European Commission

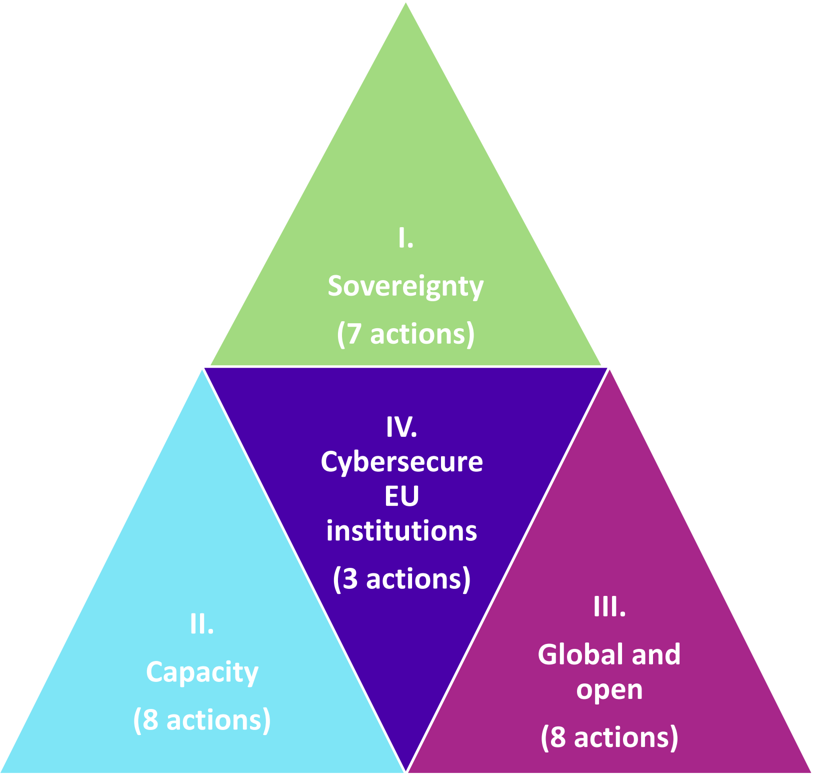
THE EU'S CYBERSECURITY STRATEGY FOR THE DIGITAL DECADE

Cyber threat landscape 2021

- Intensification of cyberattacks on **essential services**
- **Green transformation** requires secure cross-border grids, smart meters, avoiding unnecessary of data storage duplication, patchable devices
- **IoT** proliferating: 25 bn connected objects by 2025 (GSMA)
- **Pandemic dependency** on digital → expands attack surface e.g hospitals, vaccine distribution, disinformation
- **Geopolitical tensions**: authoritarian regimes weakening open, global Internet and hijack international bodies/ norm setting

The EU’s cybersecurity strategy for the digital decade December 2020

- 26 strategic initiatives/ actions
- Smart digital investment: up to €4.5bn for cybersecurity 2021-27 (EU+MS+Industry)
- New regulation (eg NIS 2.0, IoT)
- New policies (Joint Cyber Unit, Security Operations Centres)
- Comprehensive
  - ❑ internal market
  - ❑ law enforcement
  - ❑ diplomacy
  - ❑ defence



(I)

RESILIENCE, TECHNOLOGICAL SOVEREIGNTY AND LEADERSHIP

I 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

An Internet of Secure Things

- Horizontal rules on IoT security

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

Directive on security of network and information systems (NIS) 2.0

	Essential entities	Important entities
Scope	Scope of NIS1 + certain new sectors	Most new sectors + certain entities from NIS1 scope
Security requirements	Risk-based security obligations, including accountability of top management	
Reporting obligations	Significant incidents and significant cyber-threats	
Supervision	Ex-ante	Ex-post
Sanctions	Minimum list of administrative sanctions, including fines	
Jurisdiction	General rule: MS where the service is provided Exception: Main establishment + ENISA registry for certain digital infrastructures and digital providers	

