

**XIII
JORNADAS
STIC
CCN-CERT**



**Prioridades de la
política europea de
ciberseguridad**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



Miguel González-Sancho

Jefe de la Unidad

**“Cybersecurity Technology and Capacity Building”
DG CONNECT – COMISION EUROPEA**

miguel.gonzalez-sancho@ec.europa.eu

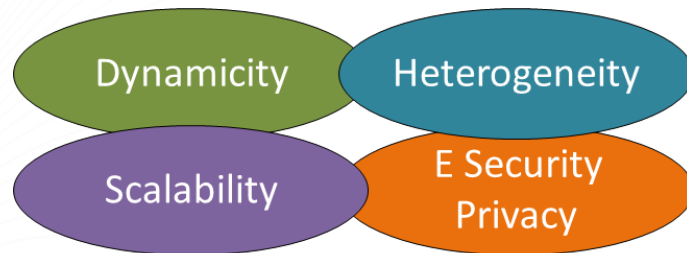
Contenidos

- Amenazas de ciberseguridad y respuesta europea
- Legislación europea:
 - ✓ Directiva “NIS” (>”Operators of Essential Services”)
 - ✓ Reglamento “Cybersecurity Act”: ENISA; Certificación)
- Orientaciones políticas (recomendaciones Comisión, conclusiones Consejo UE)
 - ✓ Respuesta coordinada a amenazas mayores (“Blueprint”)
 - ✓ Seguridad de redes 5G
- Financiación europea:
 - ✓ Programa de investigación y desarrollo “Horizonte 2020” (H2020)
 - ✓ Programa de capacitación “Connecting Europe Facility”(CEF); otros programas
 - ✓ Futuros programas: Horizonte Europa; Europa Digital (DEP)
 - ✓ Centro y red de competencias ciber

Evolución de la ciber-amenaza y de la respuesta

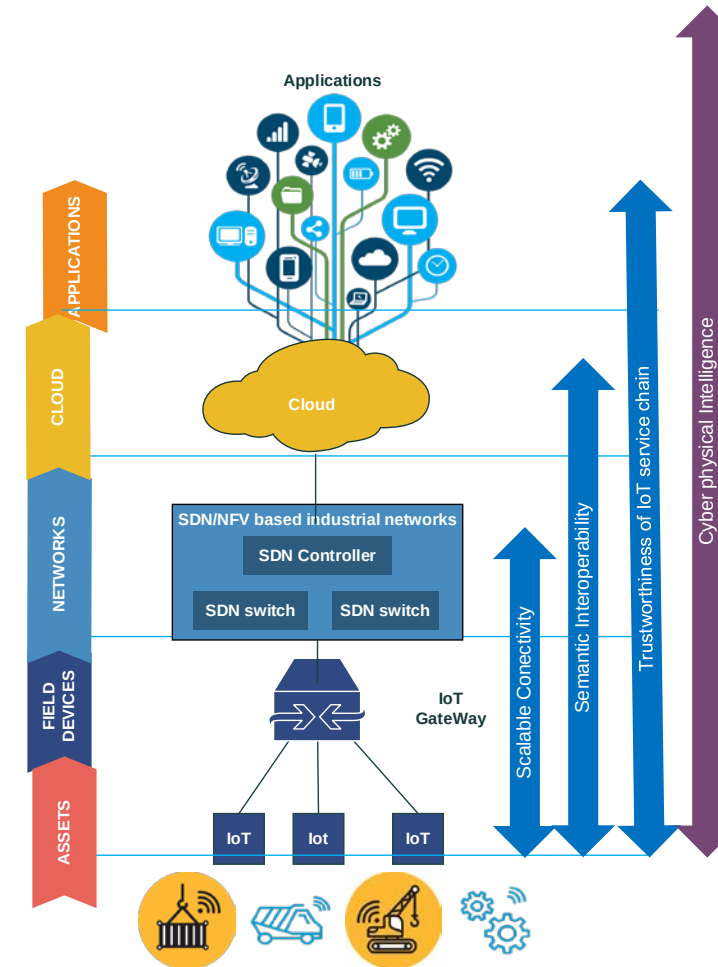
➤ Open hyperconnected world

- IoT
- 5G
- Cloud computing
- Applications



➤ Adversaries are:

- taking advantage at Gaps in Security
- moving faster
- better coordinated
- easily penetrating traditional perimeter defenses
- developing intelligence



Evolución y objetivos de la coordinación europea

Continuous policy response to the evolving threat landscape:

- **2013** EU Cybersecurity Strategy: 'An Open, Safe and Secure Cyberspace'
- **2016** Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry
- **2017** Cybersecurity package
- **2018** Proposal for the European competence centre and network
- **2019** Cybersecurity Act entered into force

Building EU Resilience to cyber attacks

Capacity Building

Enhanced national capabilities & Risk management requirements

Financial Support from the EU

Industrial capabilities

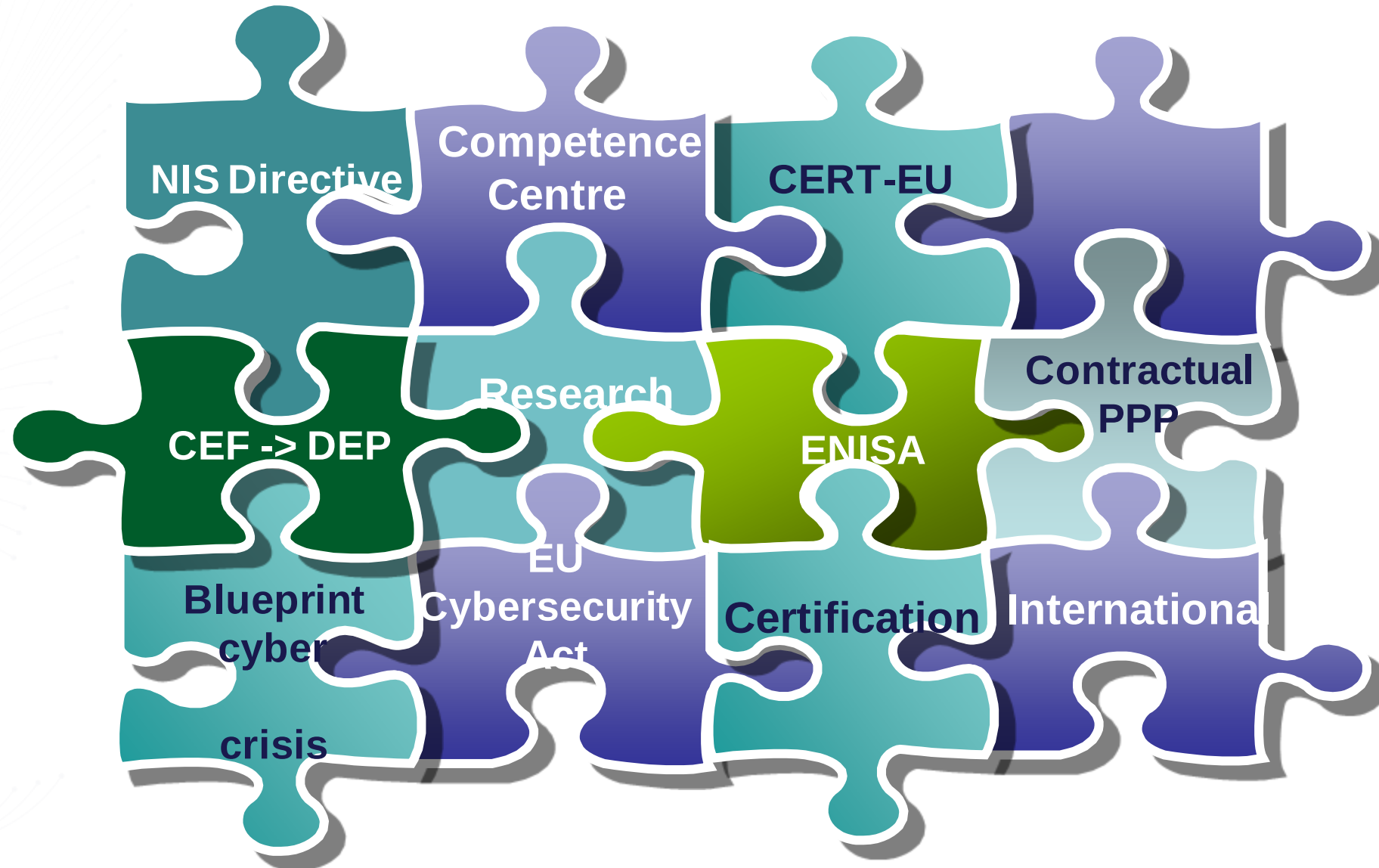
Prevention & Response Coordination

ENISA operational support & Cooperation between national CSIRTs

Coordinated response to large-scale cybersecurity incidents and crises & exercises

Single Market for certified ICT products and services

Instrumentos de la acción UE en ciberseguridad: legislación, coordinación, financiación...



Nueva Comisión Europea



