Cybersecurity Policy

2017 Cybersecurity Package, Network Information Security Directive, R&I in Horizon Europe

Dr Florent Frederix
Cybersecurity Capabilities and Technology Unit
European Commission

DGAC, Toulouse, 15 November 2018

Content

- *2017 Cybersecurity package*
  - **ENISA**
  - **EU Cybersecurity Certification**
- *Network Information Security Directive*
  - **Status**
  - **Planning**
- *Innovation and Research in H2020 and H2027*
  - **CEF call 2018 & 2019**
  - **Cybersecurity Competence Centre in H2027**
  - **Future Digital Budget**

2017 Cybersecurity package

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

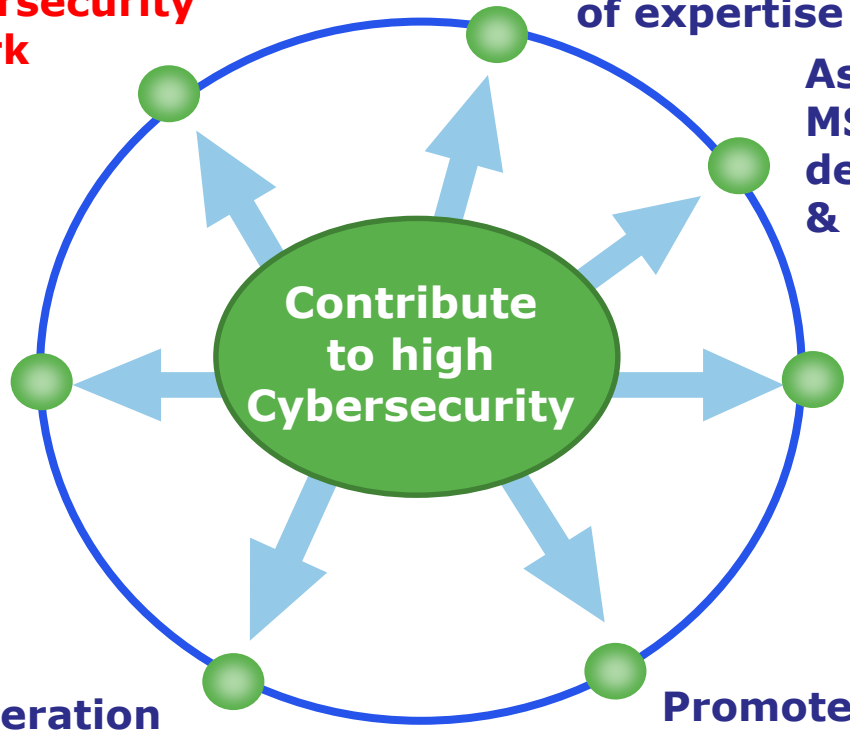
The **Cybersecurity Package** improves a more robust response to cyber-attacks by:

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

Cybersecurity package

ENISA: towards a reformed EU Cybersecurity Agency (1)

Cybersecurity package



Promote the use of certification & contribute to the cybersecurity certification framework

Be an independent centre of expertise

Assist EU Institutions/ MSs in policy development & implementation

Increase cybersecurity capabilities at Union level to complement MSs action

Support capacity building & preparedness

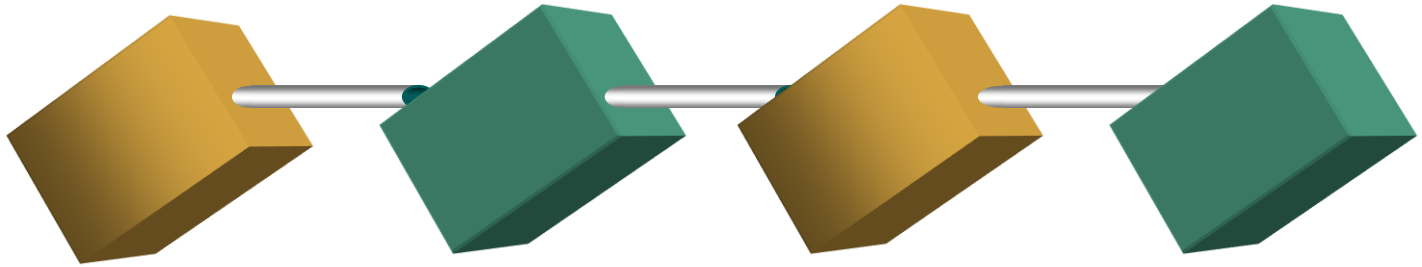
Promote cooperation &coordination at Union level

