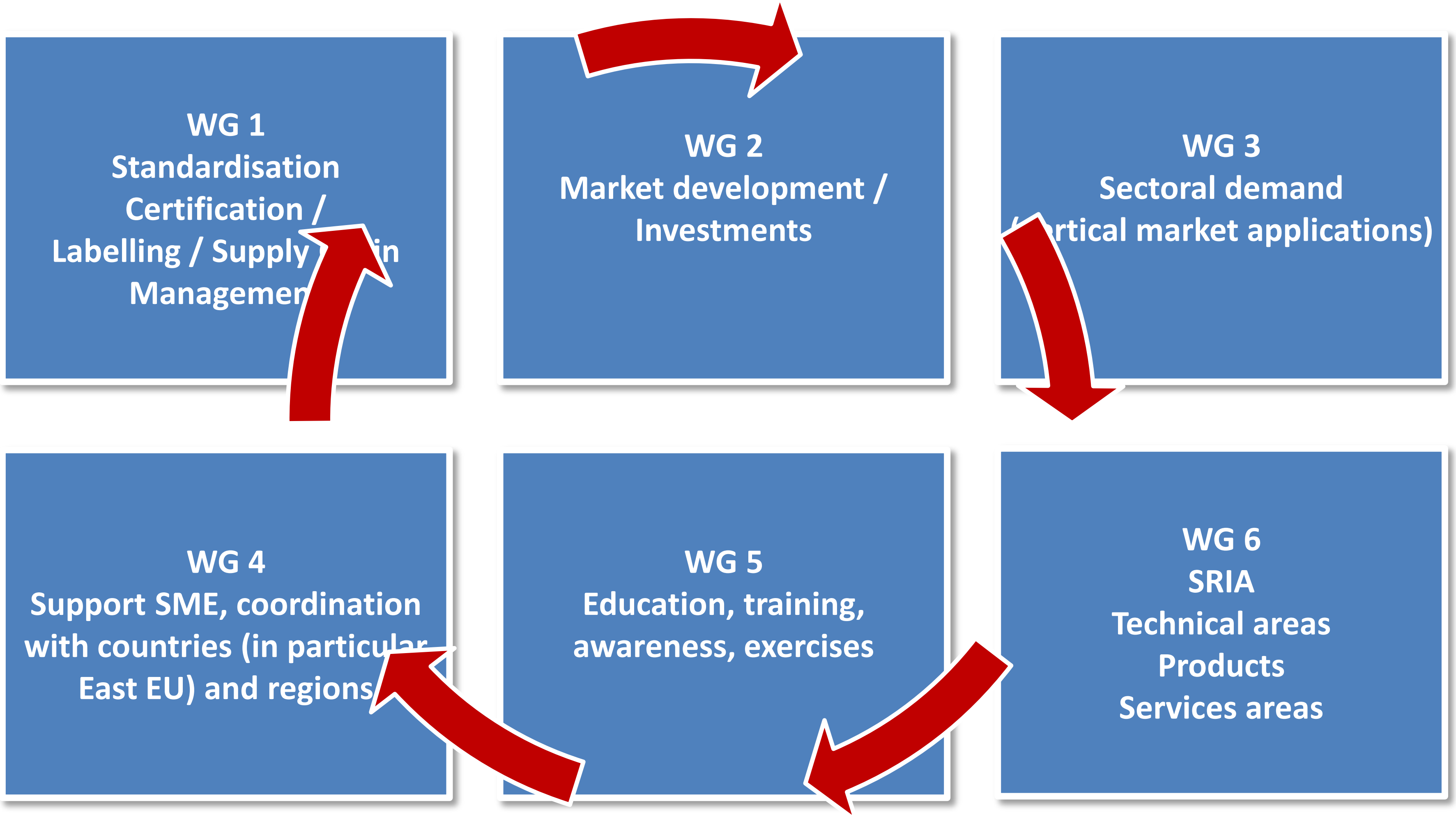
f) Public Administrations at national level (national strategy / regulatory / policy issues, incl. R&I coordination).

g) Research Centers, Academies / Universities; Associations composed only by Research Centers, Academies or Universities.

h) Others (financing bodies, insurances, consultants, etc.).

