Policies in the Quantum era

Dr Nineta Polemi

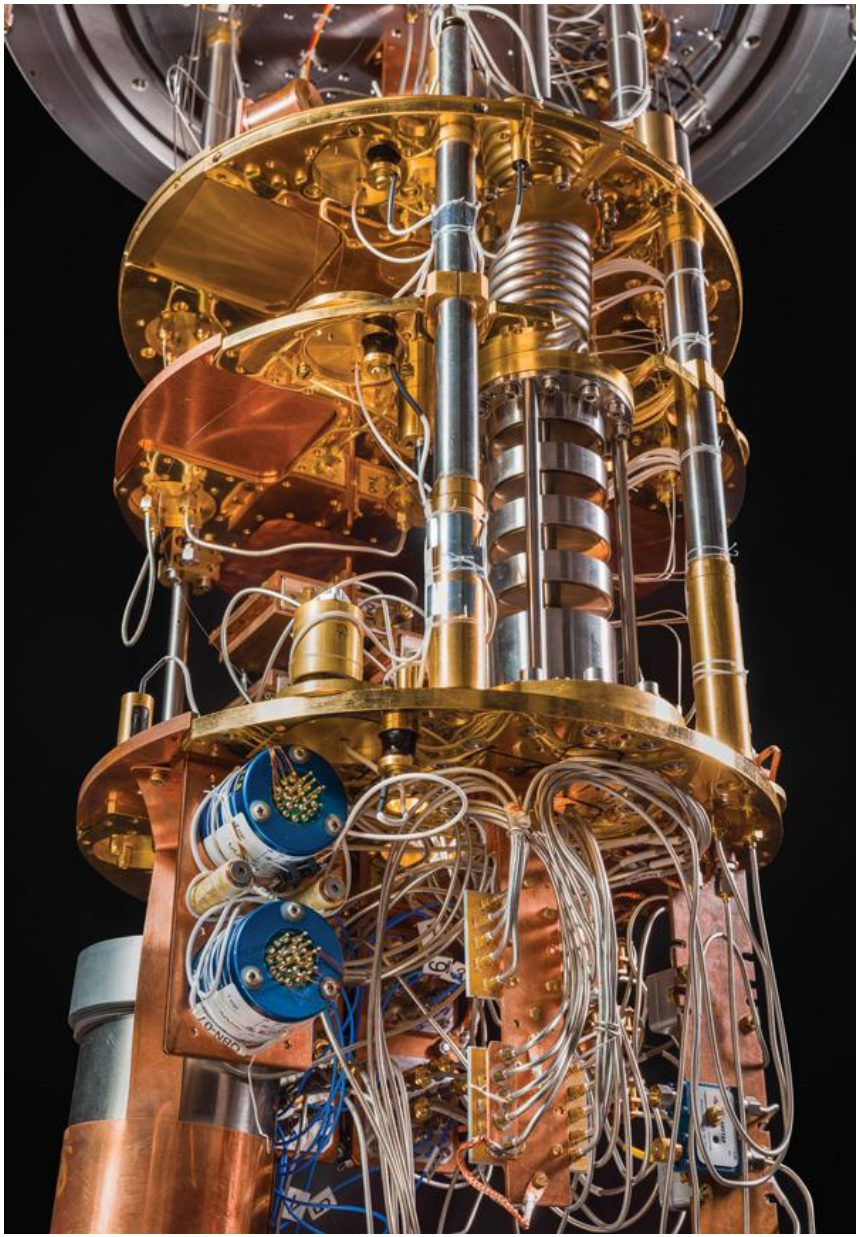
European Commission
DG CNECT/H1

ENISA-FORTH
Summer School 2018

Quantum Computer (QC)

The Idea: Exploit quantum mechanics to process information

The Ambition: Solve every computational problem "blazing fast", that no traditional computer will ever have the memory or processing power to tackle.