(NIS) 2.0 : Who's in

Essential entities	Important entities
Energy (electricity*, district heating, oil (incl. central oil stocktaking entities), gas and hydrogen)	Postal and courier services
Transport (air, rail, water, road)	Waste management
Banking	Chemicals (manufacture, production, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)	Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, Content Delivery Networks, electronic communications and trust service providers)	
Public administration (central and regional)	
Space	

*** New types of entities in electricity:** electricity generation, electricity markets participants providing aggregation, demand response and energy storage services, nominated electricity market operators,

Horizontal cybersecurity requirements for connected products

- Growing importance of IoT in particular and increased risks in general for users of “digital” products (including standalone software) in case of cybersecurity incidents + growing stakeholders demand to address also cybersecurity risks of ICT products.

- The Commission is analysing this complex matter, further defining the issues and analysing possible solutions (with the support of an external contractor). In the course of 2021, the Commission will be engaging in various types of consultations, aiming to inform the decision making process.

(II)

BUILDING OPERATIONAL CAPACITY TO PREVENT, DETER AND RESPOND

II Operational capacity: prevent, deter, respond

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

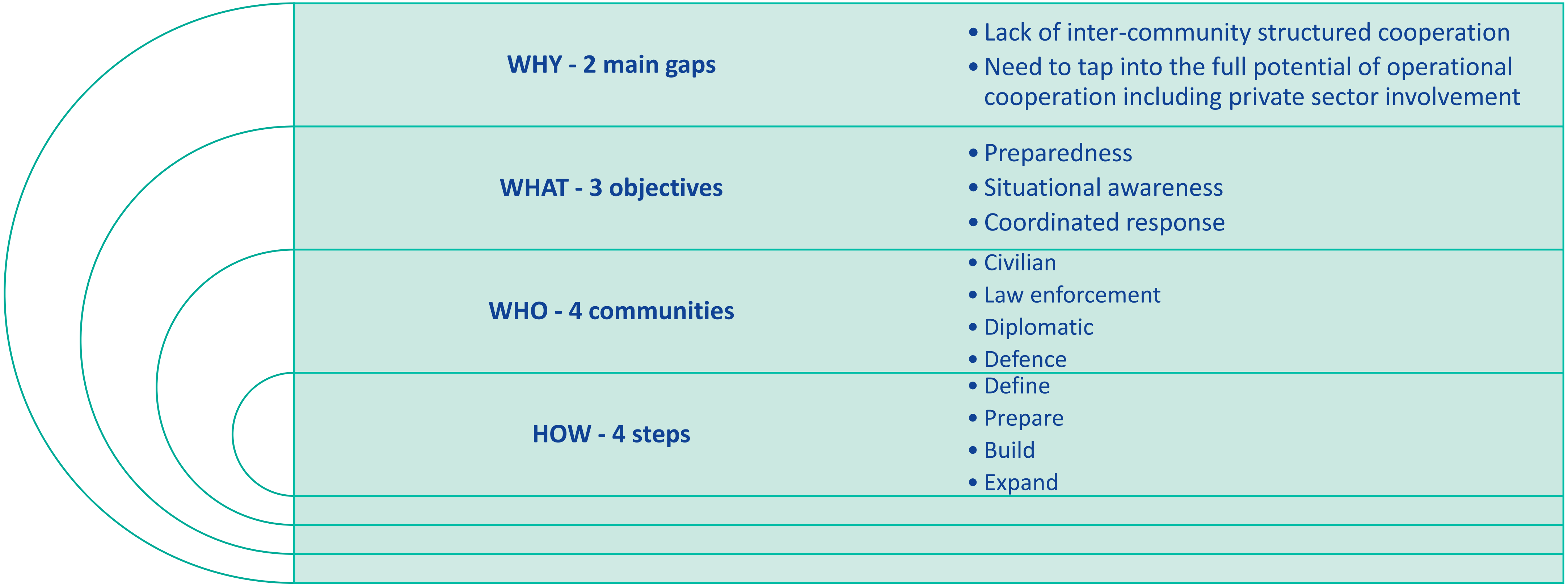
Cyber Defence

- 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

European Commission

The Joint Cyber Unit

A virtual and physical platform for cooperation for the different cybersecurity communities in the EU, with a focus on operational and technical coordination against major cross border cyber incidents and threats.



WHY - 2 main gaps	• Lack of inter-community structured cooperation • Need to tap into the full potential of operational cooperation including private sector involvement
WHAT - 3 objectives	• Preparedness • Situational awareness • Coordinated response
WHO - 4 communities	• Civilian • Law enforcement • Diplomatic • Defence
HOW - 4 steps	• Define • Prepare • Build • Expand

(III)

ADVANCING A GLOBAL AND OPEN CYBERSPACE

III 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.

The EU’s Cybersecurity Strategy for the Digital Decade: Actions (milestones)*

1. Resilience, tech sovereignty, leadership (CNECT lead)	2. Building operational capacity (CNECT, HOME, EEAS, DEFIS)	3. Advancing a global and open cyberspace (CNECT, EEAS, HOME)	4. Cybersecurity in EU institutions, bodies, agencies (HR, DIGIT)
1.1 NIS 2.0 (Common approach Q2/2021)	2.1 JCU (Mar recommendation tbc)	3.1 International standardisation objectives	4.1 Regulation on information security (proposal Q2/3 2021)
1.2 Internet of secure things (proposal on horizontal rules Q2/2022)	2.2 Cybercrime agenda (ongoing)	3.2 UN PoA for responsible state behaviour	4.2 Regulation on cybersecurity (proposal Q2/3 2021)
1.3 Investment through CCCN (MS to submit plans)	2.3 MS cyber-intelligence WG in INTCEN	3.3 Guidance on human rights in cyberspace	4.3 New legal basis for CERT-EU (as 4.2)
1.4 Network of SOCs/ Cyber Shield (in discussion with MS on use of RRF)	2.4 Cyber deterrence posture	3.4 Children’s rights (CSAM proposal Q2/2021)	
1.5 Cybersecurity support to SMEs through DIHs (ongoing)	2.5 Cyber defence framework review	3.5 Strengthen Budapest Convention (Q2/2021)	
1.6 DNS4EU resolver service (Q2/2021 call under CEF2/ pan European EU cloud federations’)	2.6 Vision/ strategy for CSDP ops	3.6 Cyber diplomacy network	
1.7 5G toolbox (Q2/2021 complete, next steps tbd)	2.7 Civil, defence, space synergies	3.7 Multistakeholder community	
	2.8 Space programme infrastructure	3.8 External cyber capacity building	

**Updated 21012021 (input awaited from EEAS). Progress monitored by CNECT with EEAS and HOME and through interservice group; regular updates to Council (HWP CI)*

**Updated 21012021 (input awaited from EEAS). Progress monitored by CNECT with EEAS and HOME and through interservice group; regular updates to Council (HWP CI)*

Cybersecurity strategy: Next steps

- ***Q1 2021*** Finalise **work programmes for DEP/ Horizon Europe**, handover to CCCN

  Discussions with MS on approach to **SOCs**, on use of **RRF for digital**/ cyber and to mainstream cybersecurity in **DIH initiative**
- ***January*** HWP CI discussions on strategy and NIS 2.0

  Develop **internal action plan** for strategic initiatives
- ***February*** COM to present process and milestones for delivering **JCU**
- ***23 March*** **Council Conclusions on strategy** to be adopted at GAC (discussion at HWP CI Jan/Feb)
- ***June*** NIS 2.0: Council Progress report/ general approach at TELECOM WG
- ***Q2/Q3 2021*** Adoption proposed cyber-/ info- security regulations for EU institutions

European Commission