# WORKING GROUPS & TASK FORCES

ECS
EUROPEAN CYBER SECURITY ORGANISATION



WG 1
Standardisation
Certification /
Labelling / Supply Chain
Management

WG 2
Market development /
Investments

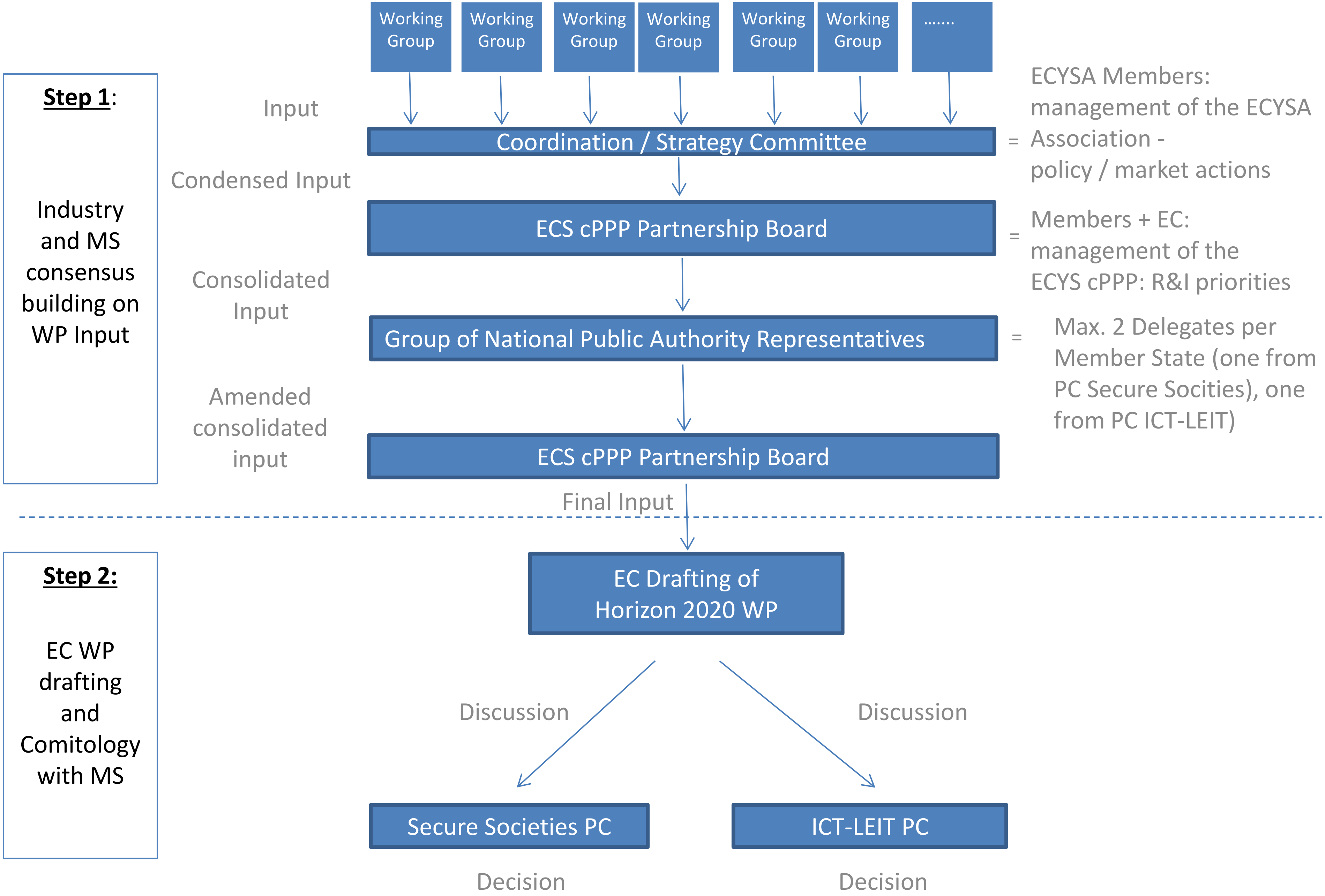
WG 3
Sectoral demand
(vertical market applications)

WG 4
Support SME, coordination
with countries (in particular
East EU) and regions

WG 5
Education, training,
awareness, exercises

WG 6
SRIA
Technical areas
Products
Services areas

# SRA Decision Making Process for ECSO



**Step 1**:

Industry and MS consensus building on WP Input

Working Group

Working Group

Working Group

Working Group

Working Group

Working Group

.......