Promote high level of awareness of citizens & businesses

ENISA: towards a reformed EU Cybersecurity Agency (2)

Capacity building

Cybersecurity package



CSIRTs Development, national Strategies, support to Cooperation Group

Facilitate Establishment & development Sectoral ISACs

Trainings, Knowledge, Expertise

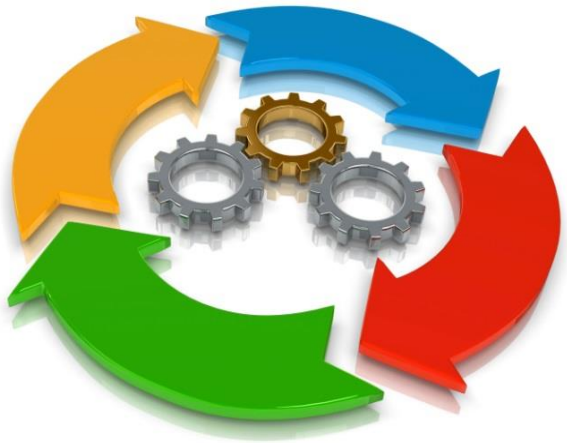
Support **d**evelopment & **R**eview of Union strategies

European Commission

EU Cybersecurity Certification Framework

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

Cybersecurity package



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

…that are valid across the EU

Aviation stakeholders can work out a certification scheme and possibly make it part of the sector specific regulation.

European Commission

Cybersecurity package

Core elements

1) One EU Cybersecurity Certification Framework, many schemes.

- *Tailored schemes specifying: scope - product/service category; evaluation criteria and security requirements ; assurance level*

2) Resulting Certificates from European schemes are valid across all Member States.

- *Once a European scheme has been established:*
  - Member States cannot introduce new national schemes with same scope
  - Existing national schemes covering same product/service cease to produce effects
  - Existing certificates from national schemes are valid until expire date

3) The use of EU certificates remains voluntary, unless otherwise specified in European Union law.

- The specified requirements of the scheme shall not contradict any applicable legal requirements, in particular requirements emanating from harmonised Union legislation.

Cybersecurity package

4) **MSs will appoint a national certification supervisory authority** that will: **supervise** the activities of Conformity Assessment Bodies (**CAB**) and the compliance of the certificates issued by CABs; be independent of the entities they supervise; **handle complaints** on certificates issued by CABs; **withdraw certificates** that are not compliant and impose **penalties; participate** in the new European Cybersecurity Certification Group

5) The European Cybersecurity Certification Group has the following tasks:

- advises the Commission and assists ENISA in the preparation of EU schemes
- proposes to the Commission that it requests ENISA to prepare a EU scheme
- adopt opinions addressed to the Commission relating to the maintenance and review of existing EU schemes
- the Commission chairs the Group and provides the secretariat with the assistance of ENISA

6) European cybersecurity certificates are accredited by a National Accreditation Body (NAB) – Reg. 765/2008

- Accreditation shall be issued for a maximum of five years
- NABs can revoke accreditation of CABs
- Member States notify the Commission of the accredited CABs for each EU scheme

7) In justified cases a European scheme may provide that a certificates can only be issued by a public body such as:

- a national certification supervisory authority
- a body accredited as a CAB
- a body established under national laws, meeting the requirements according to ISO/IEC 17065:2012.

The NIS directive

Status

- ✓ **17 member states have confirmed that they have taken the necessary steps to make NIS operational.**

Planning in 2017 cybersecurity package

- **Good practices and recommendations issued by ENISA**
- **Examples from Member States**
- **Interpretation of Directive's provisions and of how they would work in practice**

NIS Directive

e.g. good practice: Secure information in transit when possible (https://). What about secure GPS signals?

CEF call 2018

European Commission

Cybersecurity Call (CEF-TC-2018-3) : Key Facts

Research & Innovation

Cybersecurity capability development for different entities

€13 million in total

Closing call 22 November 2018

Grants:

Co-funding up to 75% of the eligible costs of the action

Pre-financing: 50% within 30 days after signed grant agreement, balance on completion

Funding per proposal: Various, depending on the objective, EC (expected) contribution ranges from € 100,000 up to €1,000,000 per action

- ***Indicative duration of the actions: 24 months***

Call objectives and eligibility

OES in Air, Rail, Water & Road Transport Subsectors

For the Transport sector!

Objective		
1	National CSIRTs (Co… Teams) designated by the … NIS Directiv…	National CS… Article 9 of th…
2	**Operators of Essential Services (OES)** and Digital Service Providers (DSP) in line with the NIS Directive	Must include at least one OES or one DSP. OES must provide a letter of support from relevant authority.
3	Public and private sector entities working on **Cooperative Connected and Automated Mobility**, in particular for electric vehicles	Any eligible applicant
4	National Competent Authorities (NCAs) and Single Points of Contact (SPOCs) designated in line with the NIS Directive	NCAs and SPOCs designated under Article 8 of the NIS Directive
5	Capability development for public bodies established by national or European legislation in a Member State to meet European Union Policy objectives associated with Operational Level Cyber Security	Must include at least one public body with a structured co-operation agreement with at least 8 other Member States.

Research & Innovation

Transport

For more info on the call: INEA

Research & Innovation

Call page: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cyber-security

Call infographic: is this call for me?: https://ec.europa.eu/inea/sites/inea/files/cybersecurity_diagram_2018.pdf

CEF Cybersecurity for Transport – info day recording: https://ec.europa.eu/inea/en/news-events/events/2018-cef-transport-call-virtual-info-day

European Commission

Research & Innovation

Research and Innovation In Horizon Europe

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

Reinforcing EU's cybersecurity technologic capabilities and skills

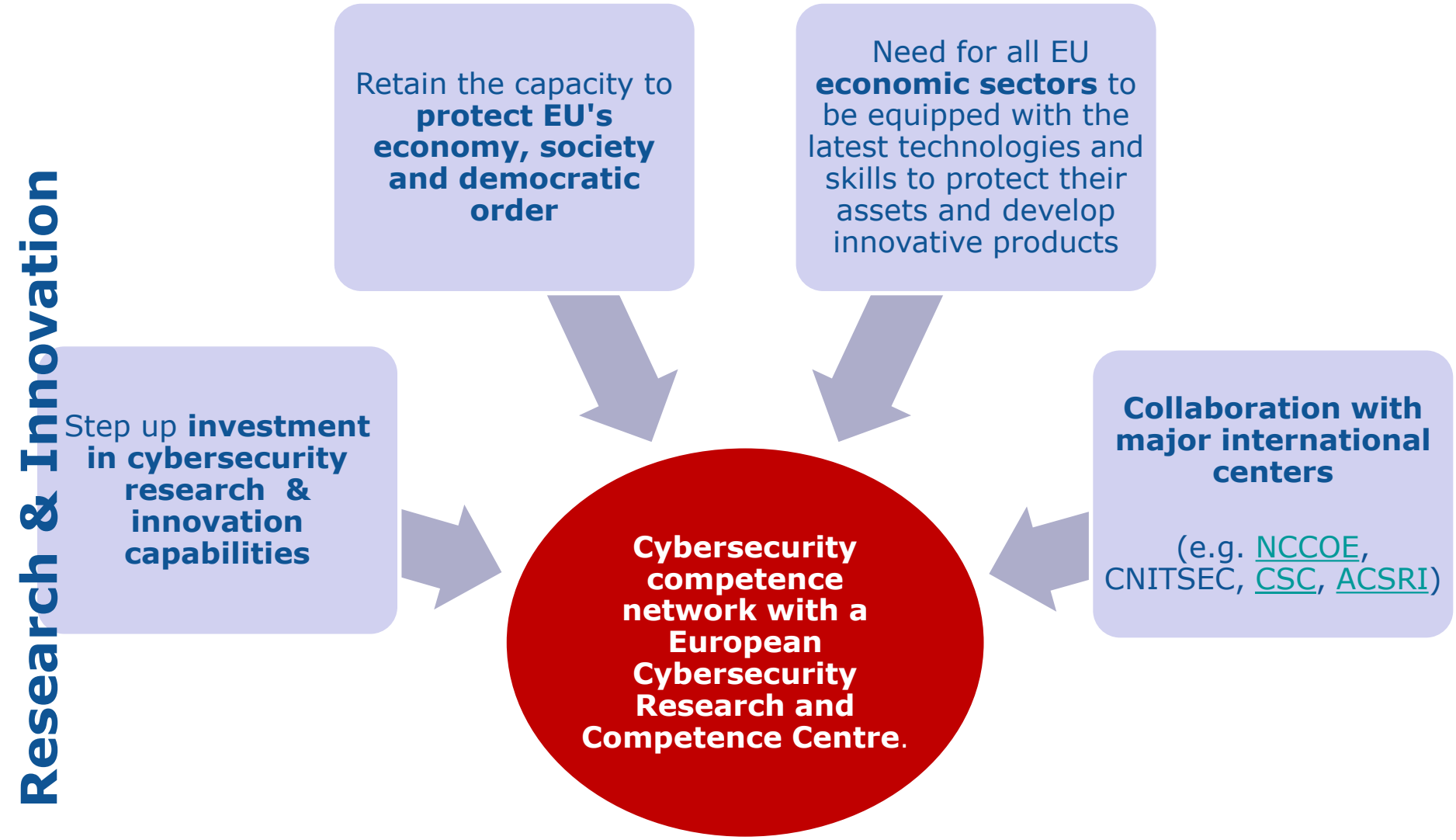
State of the Union 12/9/2018

Research & Innovation

- 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

Research & Innovation



European Commission

European Cybersecurity Technology & Innovation Ecosystem

Research & Innovation

European Competence Centre:

- manage the funds foreseen for cybersecurity under Digital Europe and Horizon Europe 2021-2027
- facilitate and help coordinate the Network and Community to drive the cybersecurity technology agenda
- support joint investment by the EU, Member States and industry and support deployment of products and solutions.

Network of National Coordination Centres:

- Nominated by Member States as the national contact point
- Objective: national capacity building and link with existing initiatives
- National Coordination Centres may receive funding
- National Coordination Centres may pass on financial support

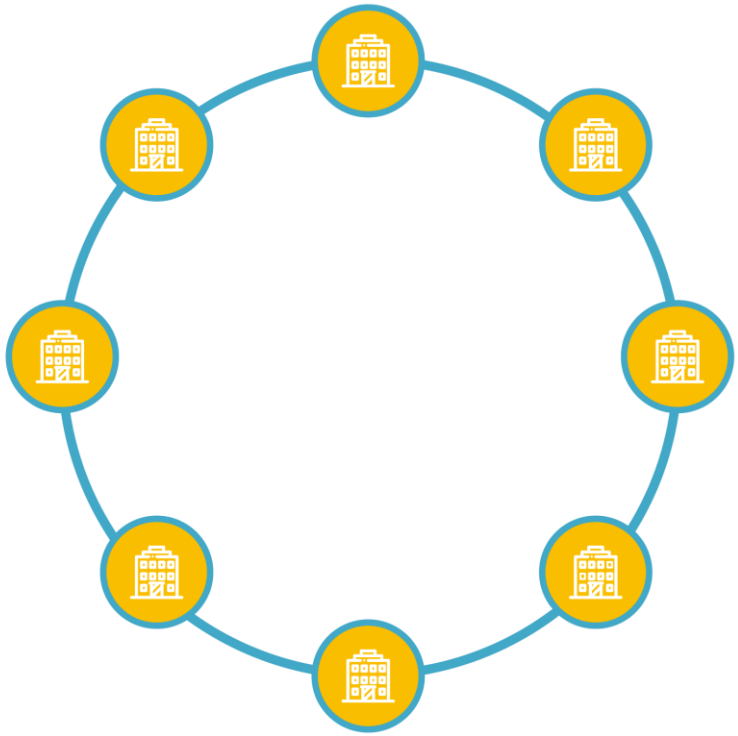
Competence Community:

- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence sectors

European Commission

Network of National Coordination Centres

Research & Innovation



National Coordination Centres:

- Nominated by Member States & notified to the Commission
- Possess or have access to technological expertise in cybersecurity
- Can effectively engage and coordinate with industry, academia and the public sector
- Can receive direct grants
- Can provide financial support to third parties

European Commission

The Competence Centre – what will it do?

Research & Innovation

- Facilitate and help coordinate the work of the Network
- Implement cybersecurity parts of Digital Europe and Horizon Europe Programmes
- Enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities
- Contribute to the wide deployment of state-of-the-art cyber security products and solutions across the economy
- Contribute to reducing skills gaps in the Union related to cybersecurity
- Contribute to the reinforcement of cybersecurity research and development
- Enhance cooperation between the civilian and defence spheres with regard to dual use technologies and applications
- Enhance synergies between the civilian and defence dimensions of cybersecurity in relation to the European Defence Fund

The future digital budget

DIGITAL IN THE NEXT MFF: OVERVIEW

Digital Europe:
Capacities & roll out

1. High Performance Computing (HPC)
2. Artificial Intelligence (AI)
3. Cybersecurity
4. Advanced digital skills
5. Digital transformation and interoperability