IBM's futuristic quantum computer

European Commission

QC: Milestones

1981- Richard Feynman

1994 Peter Shor

1998 – 2-qubits

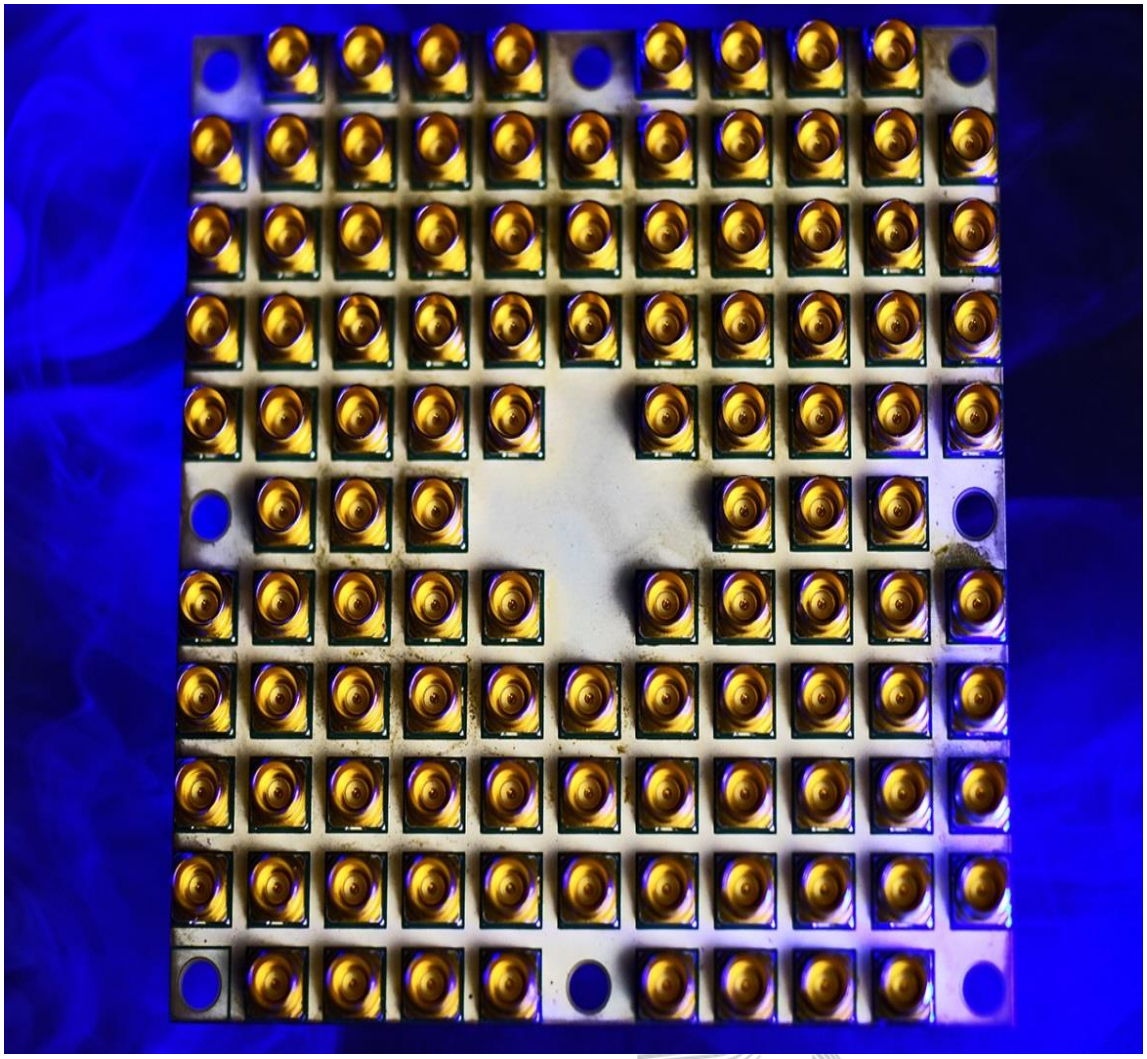
R.F.: proposed the use of properties of subatomic particles (sp) to model the behavior of other.
P.S: QC (if ever possible to build) will defeat public-key encryption system.

European Commission

Practical QC 2018

Tangle Lake: **Intel's 49-qubit** superconducting quantum test chip (2018)

Rigetti USA- **128 qubits** (2018)



Practical QC: We are not there yet

Challenges

- **QC will need at least one million qubits**
- **QC requires much more than larger arrays of qubits:**

✓ **error correction** that can detect/ correct disruptions in the fragile quantum states of individual qubits.
✓ how to **map software** algorithms to the QC hardware.
✓ **local electronics** layout necessary to control the individual qubits and read out the quantum computing results.

Building QC that can solve real computing problems will require many more years of research

Will QC break Internet encryption?

- The rise of **Post Quantum Cryptography** (Quantum Resistant Cryptography) fades this concern.

- The **QKD advantages are controversial:** QKD does not offer significant practical security advantages over what we can currently do at low-cost with conventional techniques.

- QKD seems to introduce a whole **new attacks** that are not yet well understood. **Further research** is required in order to build up knowledge of how to attack and defend commercial QKD systems.

- *NIST Post –Quantum Crypto Competition*.

- **QKD is channel dependent** and thus vulnerable.Requires new hardware for optical links (space and ground), new trusted-node satellite or entangled photon concept.

Space -QKD & Cyber- Attacks on Satellites

- ✓ **Signals jamming, monitoring** (between satellites and receivers or between transmitting ground stations and satellites)
- **Spoofing** manipulates the information and thus reduces its integrity
- **DoS** by interrupting electrical power to the space ground nodes
- …….
- **<u>Impacts of Attacks</u>**: take control of the satellite, shut it down, alter its orbit

Cyber-attacks in space infrastructures

- Space **Critical Information Infrastructures** (CII) can face physical and cyber-attacks at all levels (networks, ICT systems/equipment, services, processes)
- **Impact of Attacks**: destroy space control, operations, missions, services

Cyber-attacks in space software

- ✓ Back doors for espionage or sabotage
- ✓ Unencrypted data
- ✓ Insecure protocols
- ✓ Exploitable software flaws
- ✓ *…..*

*Space operations and services are **global supply chain services** and the propagation rate of a cyber-attack may catastrophically impact the whole world!!!!*

EC activities

QUANTUM FLAGSHIP

1 Billion €
10-year Flagship initiative (2017-2027)

The "Quantum Flagship" should prove its value as large scale mission-oriented initiative, leading the 2nd *Quantum Revolution* by accelerating the transition from laboratory science to commercial exploitation in real-world settings.

QUANTUM FLAGSHIP: Timeline toward a Q-ecosystem

2016

PREPARATORY STEPS

04/2016: Announcement in EU Cloud Initiative

09/2016: Set-up of the QT Flagship High Level Steering Committee

Intermediate report (02/2017)

Final report (09/2017)

2018

RAMP UP PHASE

+ Flagship Coordination & Support Actions: 0.5 m€ (2017) + 2 m€ (2018)
+ Flagship Research & Innovation Actions: 130 m€ (2018)

QUANT-ERA

+ QuantERA (01/2018): 26 countries, 36 m€ (1/3 EU)
+ QuantERA II (2020 - tbc): FET call: 10 m€

2019

CYBERSECURITY

+ H2020 LEIT ICT QKD Testbed call (2019): 15 m€

2020

FULL IMPLEMENTATION*

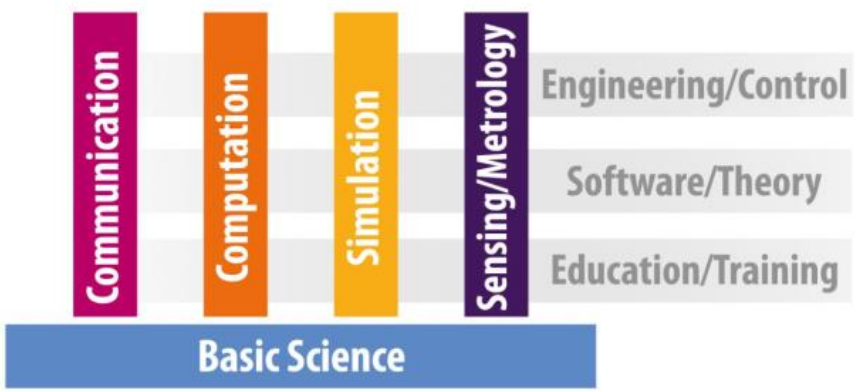
+ Series of QT calls
+ EU Quantum Key Distribution Network

