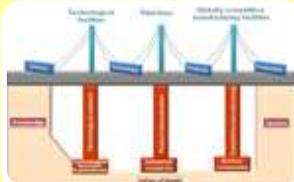


# **SOCIEDADES SEGURAS: PROTEGER LA LIBERTAD Y SEGURIDAD DE EUROPA Y SUS CIUDADANOS**

Dr. Marina Martínez García  
Programme Officer H2020  
Spanish Officer for Science and Technology, SOST-CDTI

$\approx 80.000 \text{ M}\text{\euro}$  (subvención)

## Programa Marco de Investigación e Innovación (2014-2020)



### Excellent Science

European Research Council (ERC)

Future and Emerging Technologies (FET)

Marie Skłodowska-Curie actions on skills, training and career development

European research infrastructures

### Industrial Leadership

ICT

Nanotechnology

Biotechnology

Advanced Materials

Advanced Manufacturing & Processing

Space

Access to Risk Finance

Innovation in SMEs

### Societal Challenges

Health, demographic change and wellbeing

Food security, sustainable agriculture and forestry, marine and maritime and inland water research and the bioeconomy;

Secure, clean and efficient energy;

Smart, green and integrated transport;

Climate action, environment, resource efficiency and raw materials

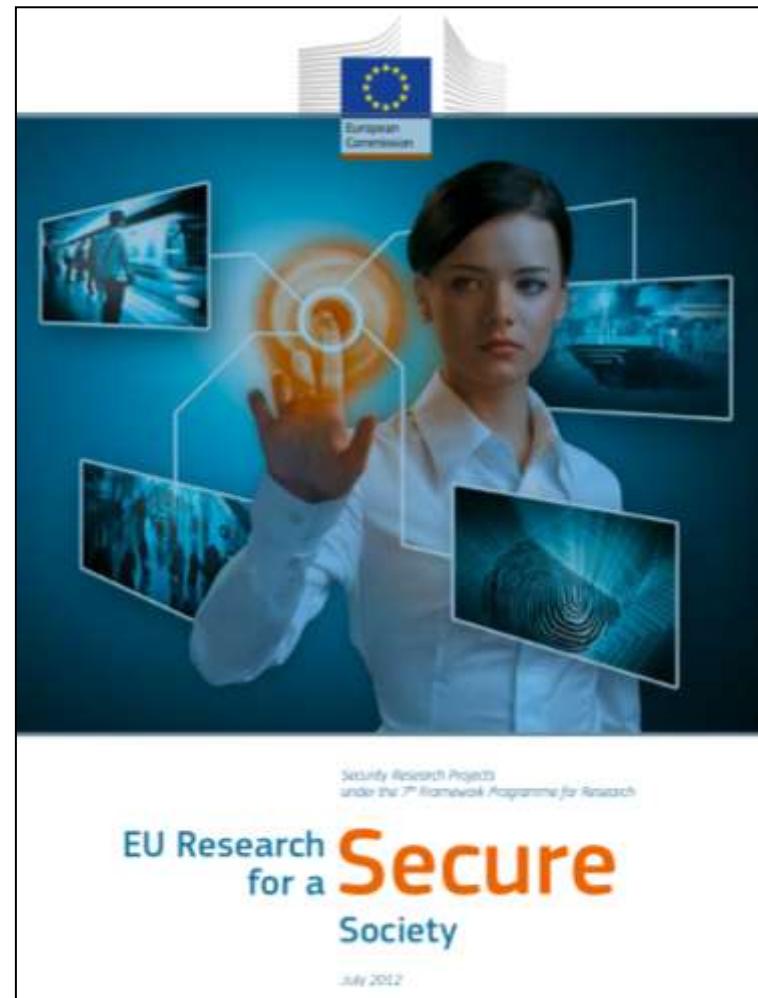
Europe in a changing world-Inclusive, innovative and reflective societies

Secure Societies: Protecting freedom and security of Europe and its citizens

$\sim 1.700 \text{ M}\text{\euro}$

# Objetivo del RS H2020 Sociedades Seguras

El objetivo de esta temática es **fomentar las sociedades europeas seguras** en un contexto de transformaciones sin precedentes y creciente **interdependencia y amenazas globales**, así como el **fortalecimiento de la cultura europea de la libertad y la justicia**.



# Principales áreas de actividad

- Luchar **contra la delincuencia, el tráfico y el terrorismo**, incluyendo la comprensión y la lucha contra las ideas y creencias de terrorismo.
- Proteger y mejorar la “*resiliencia*” de las **infraestructuras críticas, cadenas de suministro y los modos de transporte**.
- Fortalecer la seguridad a través de la **gestión de fronteras y la seguridad marítima**;
- Mejorar la **seguridad cibernética**.
- Aumentar la **recuperación de Europa frente a las crisis y los desastres**.
- Garantizar la **privacidad y la libertad**, incluyendo Internet y mejorar el entendimiento social, legal y ético de todos los ámbitos de la seguridad, riesgos y gestión.
- Mejorar la **estandarización y la interoperabilidad de los sistemas**, incluyendo los destinados a emergencias.

# La Investigación en Seguridad en H2020 vs FP7

- Mantiene su orientación a Misión
- Apoyo de políticas Europeas de seguridad interior y exterior
- Apoyo para que la industria Europea sea más competitiva
- Facilita la implicación de los usuarios finales
- Se refuerza la dimensión Social de la Seguridad
- Incluye nuevas áreas:
  - ✓ **Ciberseguridad**
  - ✓ Disaster-resilience & Climate change



# Particularidades del programa 1/3

- Respecto a **usuarios finales o “practitioners”**:
  - ✓ Es **OBLIGATORIO integrarlos en los proyectos...** Pero **se amplía el tipo de usuarios finales**: Fuerzas y Cuerpos de Seguridad, Administraciones Públicas, Empresas, pero también la sociedad en general, agencias de protección de datos, operadores de infraestructuras críticas, etc.
  - ✓ Acciones horizontales de apoyo a usuarios finales como redes de prueba/test/pilotos, y cooperación internacional.
- Destacar **los aspectos éticos y sociales**, así como las medidas o aspectos de **privacidad y protección de datos**. → Se observan más topics “sociales” en 2014-2015 que en 2016-2017. → **Incorporar partners especialistas!!!**
- Potenciales **aspectos sensibles de los proyectos** → Gestión de la información clasificada → **CONTACTAR ANS si necesario!!!!**
- A ser posible, la solución propuesta debe contemplar su **estandarización/certificación** → **Considerar AENOR, A+, DIN,...**

# Particularidades del programa 2/3

- Muchos topics **cercanos a mercado** (TRL 4 a 7, o incluso más) e incluso PCP/PPI (sólo para entidades con capacidad de licitación!!!!)
- Sinergias **civil/defensa**: coordinación, no cooperación
- Necesidad de coordinación con los programas de la **EDA y otros programas de DG-HOME (CIPS, ISEC, ISF) y en DG-RTD (ENV)**.
- Convergencia de la seguridad física y lógica en la protección de las infraestructuras críticas
- Acciones horizontales de apoyo a usuarios finales, redes de prueba/test/pilotos, y cooperación internacional
- Todos los topics son en 1-stage → Full proposals only!!! Resultados a los 5 meses del cierre (max) y firma del GA a los 8 meses del cierre (max).

**Fechas apertura / cierre diferentes al resto de programas:**  
**Opening 15-Mar-2016 → Deadline 25-Aug-2016**

# Particularidades del programa 3/3

Tipos de acciones:

- RIA
- Prizes

TRL 1 – basic principles observed  
TRL 2 – technology concept formulated  
TRL 3 – experimental proof of concept  
TRL 4 – technology validated in lab

- IA
- PCP / PPI
- FTI
- SMEs Instrument

TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)  
TRL 6 – technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)  
TRL 7 – system prototype demonstration in operational environment  
TRL 8 – system complete and qualified  
TRL 9 – actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

- CSA → Pueden ser redes de usuarios o de excelencia, organización de eventos y reuniones, estudios o estados del arte, actividades de policy, etc.... No research!