€9.2 billion

Digital in Horizon Europe
R&D&I

1. Digital under "global challenges"
   - Digital and industry cluster
   - Digital in other clusters - health, mobility, energy, environment,..
2. FET Open under Open Innovation
3. Research Infra under Open Science

> €12 billion for digital

Connecting Europe Facility - Digital
Connectivity

- 5G roll out
- BB 4EU, Connecting communities
- Synergies with Transport /Energy

€3 billion

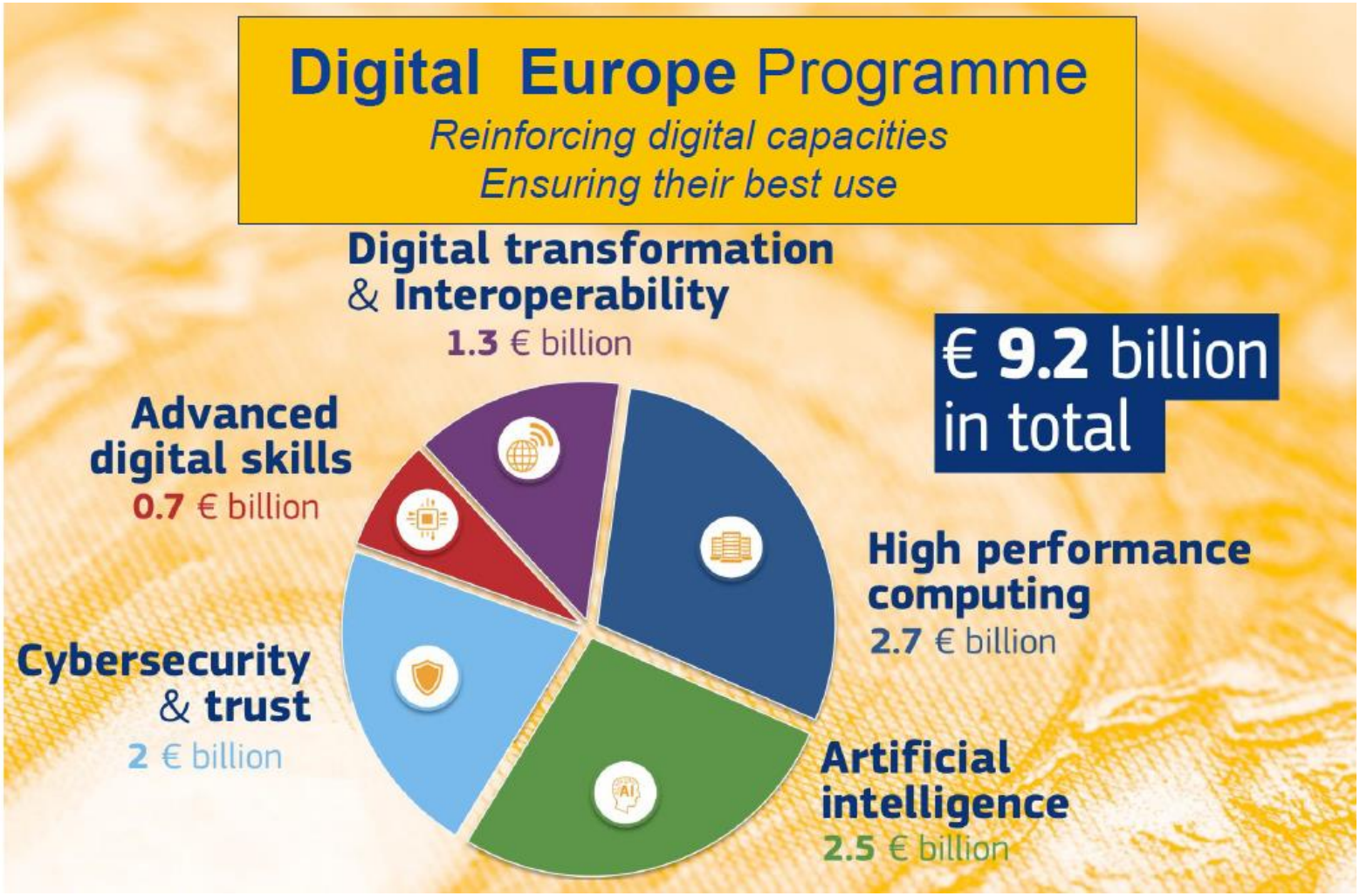
Creative Europe
MEDIA

- Distribution of works
- Creation

€1.1 billion

Policy response:

The Digital Europe Programme 2021-2027



Thank you for your attention!

florent.frederix@ec.europa.eu