Input

Coordination / Strategy Committee

= ECYSA Members: management of the ECYSA Association - policy / market actions

Condensed Input

ECS cPPP Partnership Board

= Members + EC: management of the ECYS cPPP: R&I priorities

Consolidated Input

Group of National Public Authority Representatives

= Max. 2 Delegates per Member State (one from PC Secure Socities), one from PC ICT-LEIT)

Amended consolidated input

ECS cPPP Partnership Board

Final Input

**Step 2:**

EC WP drafting and Comitology with MS

EC Drafting of Horizon 2020 WP

Discussion

Discussion

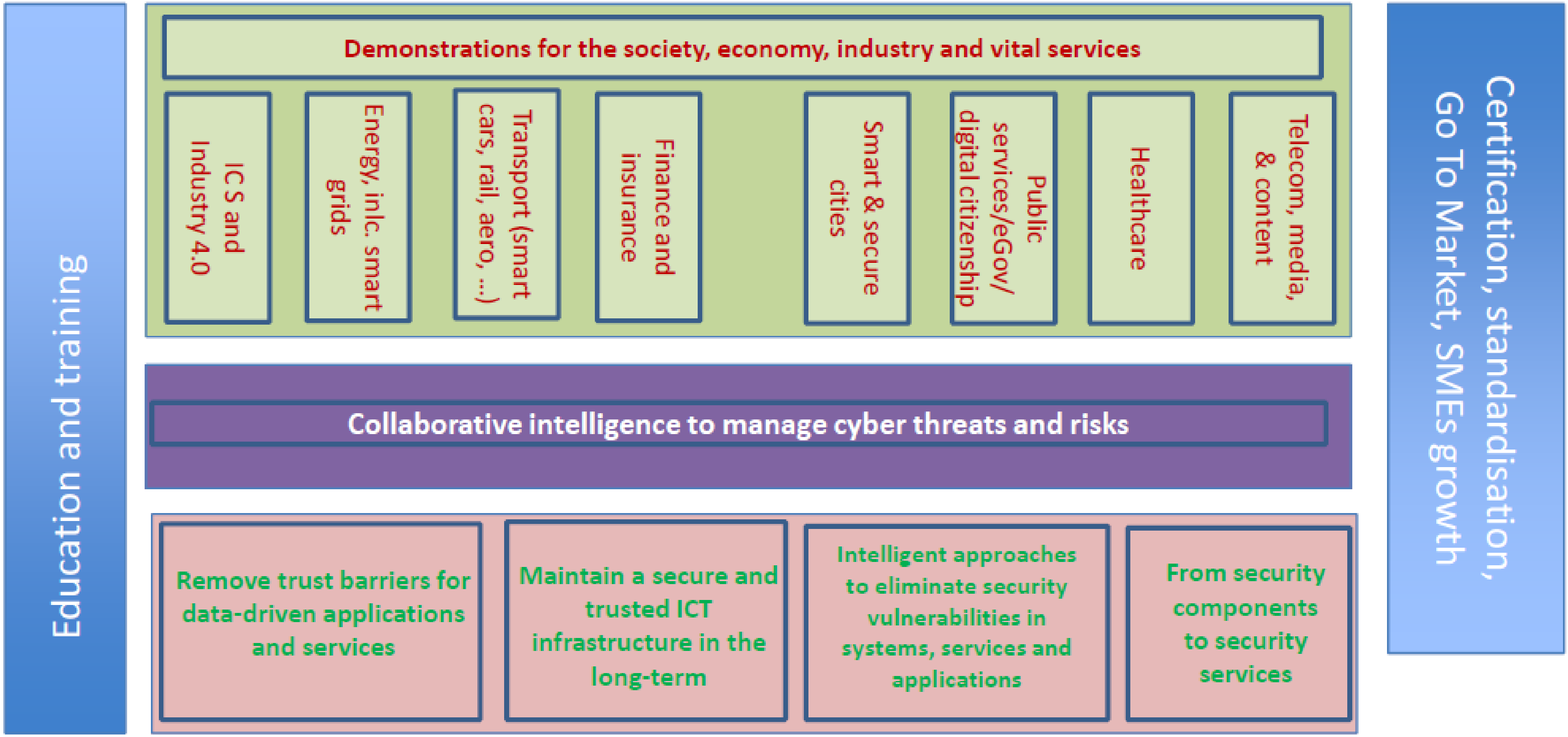
Secure Societies PC

ICT-LEIT PC

Decision

Decision

# Activités ECSO – priorités (1)



Education and training

Demonstrations for the society, economy, industry and vital services

ICS and Industry 4.0

Energy, inlc. smart grids

Transport (smart cars, rail, aero, …)