# Instrumentos de financiación en la call-2016

- ✓ Research and Innovation Action (RIA)
- ✓ Innovation Action (IA)
- ✓ Coordination and Support Action (CSA)
- ✓ SME Instrument
- ✗ Pre-Commercial Procurement Cofund (PCP) → Sólo para call-2017
- ✓ Fast Track to Innovation Pilot

# Research and Innovation Action (RIA)

- **Objetivo:** Establecer nuevo conocimiento o explorar la viabilidad de una tecnología nueva o mejorada de un proceso, producto, servicio o solución.
  - Puede incluir investigación fundamental o aplicada, desarrollo tecnológico e integración, testing y validación de un prototipo a pequeña escala en un laboratorio o entorno simulado.
- **Financiación:** Hasta el **100%** de los costes elegibles
- **Criterios de elegibilidad:** Tres entidades legales independientes, establecidas en 3 Estados Miembro o países asociados distintos.

# Innovation Action (IA)

- **Objetivo:** Producir planes y estructuras o diseños de nuevos productos, procesos o servicios modificados o mejorados
  - Puede incluir prototipos, testing, demostraciones, pilotos, validación de productos a gran escala y replicación de mercados.
- **Financiación:** Hasta el 70% de los costes elegibles (hasta el 100% para organizaciones sin ánimo de lucro)
- **Criterios de elegibilidad:** Tres entidades legales independientes, establecidas en 3 Estados Miembro o países asociados distintos.

# Coordination and Support Action (CSA)

- **Consiste en:** Medidas de acompañamiento tales como normalización, difusión, sensibilización y comunicación, creación de redes, servicios de coordinación o de apoyo, diálogos sobre políticas y ejercicios y estudios de aprendizaje mutuo, incluyendo estudios de diseño de nuevas infraestructuras y también puede incluir actividades complementarias de planificación estratégica, creación de redes y coordinación entre programas en diferentes países.
- **Financiación:** Hasta el 100% de los costes elegibles
- **Criterios de elegibilidad:** Una entidad legal establecida en un Estado Miembro o país asociado.

# Otras opciones de instrumentos de financiación...

## SMEs Instrument

- **Descripción:** El instrumento de las PYME está dirigido a todo tipo de PYME innovadoras que muestren una fuerte ambición de desarrollar, crecer e internacionalizarse. Proporciona apoyo que abarca todo el ciclo de la innovación en tres fases, complementados por un servicio de “mentoring” y “coaching”.
- **Financiación:** Hasta el **70%** de los costes elegibles
  - Fase-1 → Lump Sum de 50 k€ y duración 6 meses
  - Fase-2 → 0,5-2,5 M€ EC requested y duración hasta 2 años
  - Fase-3 Comercialización → No funding y sólo apoyo (mentoring, training, red EEN...)
- **Criterios de elegibilidad:** PYMEs con ánimo de lucro. Sólo se aceptarán solicitudes de PYMEs establecidas en Estados Miembro de la UE o asociados.

**NB:** *Múltiples fechas de cierre. Consultar el programa de trabajo.*

- Fighting crime**, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs
- Protecting and improving the **resilience of critical infrastructures**, supply chains and transport modes
- Strengthening security through **border management**
- Improving **cyber security**
- Increasing **Europe's resilience to crises and disasters**
- Ensuring **privacy and freedom**, including in the Internet, and enhancing the societal legal and ethical understanding of all areas of security, risk and management
- Enhancing **standardisation and interoperability of systems**, including for emergency purposes
- Supporting the Union's external security policies, including through conflict **prevention and peace-building**



## Otras opciones de instrumentos de financiación...

### Fast Track to Innovation (FTI)

- **Descripción:** Proyectos colaborativos pequeños (3-5 socios y unos ≈2 M€ EC requested) con idea de llevar a mercado una **solución innovadora y multidisciplinar en menos de 3 años**. No investigación, sino innovación, desarrollo, integración, validación y test a escala real, aproximación a mercado (usuario final). Importante peso empresarial.  
**Inicio TRL ≥ 6 → Final TRL = 9**
- **Financiación:** Hasta el **70%** de los costes elegibles (100% para entidades sin ánimo de lucro)
- **Criterios de elegibilidad:** Cualquier participante público o privado. Como mínimo 3 entidades establecidas en 3 Estados Miembros de la UE o asociados diferentes. Al menos 60% de presupuesto destinado a industria. Coordinador NO start-up (validación económica).

*NB: 3 fechas de cierre al año. Consultar el programa de trabajo.*

# Fast Track to Innovation Pilot

THE ULTIMATE BOOST FOR OUTSTANDING BUSINESS INNOVATORS WITH A NEED FOR SPEED...

## PREPARE YOUR PROPOSAL

Build your industry-intensive consortium\*  
minimum 3 partners - maximum 5 partners  
(all based in the EU and / or in Horizon 2020  
associated countries)

Proposal



Outstanding Business Innovation Concept  
(high-readiness level / TRL 6, meaning  
demonstrated in a relevant environment)

Continuous open call  
until end 2016

6 months time-to-grant

## DEVELOP YOUR INNOVATION

Receive an EU grant of EUR 1 million to 3 million  
(70% of funding, 100% of funding for non-profit entities)

From Mature R&D  
Demonstration  
Market-Oriented  
R&D  
to Market-Mature Innovation



## HIT THE MARKET!

Start your commercial activities



The Market  
Market-Maturity to Market  
Launch



Market-ready result  
(finished product, service,  
process/ TRL 9)

At most 36 months from grant to market

\*In a consortium with 3 or 4 partners, at least 2  
should be industry, and in a consortium with 5  
partners, at least 3; alternatively at least 60% of  
the project budget should be allocated to industry  
(i.e. private for profit entities)

... AND EAGER TO COMPETE ON GLOBAL MARKETS...!

## ACTIVITIES SUPPORTED

Systems validation in real working conditions – Testing – Piloting – Business model validation – Standard setting – Pre-normative research – EU quality label

# ¿Quién es quién en Sociedades Seguras?

Call	<u>Elaboración WP*</u>	Evaluación, Gestión & Seguimiento de proyectos
CIP	DG-Home	REA & DG-Home
DRS	DG-Home DG-RTD / ENV (Clima Change effects & impact)	REA & DG-Home
FCT	DG-Home EDA	REA & DG-Home
BES	DG-Home EDA DG-Cnect (BigData) DG-TAXUD	REA & DG-Home / DG-Cnect
DS	DG-Cnect	DG-Cnect
FTI Pilot SME Instrument	EASME - Unit A2	

\*Responsabilidad & influencia

# Alineación con las políticas UE...

Cualquier acción (proyecto) se debe alinear con las líneas generales de trabajo de la nueva Comisión Europea (JC Juncker) en cuanto a:

- A connected digital single market
- A stronger global actor
- Towards a new policy on migration
- An area of justice and fundamental rights based on mutual trust



# Qué destacamos en WP SEC 2016-2017?

# Call CIP - Critical Infrastructure Protection



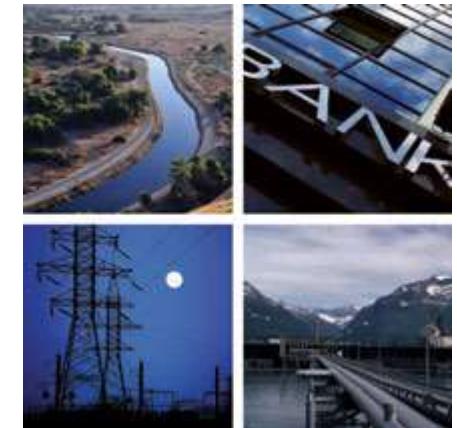
## **CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe**

### **Objective:**

- Providing security solutions to public & private operators facing hazards & cyber attacks. The solutions must include prevention, detection, response, and in case of failure, mitigation of consequences. →  
**Projects of about 8 M€ EC requested & TRL ≥ 7**
  
- It is expected than **3-4 projects approved per year!**  
(20M€ in 2016 and 20M€ in 2017).