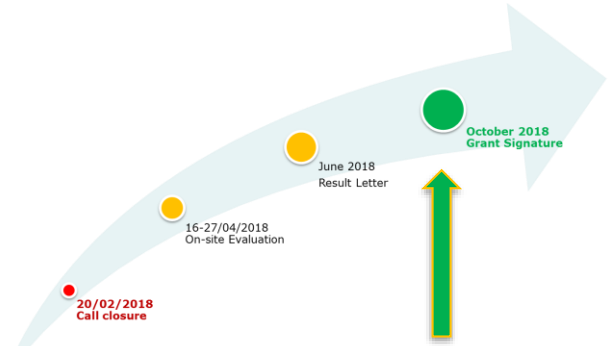
** pending adoption under the next multi-annual framework programme*

Ramp-up Phase: 2018-2020

- H2020-FETFLAG-03-2018 (1st call, closed 20.02.2018)
  - The 20 funded projects will start on October 1st 2018.

130 M€ - Research & Innovation Actions (RIAs)





All projects to start 01.10.2018
(collaborative agreement)

2 M€ - Coordination & Support Action (CSA)

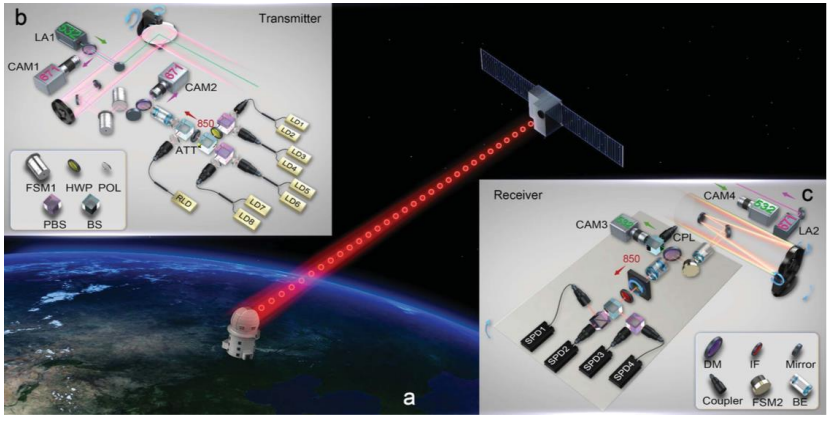
This action will follow a 1st QSA ending in 04/2019. www.qt.eu

European Commission

Joint activities with DG GROW (Galileo)

SCENARIO -1- to secure Galileo satellites (space-to-ground)

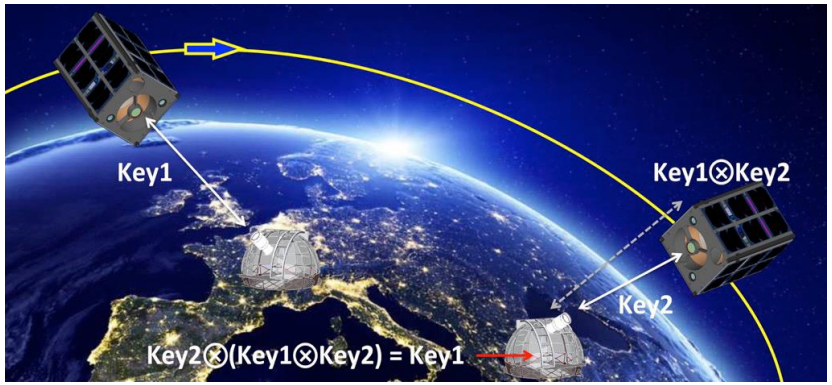
Up/downlink communications (e.g., telecommand) for the Galileo 2nd Generation (G2G)



2017: Technical workshop with EU experts
2018: Several technical meetings
→ GROW (J1), CNECT (C2), JRC-Ispra

SCENARIO -2- to secure Galileo infrastructures (ground-to-ground)

Satellite (or intersatellite link) as trusted relay sharing keys between two grounds stations



Goal for 2018: proposal for QKD payload specifications and interfaces with the satellite

ESA activities

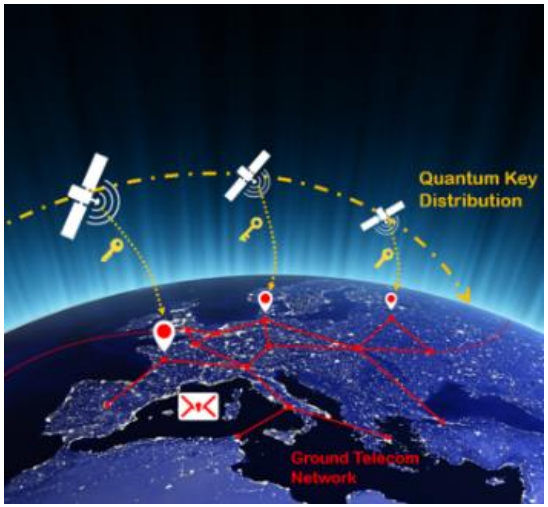
- 2003 Accommodation of a Quantum Communication Transceiver in an Optical Terminal
- 2004 Quantum Information and Quantum Physics in Space: Experimental Evaluation
- 2008 Photonic Transceiver for Secure Space Communications
- 2009 Entangled Photon Source For Quantum Communication 1
- 2009 Entangled Photon Source For Quantum Communication 2
- 2010 Introduction of Quantum Communication in Satellite Communication Networks
- 2011 Experimental Evaluation of Quantum Teleportation for Space Systems
- 2012 Applications of Optical-Quantum Links to GNSS
- 2014 Photonic Transceiver for Secure Space Communications: New Space Suitable Entangled Photon Source
- 2015 Ground Segment Development for LEO to Ground Quantum Communication
- 2017 Space Quest Phase A/B
- 2018 QUARTZ: Quantum Cryptography Telecommunication System
- 2018 Use of secure optical communication technologies to protect European critical infrastructure
- 2018 QKDSAT
- + internal studies and activities