Finance and insurance

Smart & secure cities

Public services/eGov/ digital citizenship

Healthcare

Telecom, media, & content

Collaborative intelligence to manage cyber threats and risks

Remove trust barriers for data-driven applications and services

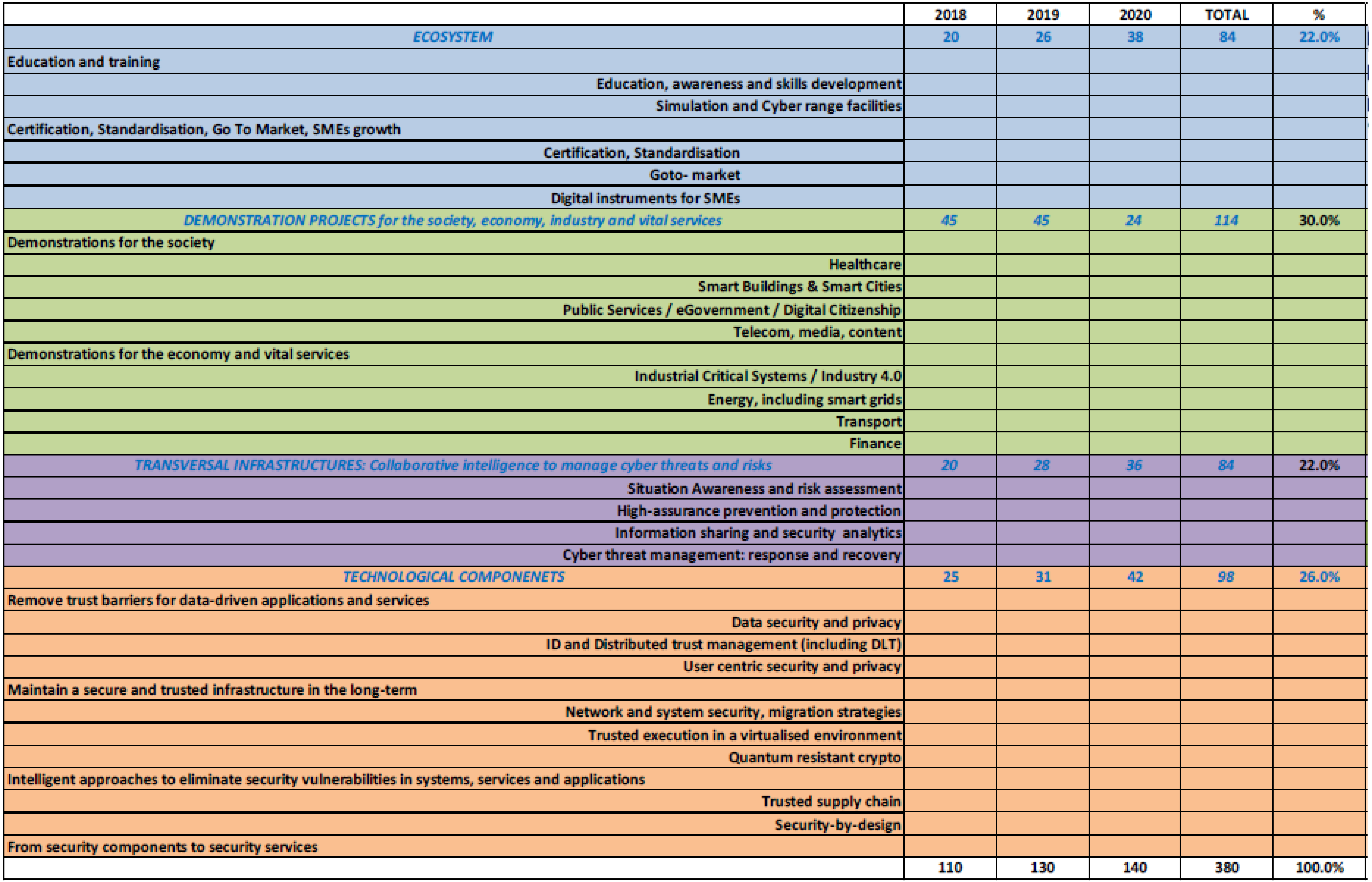
Maintain a secure and trusted ICT infrastructure in the long-term

Intelligent approaches to eliminate security vulnerabilities in systems, services and applications

From security components to security services

Certification, standardisation, Go To Market, SMEs growth

# Activités ECSO – priorités (2)



| | 2018 | 2019 | 2020 | TOTAL | % |
|---|---|---|---|---|---|
| *ECOSYSTEM* | 20 | 26 | 38 | 84 | 22.0% |
| Education and training | | | | | |
| Education, awareness and skills development | | | | | |
| Simulation and Cyber range facilities | | | | | |
| Certification, Standardisation, Go To Market, SMEs growth | | | | | |
| Certification, Standardisation | | | | | |
| Goto- market | | | | | |
| Digital instruments for SMEs | | | | | |
| *DEMONSTRATION PROJECTS for the society, economy, industry and vital services* | *45* | *45* | *24* | *114* | 30.0% |
| Demonstrations for the society | | | | | |
| Healthcare | | | | | |
| Smart Buildings & Smart Cities | | | | | |
| Public Services / eGovernment / Digital Citizenship | | | | | |
| Telecom, media, content | | | | | |
| Demonstrations for the economy and vital services | | | | | |
| Industrial Critical Systems / Industry 4.0 | | | | | |
| Energy, including smart grids | | | | | |
| Transport | | | | | |
| Finance | | | | | |
| *TRANSVERSAL INFRASTRUCTURES: Collaborative intelligence to manage cyber threats and risks* | *20* | *28* | *36* | *84* | 22.0% |
| Situation Awareness and risk assessment | | | | | |
| High-assurance prevention and protection | | | | | |
| Information sharing and security analytics | | | | | |
| Cyber threat management: response and recovery | | | | | |
| *TECHNOLOGICAL COMPONENETS* | 25 | 31 | 42 | *98* | 26.0% |
| Remove trust barriers for data-driven applications and services | | | | | |
| Data security and privacy | | | | | |
| ID and Distributed trust management (including DLT) | | | | | |
| User centric security and privacy | | | | | |
| Maintain a secure and trusted infrastructure in the long-term | | | | | |
| Network and system security, migration strategies | | | | | |
| Trusted execution in a virtualised environment | | | | | |
| Quantum resistant crypto | | | | | |
| Intelligent approaches to eliminate security vulnerabilities in systems, services and applications | | | | | |
| Trusted supply chain | | | | | |
| Security-by-design | | | | | |
| From security components to security services | | | | | |
| | 110 | 130 | 140 | 380 | 100.0% |

# Priorités ECSO - commentaires

Une difficulté majeure: ECSO est (très) jeune…

… et l’aide de DG CNECT est très relative

1/. Liste de mots clés sans réelle vision d’ensemble

2/. « *Business as usual* »

3/. Difficulté majeure sur les verticaux (DGs mais aussi acteurs)

<u>Conseil pour les priorités</u>:

- sélection sur la base des enjeux (perspectives de marché, souveraineté et/ou autonomie),
- des forces/faiblesses du secteur européen,
- de la plus-value UE (collaboratif)
- des techno./appli. Génériques (mutualisation sur plusieurs verticaux)?

# Perspectives à venir

# Les priorités FR

Besoins (origine CoFIS)

- Malveillance (y compris menace intérieure) sur sites Seveso
- Contrôles à l'entrée (physique et cyber) physique et par cercles concentriques (*affordable*)
- Forensics (très) rapide (digital et physique)
- Protection physique contre nouvelles menaces (y compris armes de guerre)
- Systèmes et outils optimisés de réponse d'urgence
- Réseau de détection NR européen (y compris CONOPS)
- Protection de lieux accueillant du public

Topiques (origine GTN)…