### **Critical infrastructures eligible are:**

- Water Systems, Energy Infrastructure (power plants and distribution), Transport Infrastructure and means of transportation, Communication Infrastructure (including satellite communications), Health Services, Financial Services.



## Pay attention to:

- Advanced testing, piloting & demo activities “within” the installations is mandatory → **No project without minimum 2 CIs on-board & do not repeat in 2017 the CIs already chosen in 2016**
- Not infrastructures isolated but work on the interdependencies, i.e., communications & transport, ...
- Solutions proposed must be in convergence with safety and security standards.... If possible even to contribute to the pre-establishment of certification mechanisms.
- Mandatory at least 1 SMEs in the consortium**
- Design and perform communication & training activities for the affected population.

## References:

- Check the [EU Programme for Critical Infrastructure Protection at DG-Home](#)

# Call DRS – Disaster and Resilience



## **Objective:**

To reduce the loss of human life, environmental, economic and material damage from natural and man-made disasters, including from extreme weather events, crime and terrorism threats.

1-CSA to understand the needs of civil protection bodies in order to prepare a future PCP/PPI action → Consortium of Civil Protection Bodies.

- Only 1-Demo project (TRL 7-8) for a management and situational awareness addressed to decision-makers.
- Attention to neighbouring countries & societal acceptance (ethics).

SEC-01-DRS-2016: Integrated tools for response planning and scenario building ..... 12

SEC-02-DRS-2016: Situational awareness systems to support civil protection preparation and operational decision making ..... 14

SEC-03-DRS-2016: Validation of biological toxins measurements after an incident:

Development of tools and procedures for quality control ..... 16

SEC-04-DRS-2017: Broadband communication systems ..... 17

SEC-05-DRS-2016-2017: Chemical, biological, radiological and nuclear (CBRN) cluster

- In 2016 → 1-CSA for collecting (catalogue) the equipment and technical needs of First Responders based on EDEN project.
- In 2017 → Several RIAs for deploying solutions and new technologies according with the catalogue above.

Continuation of the topic DRS-18-2015 where the first responders will have to issue the conditions for the PCP concours.

1-Demo on bio-threats (IA) involving at least 3 control laboratories from different MS.

# Call FCT – Fight Against Crime and Terrorism



## **Objective:**

To mitigate potential consequences of incidents, or to avoid them by using new technologies and capabilities for fighting and preventing crime (including cyber-crime), illegal trafficking and terrorism (including cyber-terrorism).

It includes the understanding and tackling of terrorist ideas and beliefs, whilst respecting human rights and privacy.

- RIAs for developing new techniques / methodologies to be applied on the field as well in laboratory. → To be consistent with the work of forensic Labs at EU level.
- Take into account national legislations (solutions/techniques taking considering privacy-by-design).
- At least 5 Forensic laboratories or institutes .

- Social based topics that have to develop tools for the law enforcement bodies and decision-making bodies for better understanding, guidelines for action and policyming.
- At least 5 LEAs in the consortium!!!

→ SEC-06-FCT-2016: Developing a comprehensive approach to violent radicalization in the EU from early understanding to improving protection .....	21	}
→ SEC-07-FCT-2016-2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts.....	23	
→ SEC-08-FCT-2016: Forensics techniques on: a) trace qualification, and b) broadened use of DNA .....	25	
SEC-09-FCT-2017: Toolkits integrating tools and techniques for forensic laboratories .....	27	↗
SEC-10-FCT-2017: Integration of detection capabilities and data fusion with utility providers' networks .....	29	
SEC-11-FCT-2016: Detection techniques on explosives: Countering an explosive threat, across the timeline of a plot.....	30	
SEC-12-FCT-2016-2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism.....	31	

PCP for national authorities

SEC-06-FCT-2016: Developing a comprehensive approach to violent radicalization in the EU from early understanding to improving protection .....	21
SEC-07-FCT-2016-2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts .....	23
SEC-08-FCT-2016: Forensics techniques on: a) trace qualification, and b) broadened use of DNA	25
SEC-09-FCT-2017: Toolkits integrating tools and techniques for forensic laboratories.	27
SEC-10-FCT-2017: Integration of detection capabilities and data fusion with utility providers' networks	29
SEC-11-FCT-2016: Detection techniques on explosives: Countering an explosive threat, across the timeline of a plot.....	30
SEC-12-FCT-2016-2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism.....	31

List of different technology needs of LEAs at EU level → At least 3 to 5 practitioners or LEAs (TRL = 6)

Also detection of improvised and home-made explosives.

In line with the work of the EU Network of Detection of Explosives as well EDA previous projects!!!

At least 3 practitioners or LEAs

Platform deployment (TRL 7-8) equipped with sensors and technologies to work in the field. → Look at EDA previous projects!!!

Among 3 to 5 LEAs in the project & demo in at least 2 cities (medium & big).

# Call BES – Border Security & Eternal Security



# Objectives:

The development of technologies and capabilities to enhance systems, equipment, tools, processes, and methods for rapid identification in order to **improve border security**, whilst respecting human rights and privacy.

Those developments must reach the expectations of the European Border Surveillance System (**EUROSUR**) and to the **Smart Borders** legislative initiative.

The call also addresses supply chain security in the frame of the EU's **customs** policy as well the support to the **Union's external security policies in civilian tasks** (civil protection, humanitarian actions, border management, peace-keeping, peace-building & mediation, post-crisis stabilisation and conflict prevention).

SEC-13-BES-2017:	Next generation of information systems to support EU external policies	
	33	
SEC-14-BES-2016:	Towards reducing the cost of technologies in land border security applications	
	35	
SEC-15-BES-2017:	Risk-based screening at border crossing .....	37
SEC-16-BES-2017:	Through-foliage detection, including in the outermost regions of the EU	
	38	
<ul style="list-style-type: none"> <li><input type="checkbox"/> RIA (TRL = 5-6) considering forest scenarios such as Turkey, Ukraine, Belarus, Russia...</li> <li><input type="checkbox"/> Coordination with EWISA previous project and EDA programmes</li> <li><input type="checkbox"/> At least 3 border authorities</li> </ul>		
<ul style="list-style-type: none"> <li><input type="checkbox"/> RIA and IA envisioning surveillance and monitoring solutions at land crossing points and gates focussing on people (TRL = 6). → Attention to ethical &amp; privacy issues.</li> <li><input type="checkbox"/> Coordination with EWISA previous project and EDA programmes</li> <li><input type="checkbox"/> Solutions or technologies according to, i.e., IATA rules</li> <li><input type="checkbox"/> At least 3 border authorities</li> </ul>		
<p>PCP continuation of the CSA BES-11-2015 where the national bodies (at least 3) are the funding organisations of the future concourse of technology solutions.</p>		

SEC-17-BES-2017:	Architectures and organizations, big data and data analytics for customs risk management of the international goods supply chain trade movements.....	40
SEC-18-BES-2017:	Acceptance of "no gate crossing point solutions" .....	41
SEC-19-BES-2016:	Data fusion for maritime security applications .....	42
SEC-20-BES-2016:	Border Security: autonomous systems and control systems .....	45

- CISE complatible solution above TRL 7
- At least 5 border authorities
- SMEs participation mandatory

- CISE complatible solution above TRL 7
- Coordination con previous EDA projects
- At least 3 border authorities & 3 indutry or technology providers

- Futuristic advanced solution for seamless crossing of borders and security checks of people.
- Close cooperation with the wining projects from topic BES-15 will be required during the life of the project.
- At least 3 border authorities

- RIA in advance cargo information systems for customs.
- At least 3 border or customs authoritites