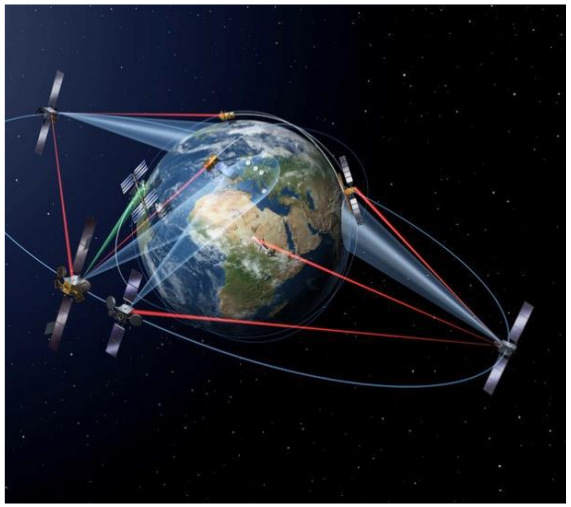
Towards a global quantum network (1/2)

Quantum communication is a mature technology, but its capabilities and its market potential is not yet fully deployed.

Our vision (under DEP): Going beyond point-to-point links, interconnected ground quantum networks (e.g., European capitals) or located anywhere on Earth. It may contain ground (quantum repeaters) and/or satellite-based trusted nodes (constellation with LEO, Galileo, GEO satellites).

Main applications: security (Q-crypto), Q-internet, time & frequency distribution.





European Commission

Towards a global quantum network (2/2)

Phase 0/A (under H2020): QKD testbed call (opening: 26.07.2018, closing: 14.11.2018), topic coordinator: A. BenMoussa (C2)

→ build an experimental platform to test and validate the concept of end-to-end security in the long-term,

→ identify the practical implementation issues, but with continuous R&D inputs from QT-Flagship (architecture, protocols, interoperability, standardization, …),

→ QKD as a service (economically justified).

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ict-04-2019.html

European Commission

Conclusions on QC

Continue building foundations for meeting QC Challenges

- **Quantum Threat Analysis and Risk management will open a path to certification of secure QKD systems.**
- **Certification on all QC, space and cyber technologies and applications**
- **Continuous standardisation efforts of Post Quantum Cryptography**
- **Build (national, EU, international) synergies between space, cyber security researchers and physicists**

Trustworthiness in QC era

Further information

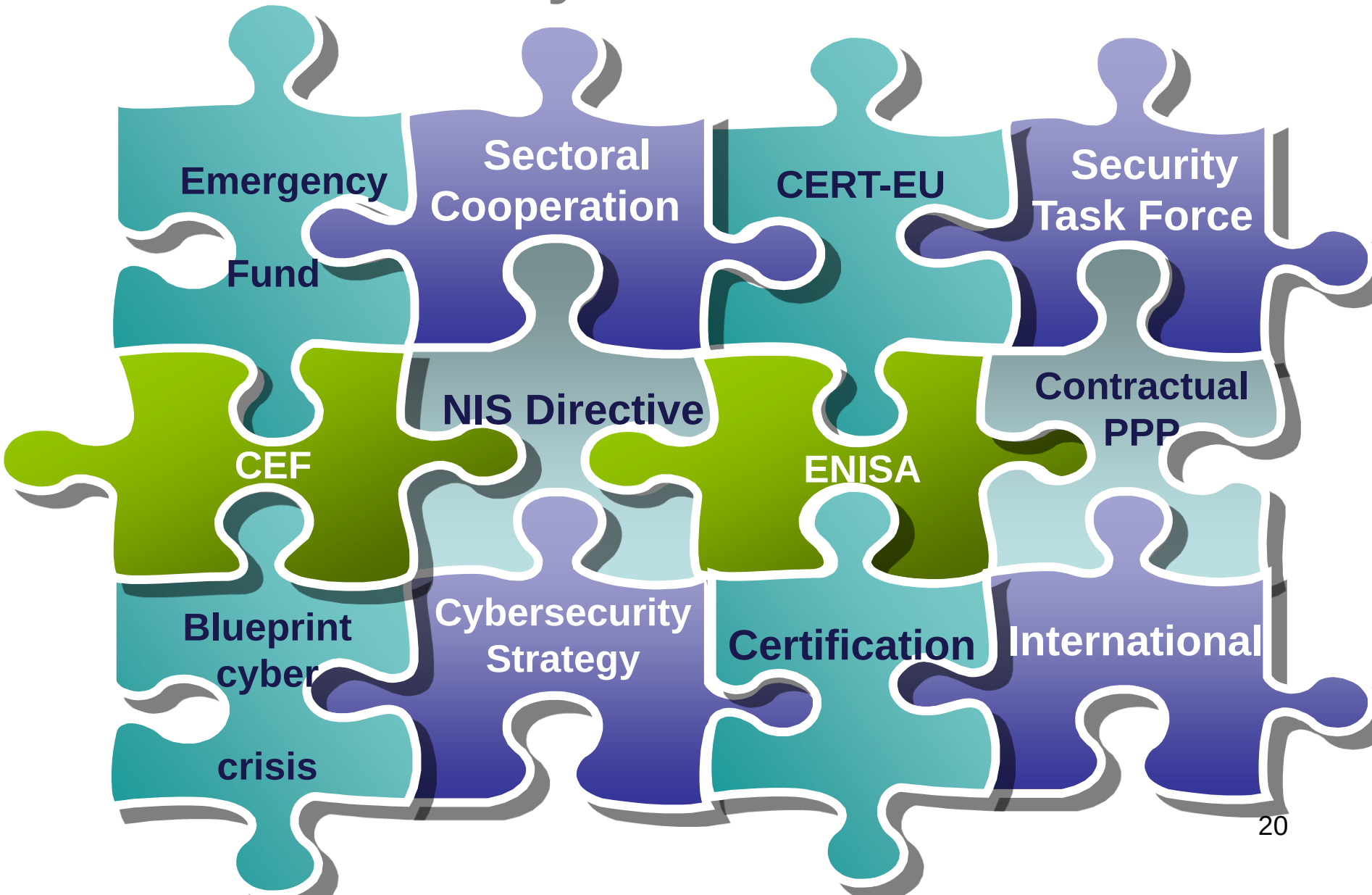
https://ec.europa.eu/digital-single-market/en/quantum-technologies

contact

cnect-quantum@ec.europa.eu

European Commission

E.C. Security Initiatives



The EU R&I in action: Core contribution

H2020 EU Contribution

219,6M 0,74% of H2020

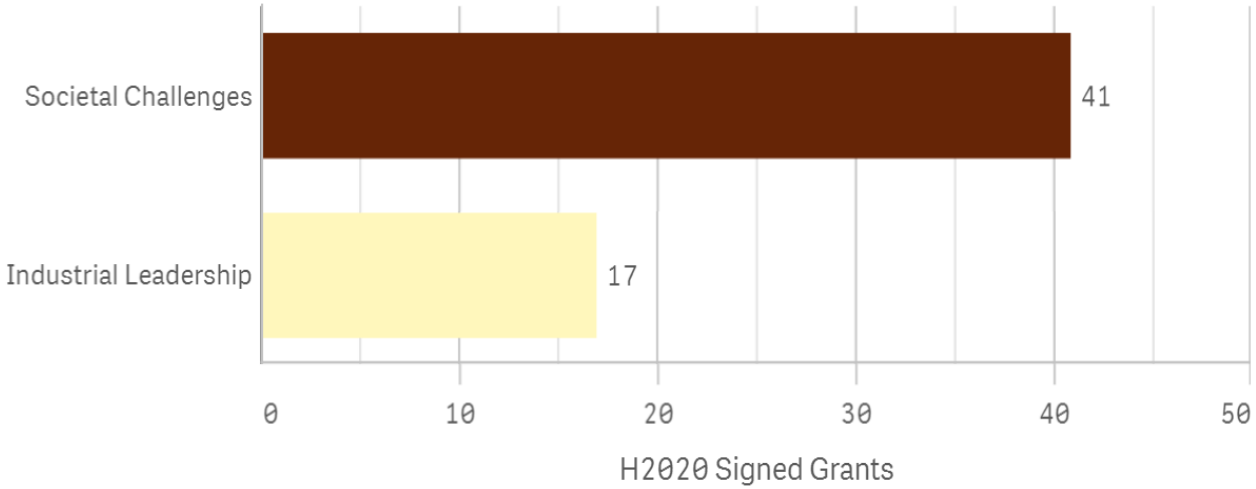
H2020 Signed Grants

58 0,35% of H2020

H2020 Total Cost

262M 0,70% of H2020

Signed Grants by Pillar / Thematic Priority



The EU R&I in action

Top Topics

Topic	Topic Descr	H2020 Signed Grants	H2020 EU Contribution
Totals		**58**	**€ 219.600.524**
ICT-32-2014	Cybersecurity, Trustworthy ICT	10	€ 38.578.248
DS-01-2016	Assurance and Certification for Trustworthy and Secure ICT systems, services and components	7	€ 23.486.256
DS-01-2014	Privacy	6	€ 19.578.047
DS-04-2015	Information driven Cyber Security Management	5	€ 20.302.856
DS-02-2016	Cyber Security for SMEs, local public administration and Individuals	5	€ 18.977.175
DS-02-2014	Access Control	4	€ 19.483.908
DS-06-2017	Cybersecurity PPP: Cryptography	4	€ 19.116.918
DS-03-2015	The role of ICT in Critical Infrastructure Protection	3	€ 16.991.061
DS-06-2014	Risk management and assurance models	3	€ 10.272.197
DS-04-2016	Economics of Cybersecurity	3	€ 5.989.903
DS-05-2016	EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation	3	€ 2.999.708
DS-05-2015	Trust eServices	2	€ 13.934.905

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

Cybersecurity Package

September 2017

GOALS: While Member States remain responsible for national security, EU further promotes cybersecurity on the global stage cybersecurity through cooperation.

The **Cybersecurity Package** improves a more robust response to cyber-attacks by:

- ✓ Encouraging a Single Cybersecurity Market
- ✓ Pooling and shaping research efforts in Cybersecurity
- ✓ Fostering NIS Directive implementation
- ✓ Proposing a reformed ENISA
- ✓ Promoting cyber skills and cyber hygiene habits
- ✓ Coordinating an emergency response
- ✓ Cooperating with NATO for effective cyber-exercises.

