



# CYBERSECURITY SKILLS CONFERENCE

20 September 2022, Athens

***“EU Cybersecurity Policy and Cyber Skills”***

*Miguel Gonzalez-Sancho, Head of Unit  
DG CNECT.H1 “Cybersecurity Technology and Capacity Building”  
EUROPEAN COMMISSION*

# Cybersecurity challenges

- Geopolitical contest over cyberspace
- Large increase in cybercrime
- Supply chain security (e.g. 5G)
- Expanding attack surface (e.g. IoT; hospitals, vaccine distribution)
- Threat from quantum computing breaking “legacy” crypto
- Advent of AI
- Skills shortage; awareness
- Capacity building, resilience
- Vulnerability of smaller organisations, SMEs
- Info sharing, joint analysis and response
- Commercialisation of R&D
- Uptake
- Single market
- Dual use
- (...)

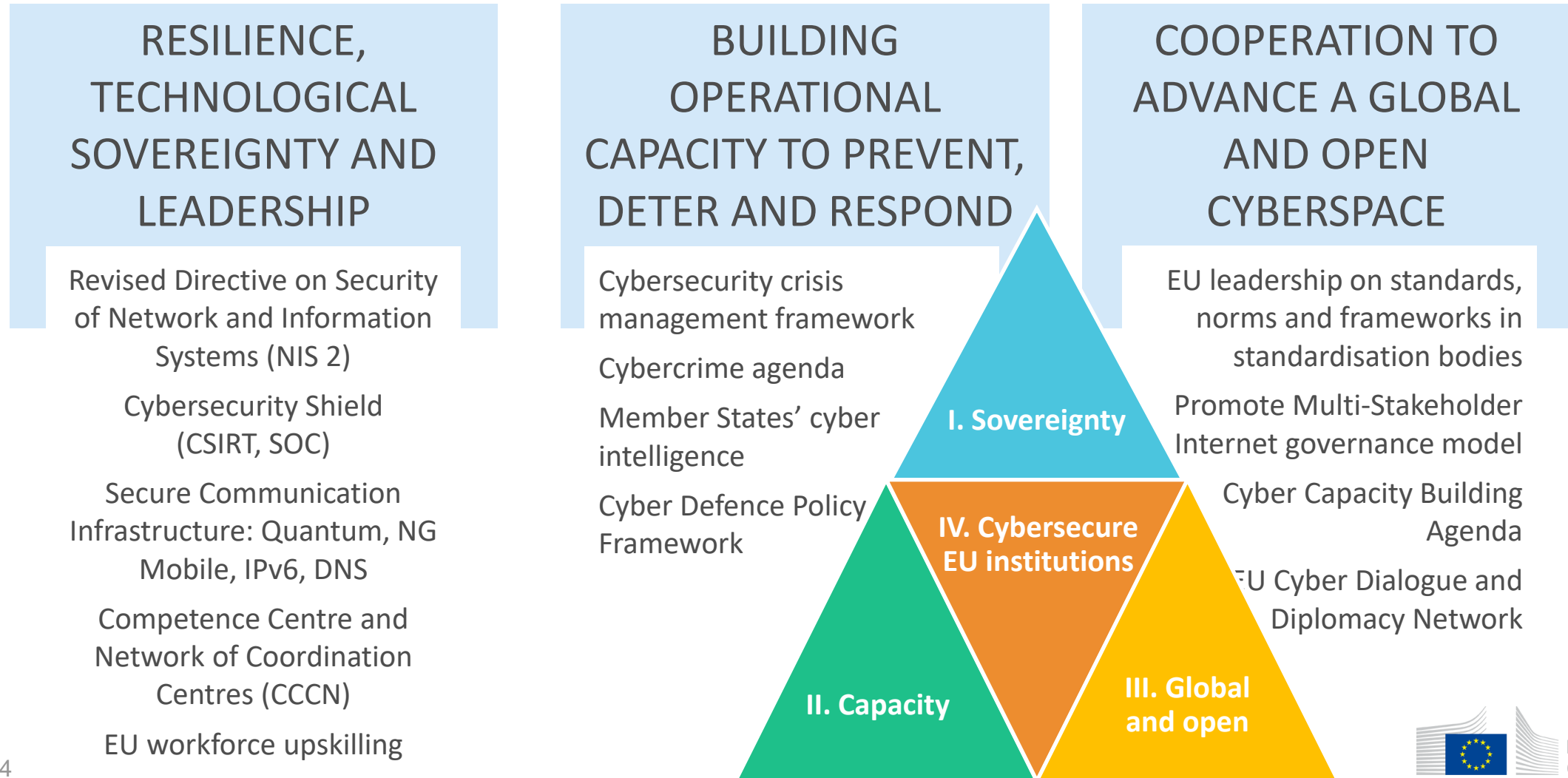
# Digital skills overview

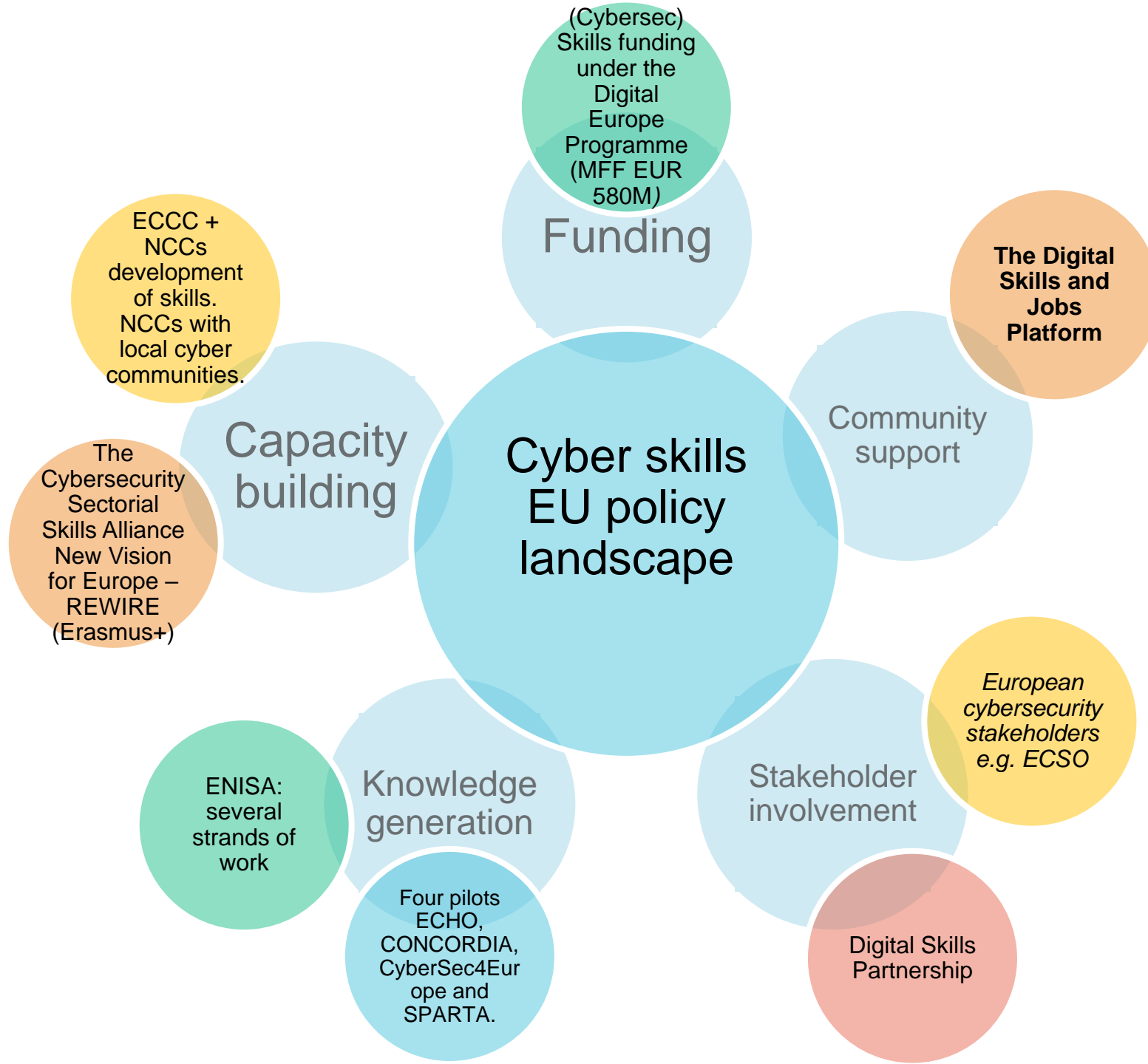
Table 1 Human capital indicators in DESI