# Call DS – Digital Security



Topic Title	Type	
<b>Secure Societies WP</b>		
Open = 24-Mar-2016 Close = 25-Aug-2016	<b>DS-02-2016:</b> Cyber Security for SMEs, local public administration and Individuals <b>DS-04-2016:</b> Economics of Cybersecurity <b>DS-05-2016:</b> EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation <b>DS-07-2017:</b> Addressing Advanced Cyber Security Threats and Threat Actors <b>DS-08-2017:</b> Privacy, Data Protection, Digital Identities	IA RIA CSA RIA IA IA
<b>LEIT-ICT WP</b>		
Open = 16-Dec-2015 Close = 12-Apr-2016	<b>DS-01-2016:</b> Assurance and Certification for Trustworthy and Secure ICT systems, services and components <b>DS-06-2017:</b> Cryptography Cryptography Prize	RIA IA CSA RIA PRIZE
<b>Health WP</b>		
Open = 30-Sep-2015 Close = 16-Feb-2016	<b>DS-03-2016:</b> Increasing digital security of health related data on a systemic level	RIA

DS-01-2016: Assurance and Certification for Trustworthy and Secure ICT systems, services and components .....	58
→ DS-02-2016: Cyber Security for SMEs, local public administration and Individuals .....	61
DS-03-2016: Increasing digital security of health related data on a systemic level.....	63
→ DS-04-2016: Economics of Cybersecurity.....	64
→ DS-05-2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation .....	65
DS-06-2017: Cryptography .....	68
DS-07-2017: Addressing Advanced Cyber Security Threats and Threat Actors .....	70
DS-08-2017: Privacy, Data Protection, Digital Identities .....	71

### 3 CSA on:

- Collaboration / synergies among EU cyber-security clusters (5 years of activitites) → 4 years and 2 M€
  - Collaboration lines with Japan → 0,5 M€
  - Collaboration lines with USA → 0,5M€
- 
- Analysis of societal, institutional & economical impact of cyber failures → Recommediations for regulators, law enforcement bodies, market operators / insurances.
  - 2-3 RIAs of 1-2 M€.
- 
- Cost-effective solutions (TRL = 5-7) addressed to this 3 kinds of end-users.
  - 4-5 Ias of 3-4 M€ EC requested.

DS-01-2016: Assurance and Certification for Trustworthy and Secure ICT systems, services and components .....	58
DS-02-2016: Cyber Security for SMEs, local public administration and Individuals ....	61
DS-03-2016: Increasing digital security of health related data on a systemic level.....	63
DS-04-2016: Economics of Cybersecurity.....	64
DS-05-2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation .....	65
DS-06-2017: Cryptography .....	68
<b>DS-07-2017: Addressing Advanced Cyber Security Threats and Threat Actors .....</b>	<b>70</b>
<b>DS-08-2017: Privacy, Data Protection, Digital Identities .....</b>	<b>71</b>

Innovation actions on:

- PET (Privacy Enhancing Technologies);
- eID (Secure Digital Identities);
- General Data Protection Regulation in practice.

This action would include:

- R&I actions on situational awareness in EU in front of cyber-attacks;
- Innovation actions on training and simulating environments to face cyber-attacks.

The IAs proposed would propose Novel designs, methods and tools to provide to the users of examples of services/activities in the network to enhance / ensure:

- a. **Or well** the control of their data (PET, Privacy Enhancing Technologies)
- b. **Or well** the General Data Protection Regulation → Oriented to assist organisations (businesses, service providers, and government agencies)
- c. **Or well** the Secure use of the Digital Identity (eID, Secure Digital Identities) → For private as well for public users

- Take care of societal & Ethical issues
- Projects of **2-3 M€ contribution and TRL = 6-7** → **Between 6-9 proposals approved in 2017!!!!**
- Topic from DS-Connect → **RAFAEL TESORO (infoday nacional)**

# General Matters: Networks of practitioners...

It is expected to fund 4 types of networks:

2016  
Duration of 6 years

- a.- Practitioners (end-users) in the same discipline and from across Europe, i.e., firefighters; police and intelligence bodies; border guards, coast guards, and custom authorities; explosive specialists; forensic laboratories; medical emergency teams; think-tanks on security; etc.**
- b.- Practitioners (end-users) from different disciplines for disaster risk and crisis management issues in a particular geographical area → Med, Artic, Danube, Baltic.**
- c.- Entities from around Europe that manage demonstration and testing sites, training facilities**
- d.- Security NCPs network continuation onwards 2017 and duration of 3 years.**

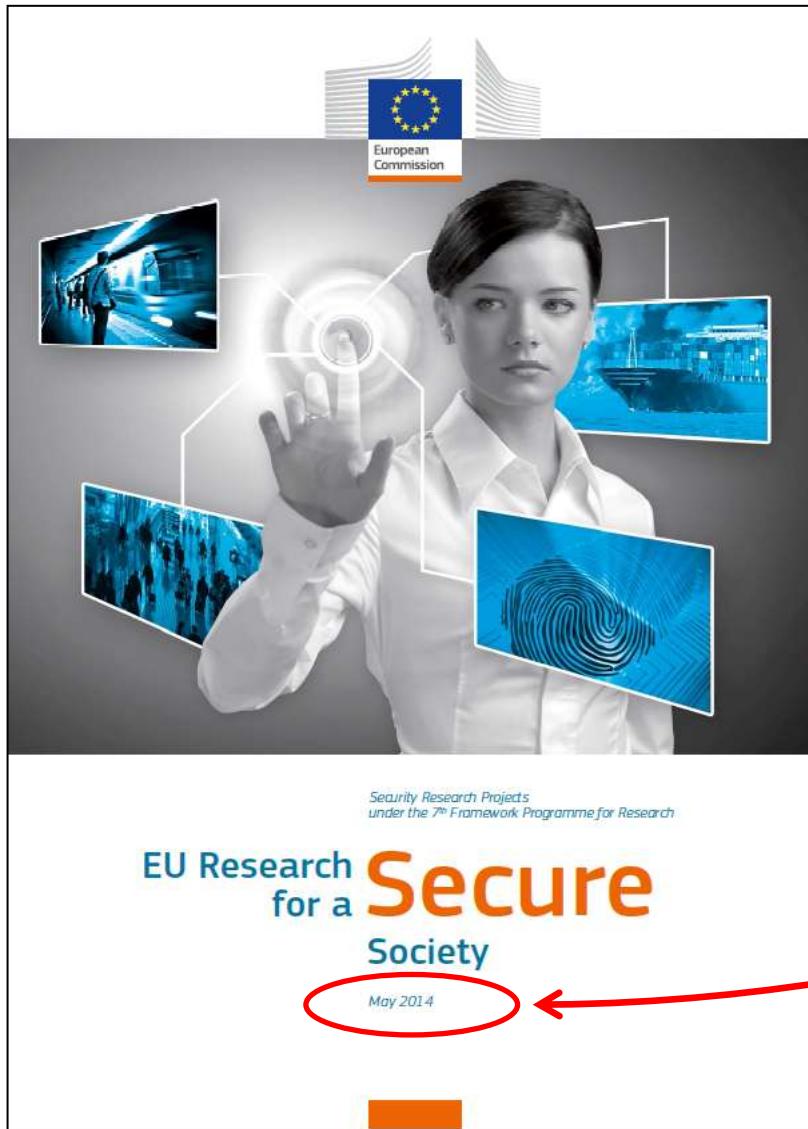
# Last but not least...

# Enlaces de interés y otra información

## Fuentes de información

<b>Programa de Trabajo 2016-2017</b>	<a href="https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/14.%20Secure%20societies_2016-2017_pre-publication.pdf">https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/14.%20Secure%20societies_2016-2017_pre-publication.pdf</a>
<b>Web EC H2020</b>	<a href="http://ec.europa.eu/research/horizon2020/index_en.cfm#">http://ec.europa.eu/research/horizon2020/index_en.cfm#</a>
<b>Web Horizonte 2020 Español</b>	<a href="http://eshorizonte2020.es/">http://eshorizonte2020.es/</a>
<b>IPR &amp; Open Access</b>	<a href="http://ec.europa.eu/research/science-society/index.cfm?fuseaction=public.topic&amp;id=1301">http://ec.europa.eu/research/science-society/index.cfm?fuseaction=public.topic&amp;id=1301</a>
<b>Ethical issues</b>	<a href="http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm">http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm</a>
<b>Búsqueda en Socios en H2020 en Sociedades Seguras (red Puntos Contacto SEREN3)</b>	<a href="http://www.security-research-map.eu/index.php?file=search.php&amp;type=1">http://www.security-research-map.eu/index.php?file=search.php&amp;type=1</a>

# Catálogo de proyectos FP7 Security Research



## Catálogo de proyectos FP7 SEC

**EU Research for a Secure Society (FP7 Security Projects)**

[http://ec.europa.eu/dgs/home-affairs/financing/funding/pdf/research-for-security/security\\_research\\_catalogue\\_2014\\_en.pdf](http://ec.europa.eu/dgs/home-affairs/financing/funding/pdf/research-for-security/security_research_catalogue_2014_en.pdf)

Last update May-2014!