EU Cybersecurity Act

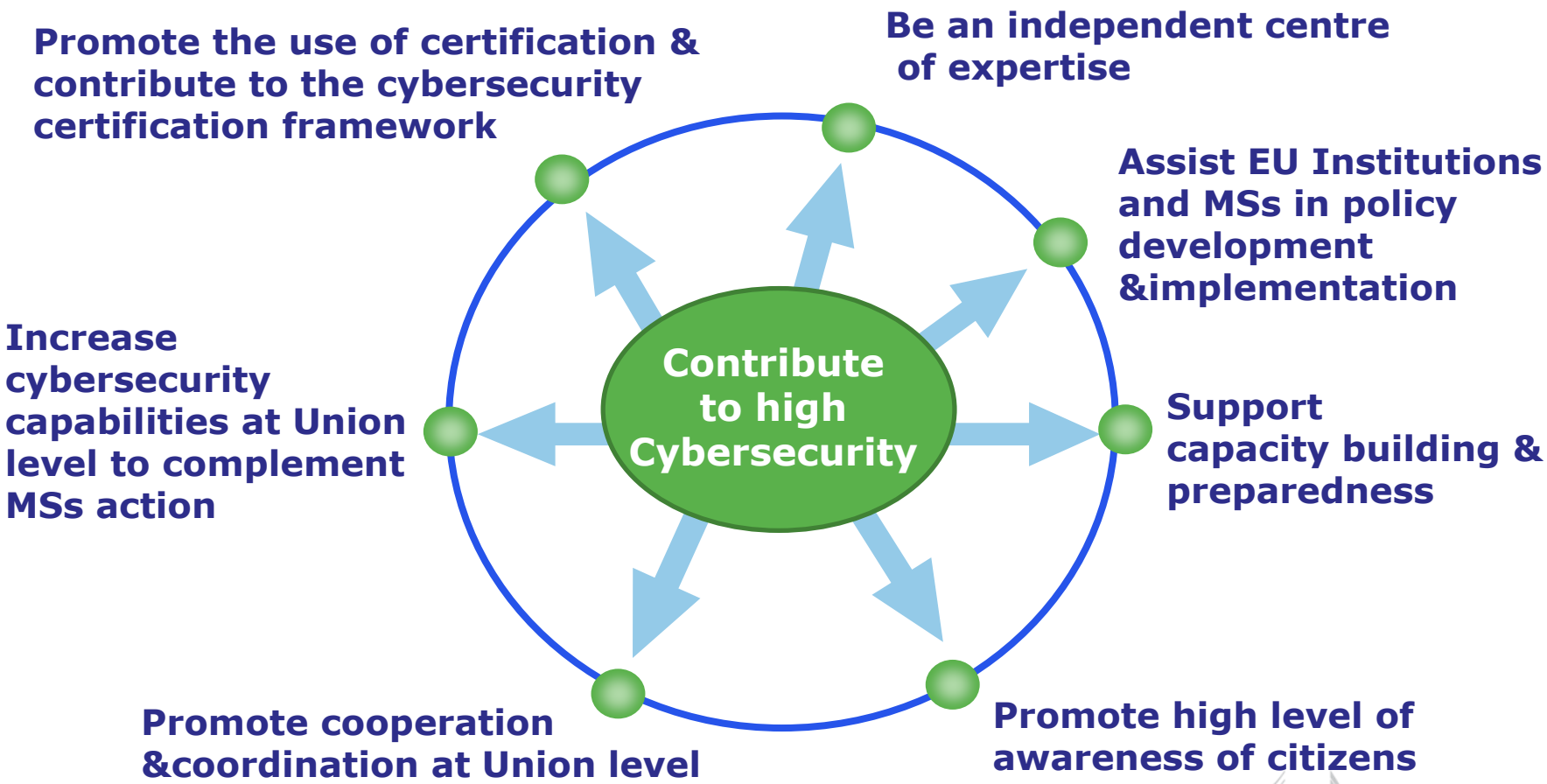
Towards a reformed
EU Cybersecurity Agency
and reinforcing the cybersecurity single market in the EU

European Commission

ENISA

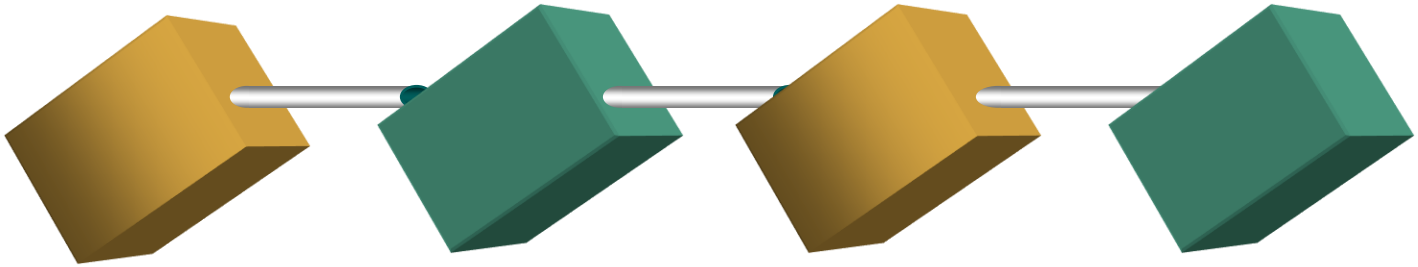
Towards an EU Cybersecurity Agency fit for current and future challenges