- **Extract of political guidelines of U von der Layen (priority 3: “A Europe fit for the digital age”):** *“it is not too late to achieve technological sovereignty in some critical technology areas... Digitalisation and cyber are two sides of the same coin”.*
- **Extract of mission letter of Commissioner Bretton:** *“...enhancing Europe’s technological sovereignty. ... building a real single market for cybersecurity, notably looking at certification, implementing rules on security of network and information systems, rapid emergency response strategies and other relevant areas. You should lead the work to build a joint Cyber Unit to better protect ourselves.*

NIS Directive: Main Features



GREATER CAPABILITIES

Member States have to improve their cybersecurity capabilities.

NATIONAL COMPUTER SECURITY
INCIDENT RESPONSE TEAM (CSIS-
RT)

NATIONAL NIS STRATEGY

NATIONAL NIS AUTHORITY



COOPERATION

Increased EU-level cooperation

EU MEMBER STATES
COOPERATION GROUP
(STRATEGIC)

EMERGENCY TEAMS
(CSIRTS) NETWORK
(OPERATIONAL)



EU MEMBER STATES; EUROPEAN COMMISSION;
EUROPEAN UNION AGENCY FOR NETWORK AND
INFORMATION SECURITY



EU MEMBER STATES; CERT-EU; EUROPEAN
UNION AGENCY FOR NETWORK AND
INFORMATION SECURITY



RISK MANAGEMENT

Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.