# Participación como experto

<http://ec.europa.eu/research/participants/portal/desktop/en/experts/index.html>

The screenshot shows the European Commission Research & Innovation Participant Portal. The top navigation bar includes links for HOME, FUNDING OPPORTUNITIES, HOW TO PARTICIPATE, EXPERTS (which is the active tab), SUPPORT, and a search bar. There are also LOGIN and REGISTER buttons. The main content area has a blue header "RESEARCH & INNOVATION" and "Participant Portal". On the left, there's a "News" box about the H2020 call for expression of interest for experts. Below it are "Quick Links" for experts and logistics to Brussels. In the center, there's a graphic of a brain and a section titled "Experts" with a sub-section "New experts". To the right, there's a box for "H2020 ONLINE MANUAL" and another section titled "Who can be an expert?" with a list of requirements. A large red arrow points from the text "Diferentes perfiles!" in the previous slide to this section. Another red arrow points from the "Who can be an expert?" list to the "What do expert assignments involve?" section, which is circled in red. This section lists various roles like peer reviewers and details about proposal evaluation, monitoring, and programme implementation. At the bottom, there's a "REGISTER AS EXPERT" button and a "Take a look at the most recently funded projects." link.

Diferentes perfiles!

Científico-técnicos,  
business, end-users,  
practitioners,...

RESEARCH & INNOVATION  
Participant Portal

European Commission > Research & Innovation > Participant Portal > Experts

HOME FUNDING OPPORTUNITIES HOW TO PARTICIPATE EXPERTS SUPPORT Search PP LOGIN REGISTER

News

H2020 call for expression of interest for experts (11/2013) New calls for expression of interest for individual experts and for organisations to suggest experts were just published in OJ C342 of 22 November 2013. European Commission will soon need experts to evaluate first Horizon 2020 proposals. Don't forget to tick the H2020 box in the registration platform and update your expertise.

New experts

Who can be an expert?

You have a chance of being selected as an expert if you:

- have high-level of expertise in the relevant fields of research and innovation (see call for details on types of expertise).
- can be available for occasional, short-term assignments.

REGISTER AS EXPERT

What do expert assignments involve?

Experts, as peer reviewers, assist in the:

- evaluation of proposals
- monitoring of actions

In addition, experts assist in the :

- preparation, implementation or evaluation of programmes and design of policies. This includes the Horizon 2020 Advisory Groups.

Assignments mainly concern research and innovation, falling within the Horizon 2020 programme designed to address the challenges Europe is facing through funding excellent science, technology and innovation.

Take a look at the most recently funded projects.

Quick Links

- FAQ for Experts
- Expert recommendations
- Guidance on the evaluation of innovation, social sciences and humanities and other aspects of H2020 proposals

Logistics for Brussels

- Map of evaluation area
- Info on hotels
- Metro map
- From airport to Brussels

In order to access the expert registration form, you are first asked to login with a valid Participant Portal (ECAS) account. If you do not have it yet, it's easy to [create your Portal \(ECAS\) account](#).

Registered experts

- Registered experts can complete or update their profile at any time by [logging-in](#) to their Portal account (ECAS) and accessing My Expert Area.
- Your profile is only available to the Commission for consideration once it is complete and valid.

# Otras Guías y Documentos útiles

- **Participant Portal H2020 Online Manual**

[http://ec.europa.eu/research/participants/docs/h2020-funding-guide/index\\_en.htm](http://ec.europa.eu/research/participants/docs/h2020-funding-guide/index_en.htm)

- **Self-Evaluation Forms**

[http://ec.europa.eu/research/participants/data/support/sep\\_usermanual.pdf](http://ec.europa.eu/research/participants/data/support/sep_usermanual.pdf)

- **Guidance for evaluators of Horizon 2020 proposals**

[http://ec.europa.eu/research/participants/data/ref/h2020/grants\\_manual/pse/h2020-evaluation-faq\\_en.pdf](http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/pse/h2020-evaluation-faq_en.pdf)

- **Proposal Submission Service User Manual**

[http://ec.europa.eu/research/participants/data/support/sep\\_usermanual.pdf](http://ec.europa.eu/research/participants/data/support/sep_usermanual.pdf)

# Próximos eventos destacados...

- Networking event **CIP-01-2016-2017** “Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe” → **08-Mar-2016 Bilbao**  
<http://eshorizonte2020.cdti.es/index.asp?MP=87&MS=721&MN=2&TR=A&IDR=16&IDP=682&IDS=4&id=3446&xtmc=&xtcr=1>
- **Community of Users** meeting (CoU meeting) on **CBRN-related topics** → **29-Feb-2016 Brussels**
- **EU Infoday** call-2016 → **05-06 Apr-2016 Brussels**
- **Security Research Conference** → **01-02 Jun-2016 Den Hague**

# Eventos de interés pasados...

## ICT 2015 Innovate, Connect, Transform

Article

Newsroom

The biggest ICT event in the EU calendar is back! Join us during ICT 2015 to network, follow interesting debates in the conference, hear the latest news on the European Commission's new policies and initiatives with regard to R&I in ICT, find information about funding opportunities and much more!

The European Commission, together with the [Fundação para a Ciência e a Tecnologia](#) bring you: **ICT 2015 - Innovate, Connect, Transform**, on 20-22 October 2015 in Lisbon, Portugal.

The ICT 2015 event will comprise a number of parallel activities:

- A policy [conference](#) presenting the new Commission's policies and initiatives on Research & Innovation in ICT ([Horizon 2020](#) Programme);
- An interactive [exhibition](#) showcasing the best results and impact of most recent EU ICT Research & Innovation;
- Many [networking](#) opportunities to enhance quality partnerships, help participants find partners, connect Research and Innovation and trigger collaboration;
- Funding opportunities: ICT 2015 will also be the place to gather information on the 2016-17 Work Programme of [Horizon 2020](#).



SHARE THIS

[Register for ICT 2015](#)

You may also find opportunities for cyber applications at:

- SC-1 under the eHealth & security for data protection
- LEIT-ICT (8.1, 8.2 & 8.3)

- SMIGs-2016 Networking event → BRU 26-27 JAN 2016**



Home National Research Maps Logos Contact

Login

R&D profiles

Insert

Update

Search

Show all

Projects Ideas

Show All

Organisations

Austria 2

Belgium 61

Bulgaria 1

Croatia 5

Cyprus 4

Czech Republic 5

Estonia 7

Finland 16

France 22

Germany 11

Greece 14

Ireland 10

Iceland 1

Israel 4

Italy 55

Lithuania 4

Latvia

## Security Research Database

The purpose of the Security Research Map (SeReMa) is to increase the visibility of security related research in Europe and to optimize the networking between research facilities, universities, public authorities, end users, suppliers of security solutions and operators of critical infrastructures.

The database has been developed within the network of National Contact Points for Security in the 7th EU-Framework Programme (SEREN 2).