	EU DESI 2022
<b>1a1 At least basic digital skills</b> % individuals	<b>54%</b> 2021
<b>1a2 Above basic digital skills</b> % individuals	<b>26%</b> 2021
<b>1a3 At least basic digital content creation skills</b> % individuals	<b>66%</b> 2021
<b>1b1 ICT specialists</b> % individuals in employment aged 15-74	<b>4.5%</b> 2021
<b>1b2 Female ICT specialists</b> % ICT specialists	<b>19%</b> 2021
<b>1b3 Enterprises providing ICT training</b> % enterprises	<b>20%</b> 2020
<b>1b4 ICT graduates</b> % graduates	<b>3.9%</b> 2020

Source: DESI 2022, European Commission

# The EU's Cybersecurity Strategy for the Digital Decade (16.12.2020); 3 instruments (regulatory, investment, policy initiatives) 3 to three pillars





# Funding

(Cybersec) Skills funding under the Digital Europe Programme (MFF EUR 580M)

# Community support

The Digital Skills and Jobs Platform

# Stakeholder involvement

Digital Skills Partnership

European cybersecurity stakeholders e.g. ECSO

# Capacity building

European Cybersecurity Competence Centre + National Centres development of skills. National ones work with local cyber communities.

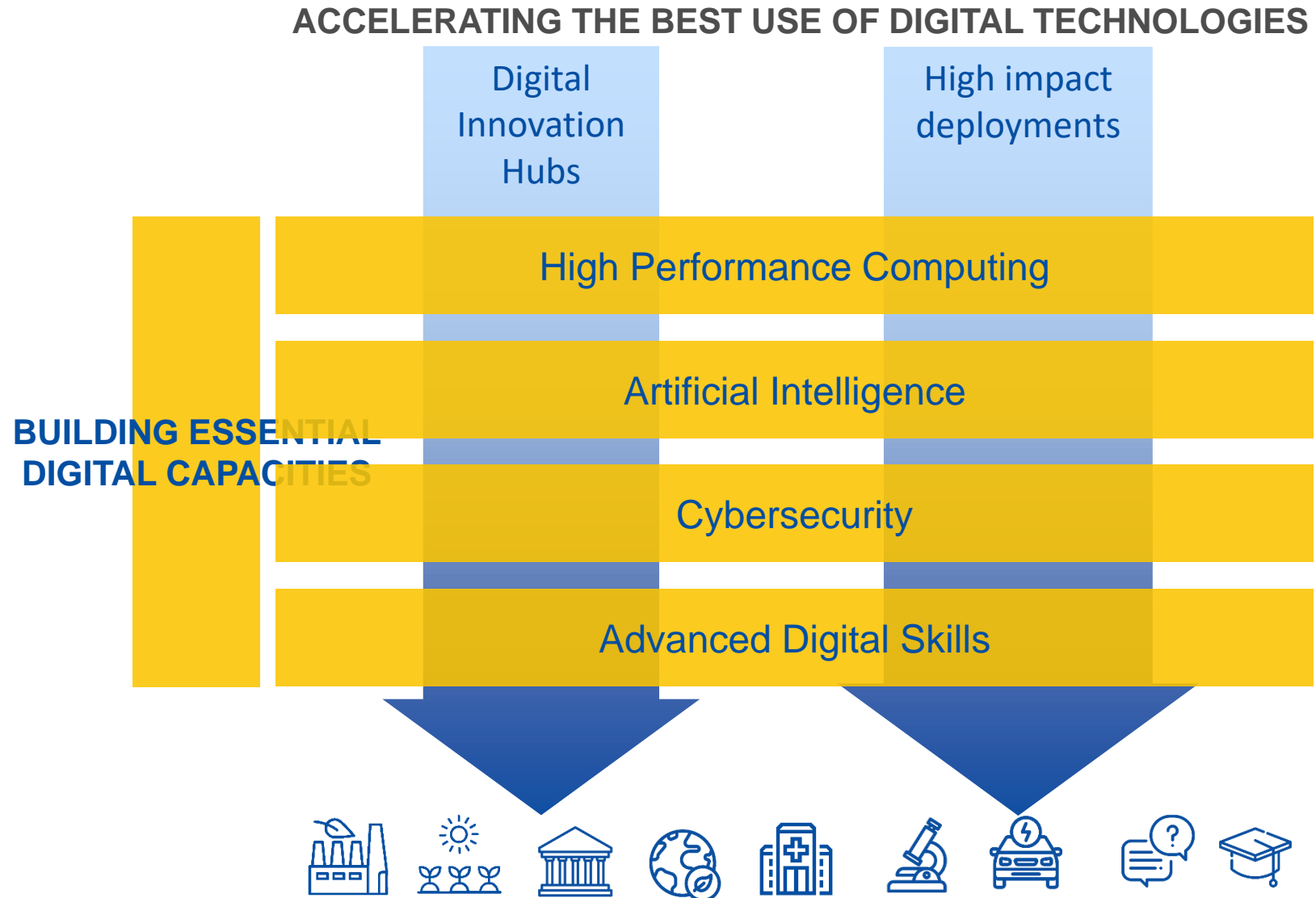
The Cybersecurity Sectorial Skills Alliance New Vision for Europe – REWIRE (Erasmus+)