SECURITY MEASURES

NOTIFICATION OF
MAJOR INCIDENTS

Cybersecurity Act

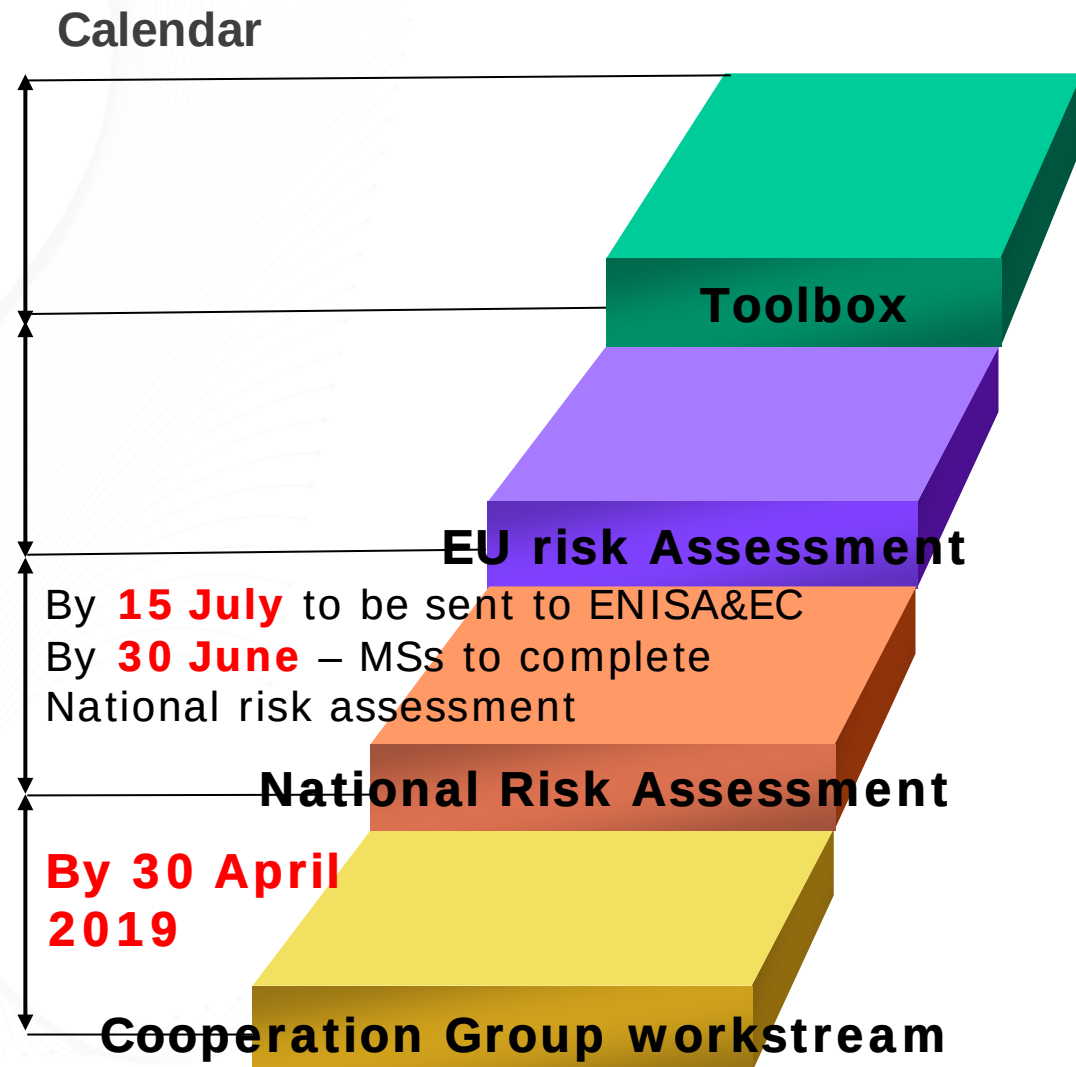
REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

- ENISA, what's new:
 - ✓ Permanent status
 - ✓ Stronger resources
 - ✓ Renewed mandate including operational tasks (certification, NIS Directive, CSIRTs support...)
- A voluntary European cybersecurity certification framework to enable the creation of tailored EU cybersecurity certification schemes for ICT products, services and processes that are valid across the EU.

Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises



Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks C(2019) 2335 final



Conclusions from EU coordinated risk assessment of the cybersecurity of 5G networks