### Why register?

- Call the attention of the network about your competencies
- Promote your research ideas
- Find partners for security research projects

### Your advantages:

- Stay informed on upcoming Horizon 2020 Calls
- Meet a lot of potential co-operation partners through this Website and database
- Your profile will be promoted all over Europe

### Insert profile

If you are a researcher who is actively involved in security research and interested in international cooperation, register yourself and help building a map of security research all over the world

### Search database

Identify researchers who work in the area of security research, either within the context of



## Support & Finance



South Africa





• Inicio / Retos sociales / Sociedades seguras

- Salud, cambio demográfico y bienestar
- Seguridad alimentaria, agricultura y silvicultura sostenibles, investigación marina, marítima y de aguas interiores y bioeconomía
- Energía segura, limpia y eficiente
- Transporte inteligente, ecológico e integrado

La temática de Sociedades Seguras de Horizonte 2020 se enmarca en el pilar de "Retos Sociales" y cuenta con un presupuesto estimado de 1.695 M€ para el período 2014-2020. Está gestionada por la Dirección General de Empresa e Industria de la Comisión Europea.

El **objetivo** es fomentar las sociedades Europeas seguras en un contexto de transformaciones sin precedentes y creciente interdependencia y amenazas globales, así como el fortalecimiento de la cultura europea de la libertad y la justicia.

Se perseguirán los siguientes objetivos específicos:

- Luchar contra la delincuencia, el tráfico y el terrorismo ilegal, incluyendo la comprensión y la lucha contra las ideas y creencias de terrorismo

## SERVICIOS

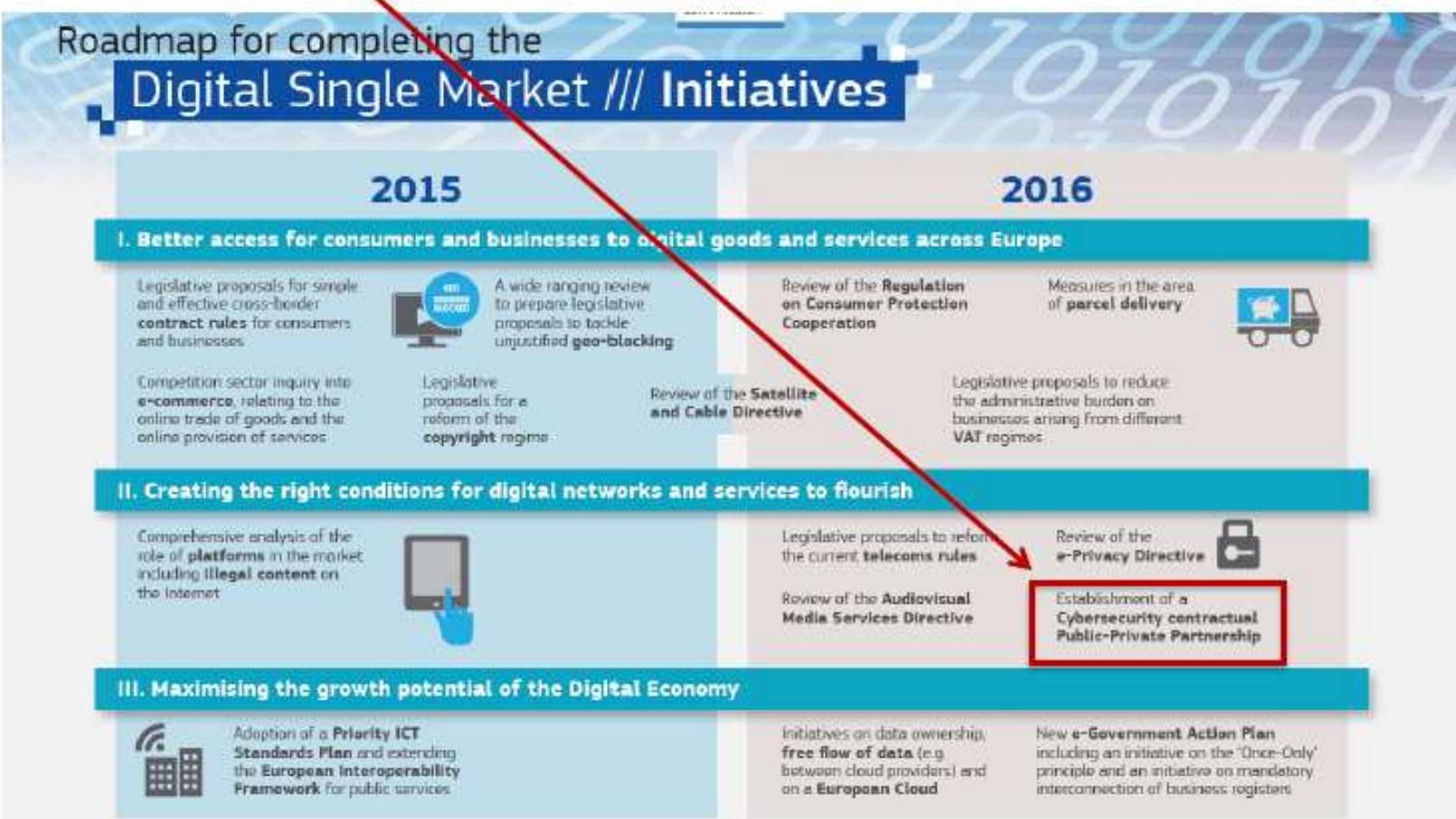
- Contacto / Buzón
- Listas de distribución
- Enlaces de interés
- Eventos
- Noticias
- Documentación relacionada
- Convocatorias
- Listado de correos informativos
- Ayudas Preparación de Propuestas (APC)
- Inicio

- Representante → Maite Boyero, CDTI ([mtbe@cdti.es](mailto:mtbe@cdti.es))  
 NCPs → Ainara Ripa Centeno, INTA ([ripaca@inta.es](mailto:ripaca@inta.es))  
 Bruselas → Marina Martínez, CDTI-SOST ([marina.cdti@sost.be](mailto:marina.cdti@sost.be))

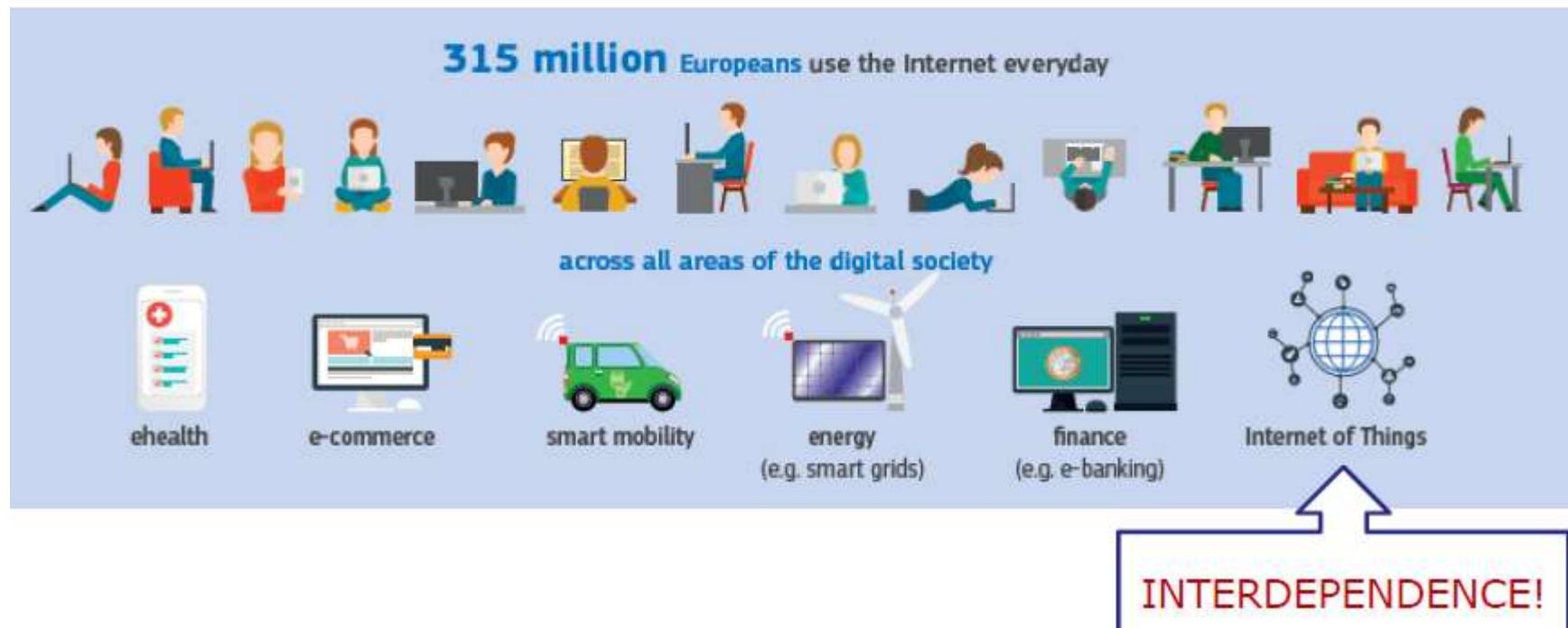


# Few words on the next coming cPPP\_Cyber...

# cPPP – an initiative under Digital Single Market Strategy



# Cyberspace: a backbone of digital society & economic growth



**Cybersecurity incidents are increasing at an alarming pace with potentially profound effect on daily functioning of society & economy, both online and offline**