# Knowledge generation

Four pilots ECHO, CONCORDIA, CyberSec4Europe and SPARTA.

ENISA: several strands of work

# Digital Europe programme structure



# Next cybersecurity call (opening 29.9.2002)

- **European Cyber-shield (169.5M)**

- EU cybersecurity resilience, coordination and Cybersecurity Ranges
- Capacity building of Security Operation Centres (SOCs)
- Securing 5G Strategic Digital Infrastructures and Technologies
- Uptake of innovative Cybersecurity Solutions
- Support To Cybersecurity In The Health Sector

- **Support to implementation of relevant EU Legislation (83M)**

- Deploying the Network of National Coordination Centres with Member States
- Cybersecurity Community support
- NIS Directive Implementation and National Cybersecurity Strategies
- Testing and Certification Capabilities



# EU Cyber Competence Centre and Network of NCCs



## 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

# Thank you



© European Union 2021

Reuse of this presentation authorised under the CC BY 4.0 license.



# Back-up slides

# Resilience, sovereignty, leadership

## Infrastructure

Adopt NIS 2.0

## Cyber Shield

Develop Network of Security Operations Centres

## Ultra secure connectivity

Quantum enabled encryption

## 5G networks

Complete implementation of Toolbox

## Internet security

Develop DNS4EU

## Supply chain autonomy

Encourage EUR 4.5 bn investment across digital supply chain through Competence Centre and Network

## Skills

Eg investment in business resilience against cyber-enabled IP theft

# Resilience, sovereignty, leadership

## Joint Cyber Unit

Milestones and process to be set out Feb 2021

## Cybercrime

Complete Security Union agenda

## Cyberdiplomacy toolbox

Strengthen cyber deterrence posture and shared situational awareness

Explore additional measures, and increase cooperation with international partners

Review Implementing Guidelines

## Cyber Defence

Review the Cyber Defence Policy Framework to increase cyber defence cooperation and coordination

Encourage Member States' cyber defence capability development, notably through PESCO and EDF

# Global and open cyberspace

## EU leadership on international norms and standards

Step-up EU engagement on international standardisation, i.e. ITU

Take forward the Programme of Action to Advance Responsible State Behaviour in Cyberspace  
Promote the Budapest Convention and engage in multilateral discussions

Promote and protect human rights and fundamental freedoms online

## Cooperation with partners

Strengthen and expand cyber dialogues with third countries, regional and international organisations

Reinforce regular and structured exchanges with the multi-stakeholder community

Form an informal EU Cyber Diplomacy Network with EU “cyber attachés” around the world to promote the EU vision of cyberspace

## Strengthen global capacities to tackle cyber threats

Develop an EU External Cyber Capacity Building Agenda

Set-up an EU External Cyber Capacity Building Agenda Board

Priorities on Western Balkans, EU’s neighborhood and partner countries experiencing a rapid digital development