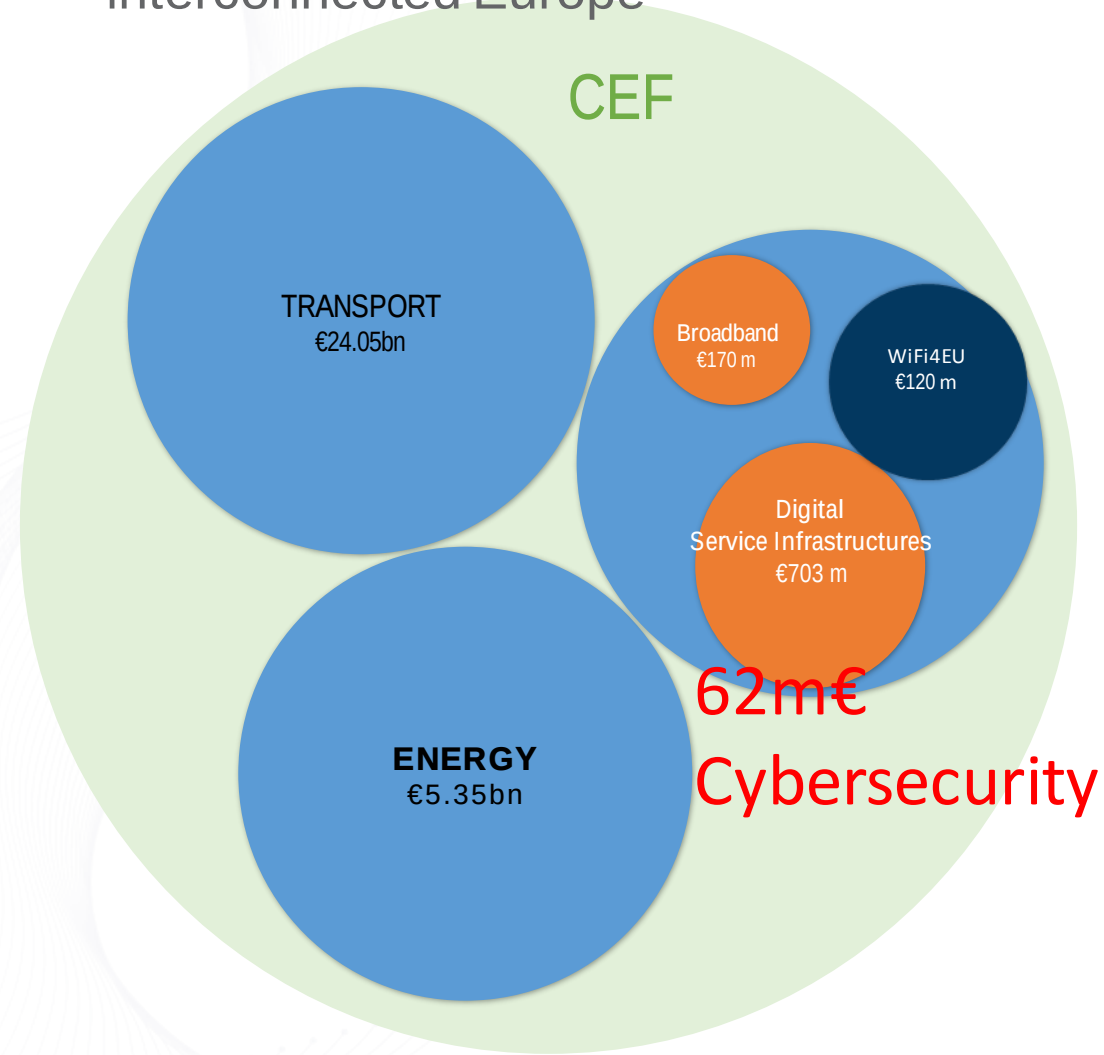
- 5G will increase the overall **attack surface** and the number of potential **entry points** for attackers;
- certain pieces of equipment will become **more sensitive** (as critical functions move to the edge of the network);
- Increased exposure to risks related to **reliance on suppliers**; increased number of attack paths for threat actors, in particular state or state-backed ones.
- Importance of the **risk profile** of individual suppliers;
- Increased risks from major **dependencies** on suppliers;
- On top of confidentiality and privacy, **availability and integrity** of networks will become major concerns.

Horizon 2020 EU program on R&I, upcoming cyber topics

- SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems. (RIA, 47.00 MEUR 19/11/2019)
- SU-DS02-2020: Intelligent security and privacy management. (RIA/IA, 38.00 MEUR 27/08/2020)
- SU-DS03-2019-2020: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises. (IA, 10.80 MEUR 27/08/2020)
- SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches. (IA, 20.00 MEUR 27/08/2020)
- SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe. (IA, 20.70 MEUR 27/08/2020)
- SU-AI-2020: Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe (IA, CSA 20.00 MEUR 27/08/2020)

Connecting Europe Facility (CEF) 2014 to 2020

Infrastructure programme to support the establishment of trans-European networks to reinforce an interconnected Europe



DIGITAL SERVICE INFRASTRUCTURES

Financial incentive
Mostly **PROCUREMENT**

CORE SERVICE PLATFORM

Central hubs of digital service infrastructures aiming to ensure trans-European connectivity, access and interoperability ...