### **Cybersecurity incidents may**

**disrupt the supply of essential services** such as



water, healthcare, electricity or mobile services

**Undermine trust in digital services & products**

only 22% of Europeans



have **full trust** in companies such as **search engines, social networking sites & e-mail services**

Only 38% of Europeans feel

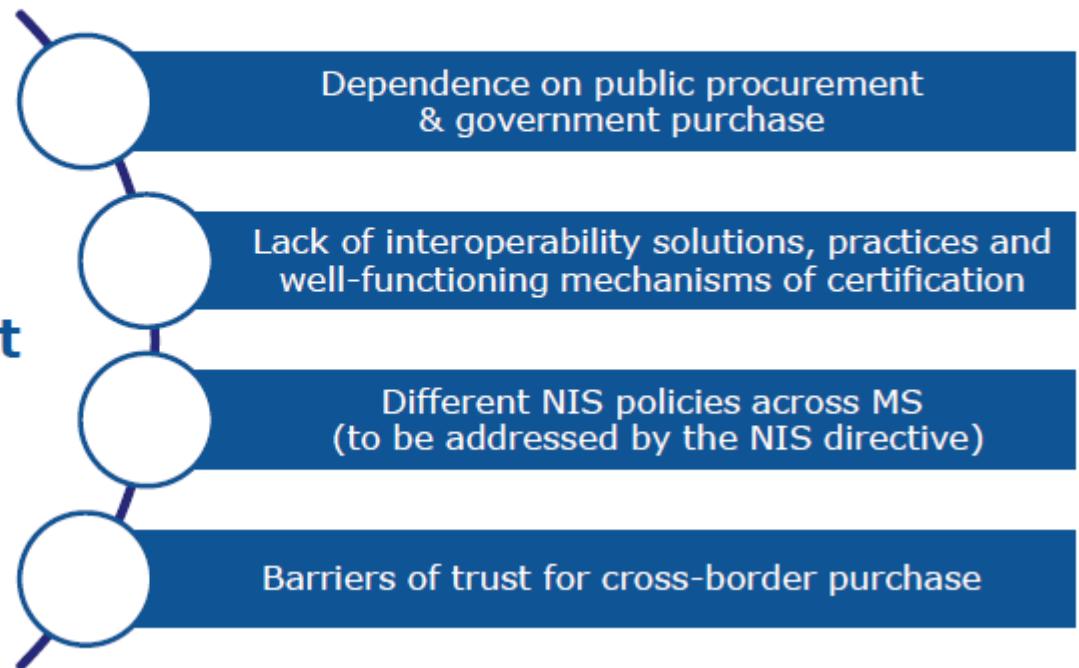


**confident about online purchasing from another EU Member State**

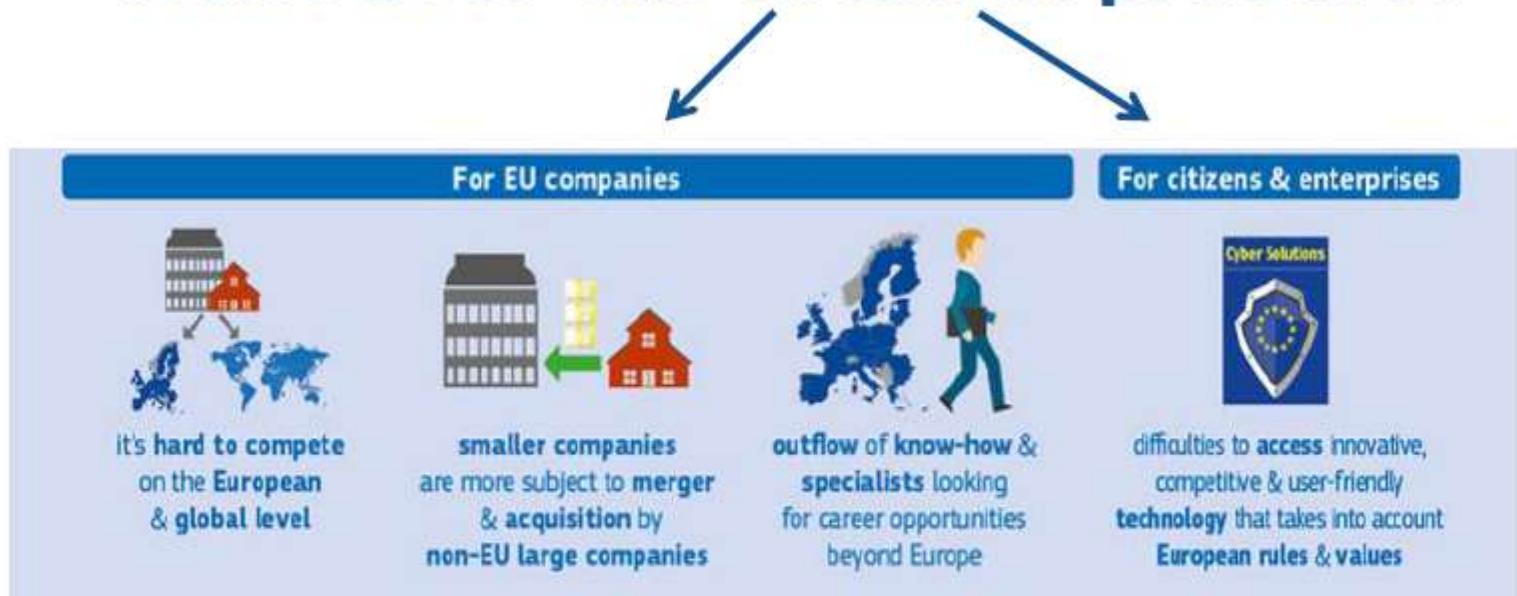
**...as well as financial theft, loss of intellectual property, data breaches, etc.**

# Cyberspace is borderless by nature...

**unlike  
heavily  
fragmented  
European market  
for ICT security  
products &  
services due to:**



# What does this mean in practice?

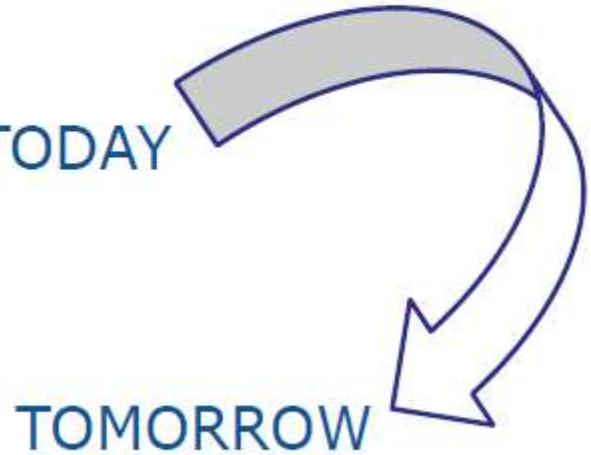


The survival of strong European cybersecurity industry all together is at stake!

# Cybersecurity is also an opportunity!



TODAY



TOMORROW

The **global cyber security market** is expected to be among the **fastest growing** segments of the ICT sector in the coming decade. It is expected to **grow to \$80-120 billion** by 2018.

# Cybersecurity contractual Public-Private Partnership (cPPP)



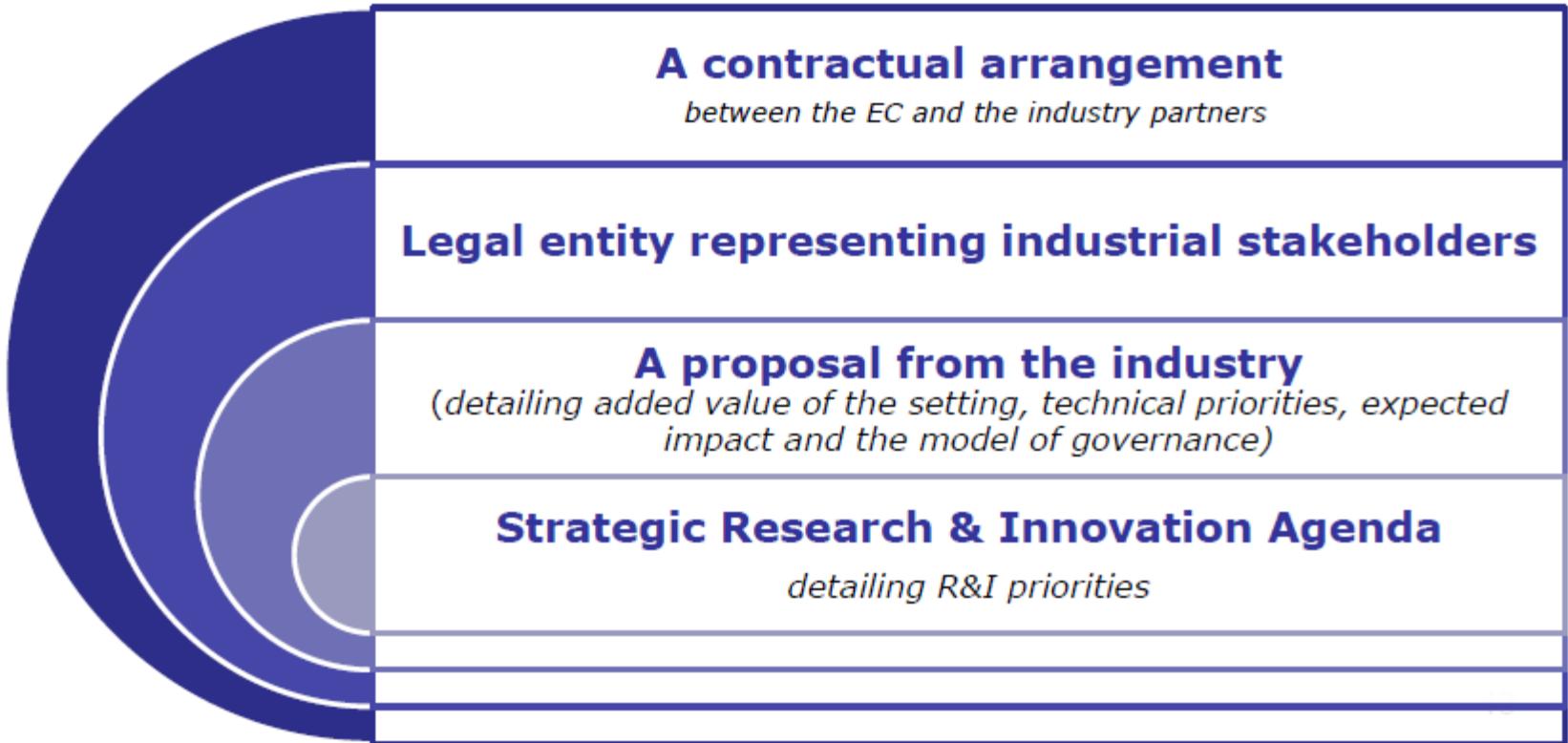
- Stimulate the competitiveness and innovation capacities of the digital security and privacy industry in Europe
- Ensure a sustained supply of innovative cybersecurity products and services in Europe

# Intended Objectives of the cPPP

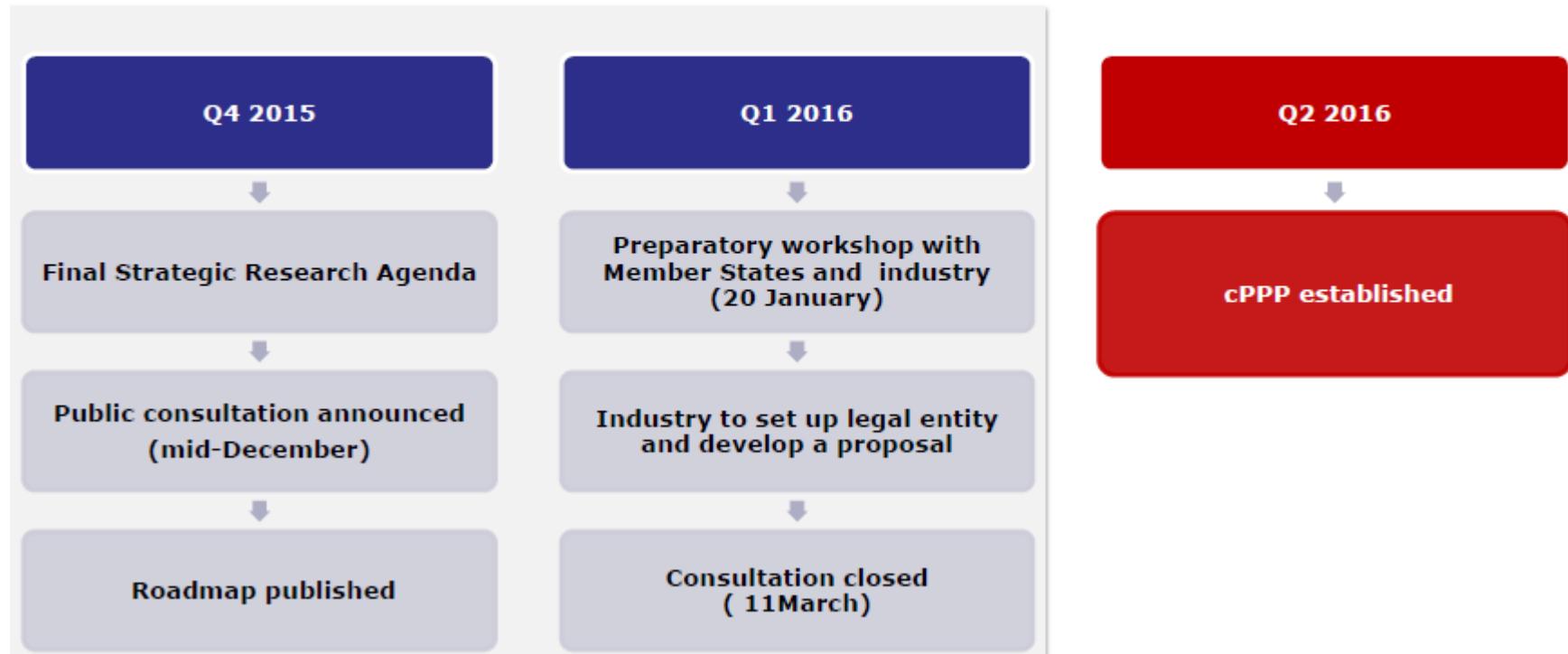
- Gather industrial and public resources to deliver innovation against a jointly-agreed strategic research and innovation roadmap.
- Maximize available funds through better coordination with MS.
- Focus on a few technical priorities defined jointly with industry.
- Seek synergies to develop common, sector-neutral technological building blocks with maximum replication potential
- Obtain economies of scale through engagement with users/demand side industries and bringing together a critical mass of innovation capacities.
- Be a platform to discuss other supporting measures for the industry

11

# H2020 requirements for cPPP



# Working against tight timeline!



# Gracias por su atención...

[marina.cdti@sost.be](mailto:marina.cdti@sost.be)