Mandate and objectives



European Commission

Capacity building



CSIRTs Development, national Strategies, support to Cooperation Group

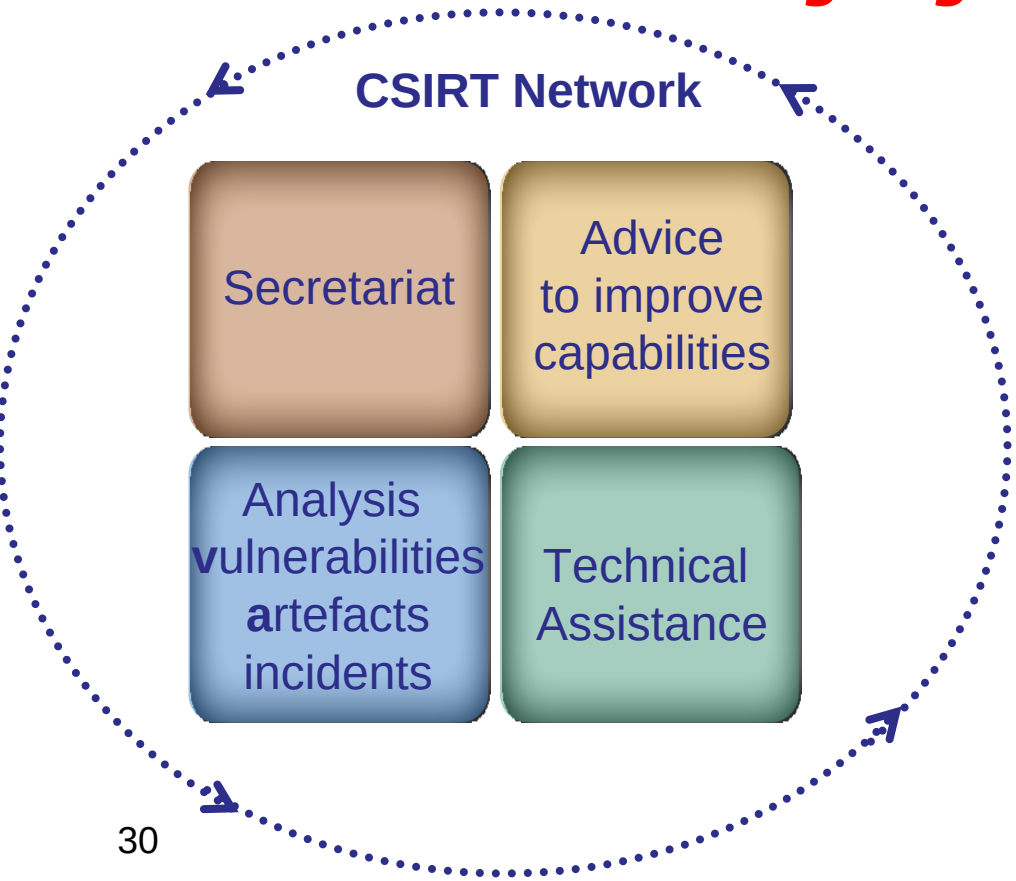
Facilitate Establishment & development Sectoral ISACs

Trainings, Knowledge, Expertise

Support **d**evelopment & **R**eview of Union strategies

Operational cooperation

Ongoing cooperation



Regular *EU Cybersecurity Technical Situation Report*

Annual cybersecurity exercise

European Commission

Knowledge, information & awareness

- Long term strategic analyses of cyber threats& incidents
- Analyses of emerging technologies

Knowledge

One stop shop portal of information from EU institutions, Agencies and bodies

Information Hub

- Compiling reports to provide guidance after big incidents
- Provide guidance on good practices for individual users
- Regular campaigns

Awareness Raising

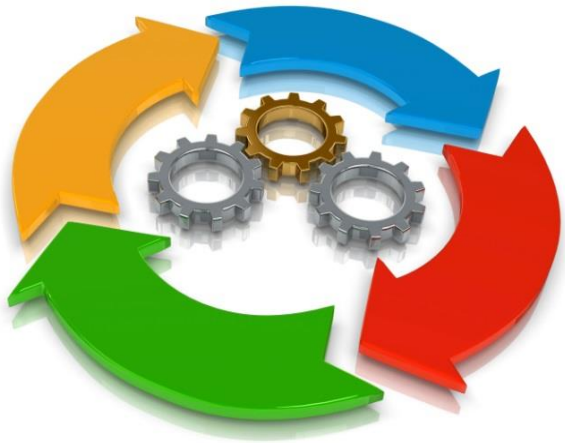
European Commission

ICT cybersecurity certification

Towards a true cybersecurity single market in the EU

Our proposal

*A **voluntary European** cybersecurity certification **framework….***



…to enable the creation of individual EU certification schemes for ICT products and services…

…that are valid across the EU

European Commission

…For vendors/providers

- *The possibility to obtain cybersecurity certificates that are valid across the EU would:*
  - *Generate higher incentive to certify and enhance the **quality** of digital products / services*
  - *Enhance **competitiveness** through reduced **time** and **cost of certification***
  - *Help gain access to market segments where certification is required*
  - *Contribute to promote a **chain** **of** **trust between** vendors **and** end-users*
- *For **SMEs** and **new business…***
  - *Elimination of a potential market-entry barrier*

European Commission

Blueprint

Resilience through crisis management and rapid emergency response

Improving resilience through crisis management and rapid emergency response – with a focus on Response

European Commission

Improving resilience through crisis management and rapid emergency response - 3 lines of actions

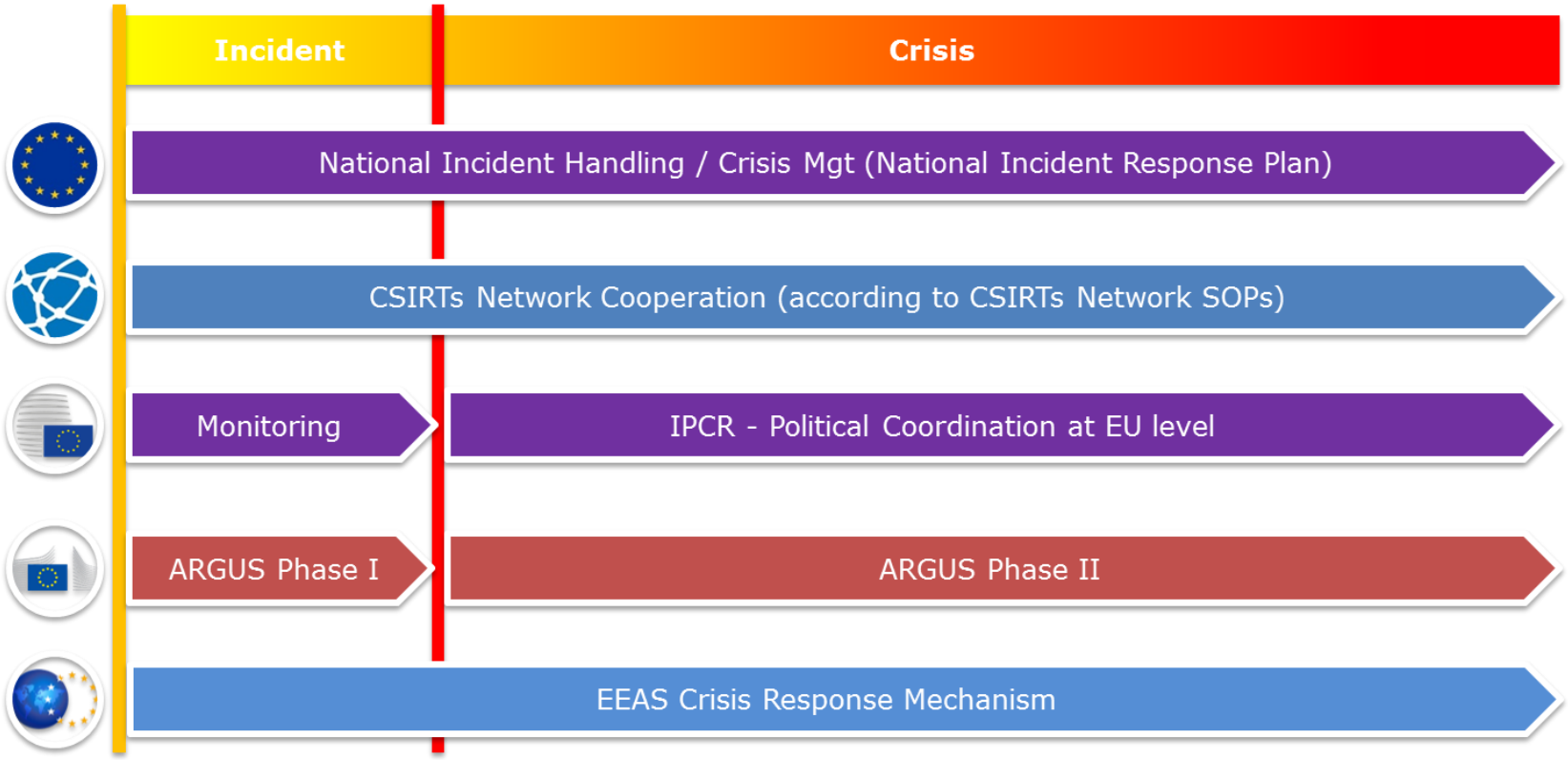
1. **Blueprint** - Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (COM(2017) 6100).

2. **ENISA** (COM(4776/2)) - Tasks relating to operational cooperation at Union level
   - The Agency shall contribute to develop a cooperative response, at Union and Member States level, to large-scale cross-border incidents or crises related to cybersecurity

3. **Cybersecurity Emergency Response Fund -** Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450/1

Blueprint – Core objectives

Blueprint – key mechanisms



Member States | CSIRTs Network | IPCR | ARGUS | EEAS CRM

European Commission

European Commission

Cybersecurity Emergency Response Fund

Resilience through crisis management and rapid emergency response

Cybersecurity Emergency Response Fund

- Investigate the creation of Cybersecurity Emergency Response Fund.
- Allow Member States to seek help at the EU level during or following a major incident.
- 'Moral hazard' safeguards.
- Complement existing crisis management mechanisms at EU level.
- Rapid response capability in the interests of solidarity.
- Draw on national expertise along the lines of the EU Civil Protection Mechanism.

European Commission

Communication on 'Making the most of NIS:

towards the effective implementation of the NIS Directive

Key messages of the Communication

- **Put in place comprehensive and ambitious national strategies**
- **Ensure *effective and adequately resourced national CSIRTs***
- **Ensure effectiveness of implementation and enforcement**
- **Align the national approaches on Operators of Essential**
- **Extend the scope of the NIS Directive to additional sectors, e.g. public administration**

European Commission

A cybersecurity competence network with a European Cybersecurity Research and Competence Centre

Reinforcing EU's cybersecurity technologic capabilities and skills

Retain the capacity to **protect EU's economy, society and democratic order**

Need for all EU **economic sectors** to be equipped with the latest technologies and skills to protect their assets and develop innovative products

Step up **investment in cybersecurity research & innovation capabilities**

Cybersecurity competence network with a European Cybersecurity Research and Competence Centre.

Collaboration with major international centers

(e.g. NCCOE, CNITSEC, CSC, ACSRI)

Building on the work of Member States and the cPPP, a **cybersecurity competence network** with a **European Cybersecurity Industrial Research and Competence Centre** will stimulate the development and deployment of secure products in all sectors, thus contributing to build a robust technological advantage for the EU.

Proposal for a Regulation

Brussels, ***12.9.2018*** *COM(2018) 630 final*

2018/0328 (COD) REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL **establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**

European Commission

Pilot Projects

- CONCORDIA
- ECHO
- SPARTA
- Cybersecurity4Europe (reserved)

Will provide in **a clustered manner the necessary evidence** for properly establishing the actual European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

European Commission

State of the Union 12/9/2018

- measures for keeping up with the raising cyber threats, including the creation of a Network of Cybersecurity Competence Centres

- EC will continue its efforts on cybersecurity for the benefit of the EU's digital economy, society and democracies in the next MFF

European Commission

EC Cybersecurity Investments 2021-2027

Digital Europe programme €2 billion into safeguarding the EU's digital economy, society and democracies through polling expertise, boosting EU's cybersecurity industry, financing state-of-the-art cybersecurity equipment and infrastructure. Cybersecurity research and innovation will additionally be supported under the Horizon Europe programme.

European Commission

Conclusions on EC security initiatives

Develop mutually agreed, holistic mitigation frameworks, compliant with: EU strategies/policies (e.g. Space Strategy for Europe 2016/2325(INI), Common Security and Defence Policy –CSDP-, Decision No 541/2014/EU), directives (e.g. NIS, GDPR);

Certification, Capabilities (skills, innovation) building, Liability, Accountability, Trustworthy collaboration (CSIRT network, TERENA, etc);

The outcomes of the EC projects need to be monitored and derive evidence for targeted policies

Build Trust & Collaboration

European Commission

Thank you for your attention

Follow us on Twitter:
https://twitter.com/Cybersec_EU

Subscribe to our newsletter:
http://europa.eu/!yT68Jg

Nineta.POLEMI@ec.europa.eu

European Commission