Financial incentive
GRANTS

GENERIC SERVICES

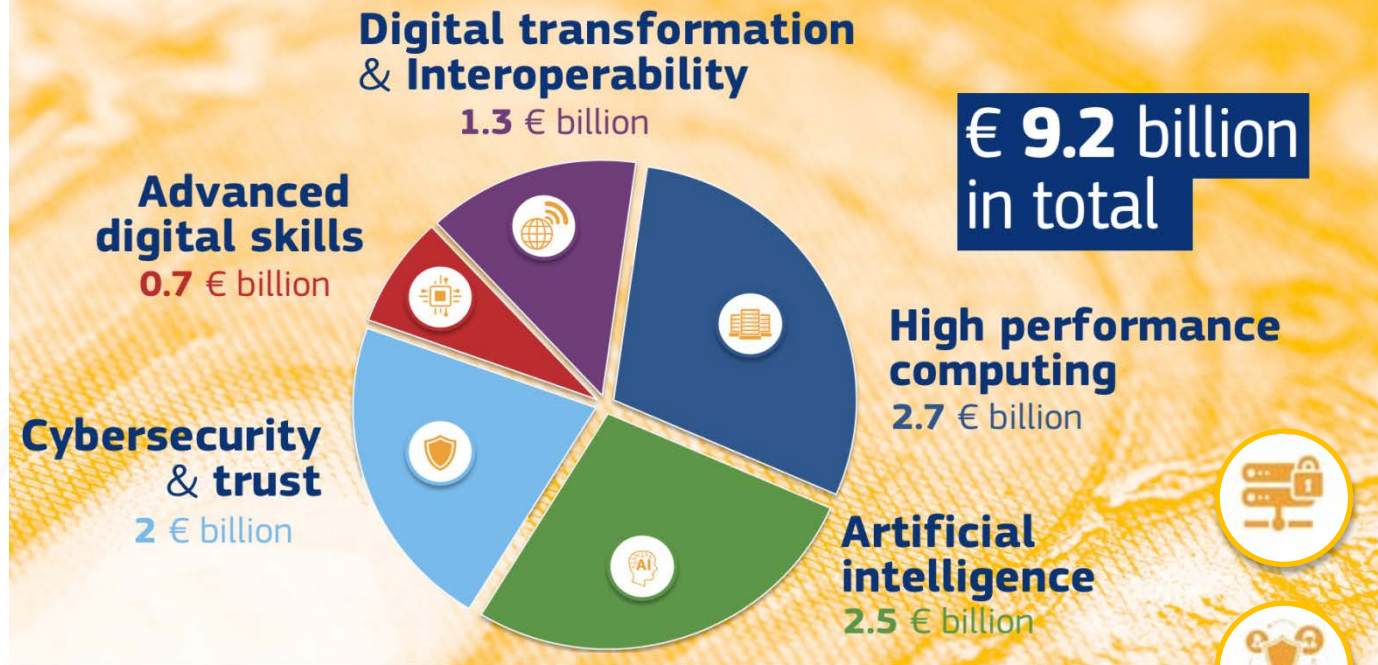
Gateway services linking one or more national infrastructures to core service platforms

Multiple DSIs including Cybersecurity DSI

CEF 2019 Call: Objectives & Outcomes

Call Objective	Title	Beneficiaries are expected to have...
1	Cooperation among designated national CSIRTs for the joint use of MeliCERTes	Demonstrated the sustained use of the MeliCERTes facility at least throughout the duration of the Action from teams in at least 2 Member States
2	Support for identified Operators of Essential Services (OES) for capability development and for the set-up of Information Sharing and Analysis Centres (ISACs)	Improved internal capabilities to meet security and reporting requirements under NIS Directive and enhanced situational awareness with effective information sharing through involvement with relevant ISAC
3	Support to National Competent Authorities (NCAs) and Single Points of Contact (SPOCs) to undertake the liaison, regulation and enforcement obligations set out in the NIS Directive	In-house capabilities, facilitation of reporting from OES and DSPs and structured interaction. Engagement with cybersecurity co-operation facilitation manager for NCAs and SPOCs (set-up by the EC) and use of the support services of that manager
4	Trans-European cooperation for effective joint cybersecurity operations and to build mutual trust/confidence	Used Blueprint Recommendation (operational layer), other operational cybersecurity measures. Engagement with the cybersecurity co-operation facilitation manager for NCAs and SPOCs (set-up by the EC) and to use the support services of that manager
5	Support to a common level of maturity in cybersecurity certification	Built up internal capabilities, exchanged best practises, increased operational capacities for certification and contributed to activities and working groups of the European Cybersecurity Certification Group established in line with the EU Cybersecurity Act.

Digital Europe programme; reinforcing digital capacities and their use



#EUBudget
#DigitalEurope

€2 billion proposed for
Cybersecurity to:

- Support procurement of advanced equipment, tools & data infrastructures
- Support the best use of European knowledge, capacity and skills
- Ensure wide deployment of latest solutions across the economy
- Reinforce capabilities for high level of network & information systems

Proposal for a European Cybersecurity Industrial Technology and Research Competence Centre, Network of National Coordination Centres, and Cybersecurity Community



Centre's Role:

Network coordination and support

Research programming and implementation

Procurement

Ensuring synergies between civilian and defence spheres

Cybersecurity Competence Network Pilots

More than **€63.5 million** invested in **4 projects**



Partners: **46**

EU Member States involved: **14**

Key words

SME & startup ecosystem
Ecosystem for education
Socio-economic aspects of security
Virtual labs and services
Threat Intelligence for Europe
DDoS Clearing House for Europe
AI for cybersecurity
Post-Quantum cryptography



Partners: **43**

EU Member States involved: **20**

Key words

Cybersecurity for citizens
Application cases
Research Governance
Cyber Range
Cybersecurity certification
Training in security



Partners: **30**

EU Member States involved: **15**

Key words

Network of Cybersecurity centres
Cyber Range
Cybersecurity demonstration cases
Cyber-skills Framework
Cybersecurity certification
Cybersecurity early warning



Partners: **44**

EU Member States involved: **14**

Key words

Research Governance
Cybersecurity skills
Cybersecurity certification
Community engagement
International cooperation
Strategic Autonomy

Last updated 26 February 2019

More than **160 partners** from **26 EU Member States**

More info at:

<https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network>

Conclusiones

- UE en el mundo: Autonomía estratégica > Soberanía tecnológica > Ciberseguridad
- Prioridades de ciberseguridad : Defensa, Resiliencia, Excelencia
 - ✓ Capacitación (mínima de cada uno; la mayor posible en conjunto)
 - ✓ Coordinación (mediante instrumentos y objetivos compartidos)
 - ✓ Información (intercambiar, aprender, ayudarse)
 - ✓ Inversión (pública UE, pública nacional y local, privada)
- Desafíos de la coordinación EU
 - ✓ Seguridad nacional vs mercado (interior...)
 - ✓ Coordinación en la diversidad (o cómo superar la fragmentación respetando las diferencias)
 - ✓ Tensiones y presiones internacionales (competencia comercial, lucha por influencia)
 - ✓ Amenazas múltiples e híbridas (el componente ciber cada vez más importante)
- Estímulos comunitarios: conjunto de instrumentos
 - ✓ Compromisos políticos: alinear y coordinar acciones nacionales
 - ✓ Legislación (“horizontal”, “vertical”): obligaciones nacionales (y de otros actores, ej. operadores críticos); mercado interior
 - ✓ Financiación: apoyo puntual y repartido vs inversión selectiva y estratégica

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional