Council of the European Union
General Secretariat

Brussels, 29 June 2021

WK 8637/2021 INIT

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Building the Joint Cyber Unit - Commission Recommendation and Annex

Delegations will find in Annex the presentation of the Commission Recommendation and Annex on building a Joint Cyber Unit, given by the Commission during the HWP on Cyber Issues meeting on 28 June 2021.

Building the Joint Cyber Unit

Commission Recommendation and Annex

The Joint Cyber Unit

‘Digitalisation and cyber are two sides of the same coin.

This starts with a ***different mindset: We need to move from “need to know” to “need to share”.***

We should do this ***through a joint Cyber Unit to speed up information sharing and better protect ourselves****.’*

President Von der Leyen Political Guidelines

The Joint Cyber Unit is 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.

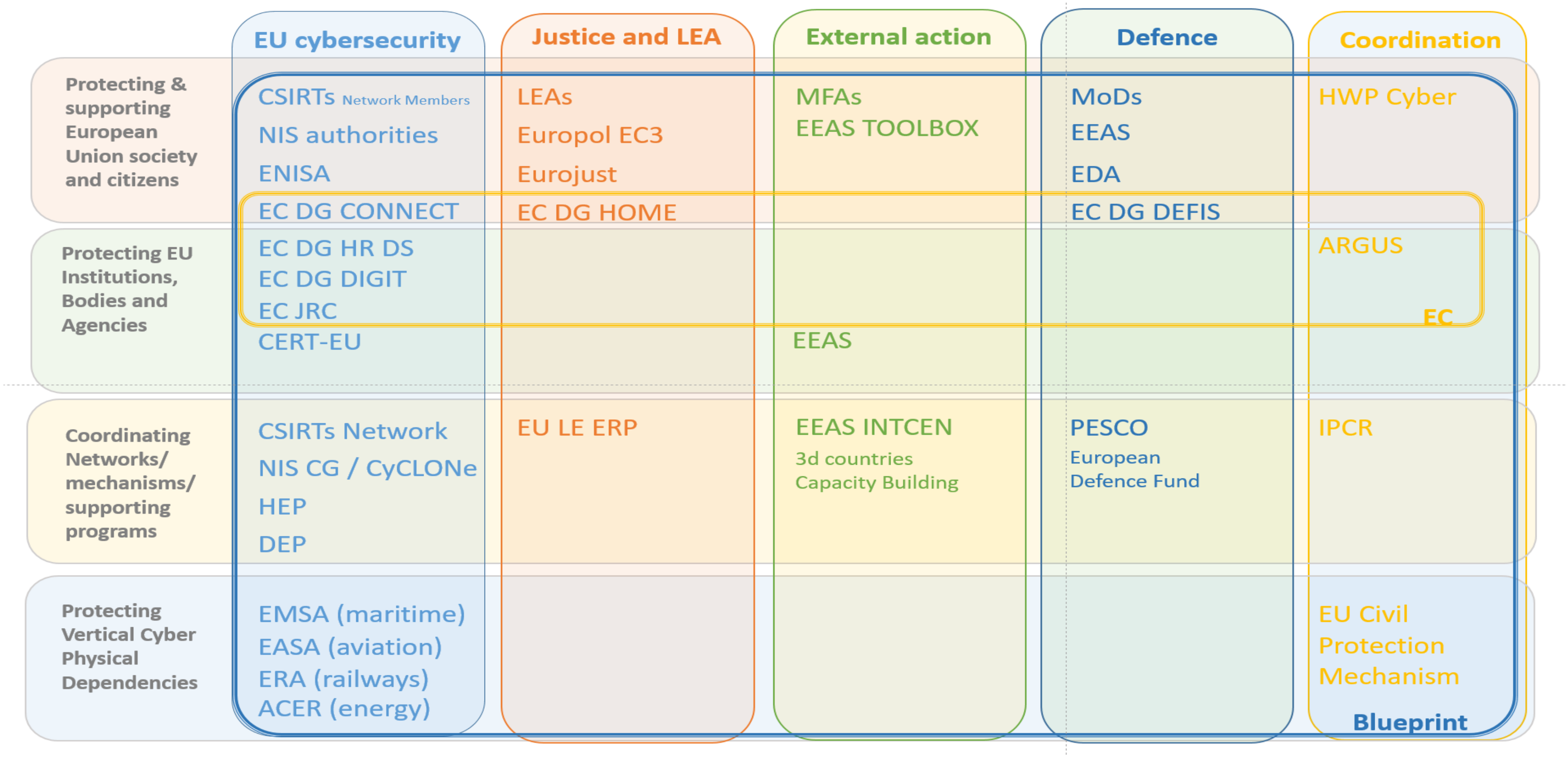
(The EU’s Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final)

European Commission

The consultation process

16 July '20	Presentation by the Commission at the HWP
Jul–Sept '20	Informal discussion paper shared by the Commission (feedback from 17 MS)
Sept -Dec '20	ENISA mapping update
29 Sept '20	Blue OLEx II - Strategic policy discussion on Joint Cyber Unit with heads of EU cybersecurity authorities
20 Dec '20	JCU section in the EU Cybersecurity strategy
Feb-Mar '21	Bilateral meetings with all Member States
23 June '21	Recommendation C(2021) 4520 final issued

EU cybersecurity communities

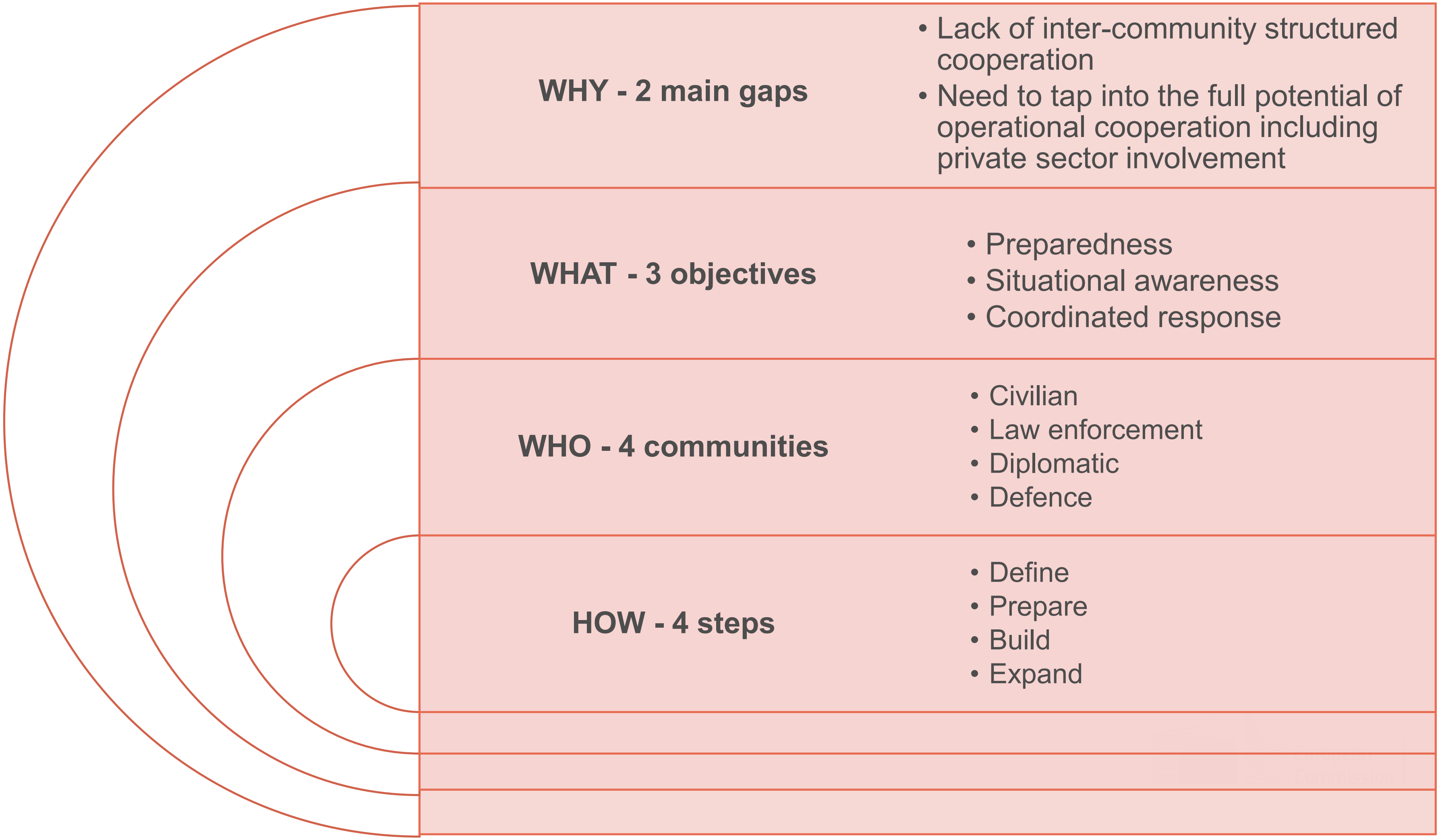


	EU cybersecurity	Justice and LEA	External action	Defence	Coordination
Protecting & supporting European Union society and citizens	CSIRTs Network Members NIS authorities ENISA EC DG CONNECT	LEAs Europol EC3 Eurojust EC DG HOME	MFAs EEAS TOOLBOX	MoDs EEAS EDA EC DG DEFIS	HWP Cyber
Protecting EU Institutions, Bodies and Agencies	EC DG HR DS EC DG DIGIT EC JRC CERT-EU		EEAS		ARGUS EC
Coordinating Networks/ mechanisms/ supporting programs	CSIRTs Network NIS CG / CyCLONe HEP DEP	EU LE ERP	EEAS INTCEN 3d countries Capacity Building	PESCO European Defence Fund	IPCR
Protecting Vertical Cyber Physical Dependencies	EMSA (maritime) EASA (aviation) ERA (railways) ACER (energy)				EU Civil Protection Mechanism Blueprint

Source: ENISA mapping

The Joint Cyber Unit - Vision

***Member States and relevant EU institutions, bodies and agencies** should ensure that, in cases of large-scale cybersecurity incidents and crises, they coordinate their efforts through a Joint Cyber Unit which enables **mutual assistance** […] The Joint Cyber Unit should also allow participants to **engage in cooperation with the private sector**.*



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

Objectives

Caveats:
- To the extent allowed by their mandates
- Take into account existing processes and the expertise of the different cybersecurity communities

*Ensure a **coordinated EU response** to and recovery from large-scale cyber incidents and crises*

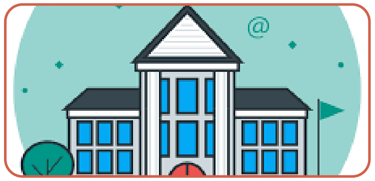
Operational participants to swiftly and effectively mobilise operational resources for mutual assistance - subject to the request from one or more Member States.

share best practices
harness continuous **shared situational awareness**
ensure necessary **preparedness**

Key elements and principles

To complete **EU Cybersecurity Crisis Response Framework (‘Blueprint’)**

- It tackles **large-scale incidents and crises** (i.e. with a significant impact in at least two Member States)
- Focuses on **technical and operational levels** (link with political ensured through the Integrated Political Crisis Response arrangements, IPCR)



It is not a new body

- **A platform** assisting participants to perform crisis management operations more effectively
- Participants contribute to the **extent allowed by their mandates** (e.g. Article 7 of Regulation 2019/881, Cyber-Act, and Article 3 of Regulation 2016/794, Europol)
- Funding provided through **DEP**

Recommendation sets out **process, milestones and timeline**

- **Four steps** over **two years**
- **Core** and **supporting actions**, depending on the objective

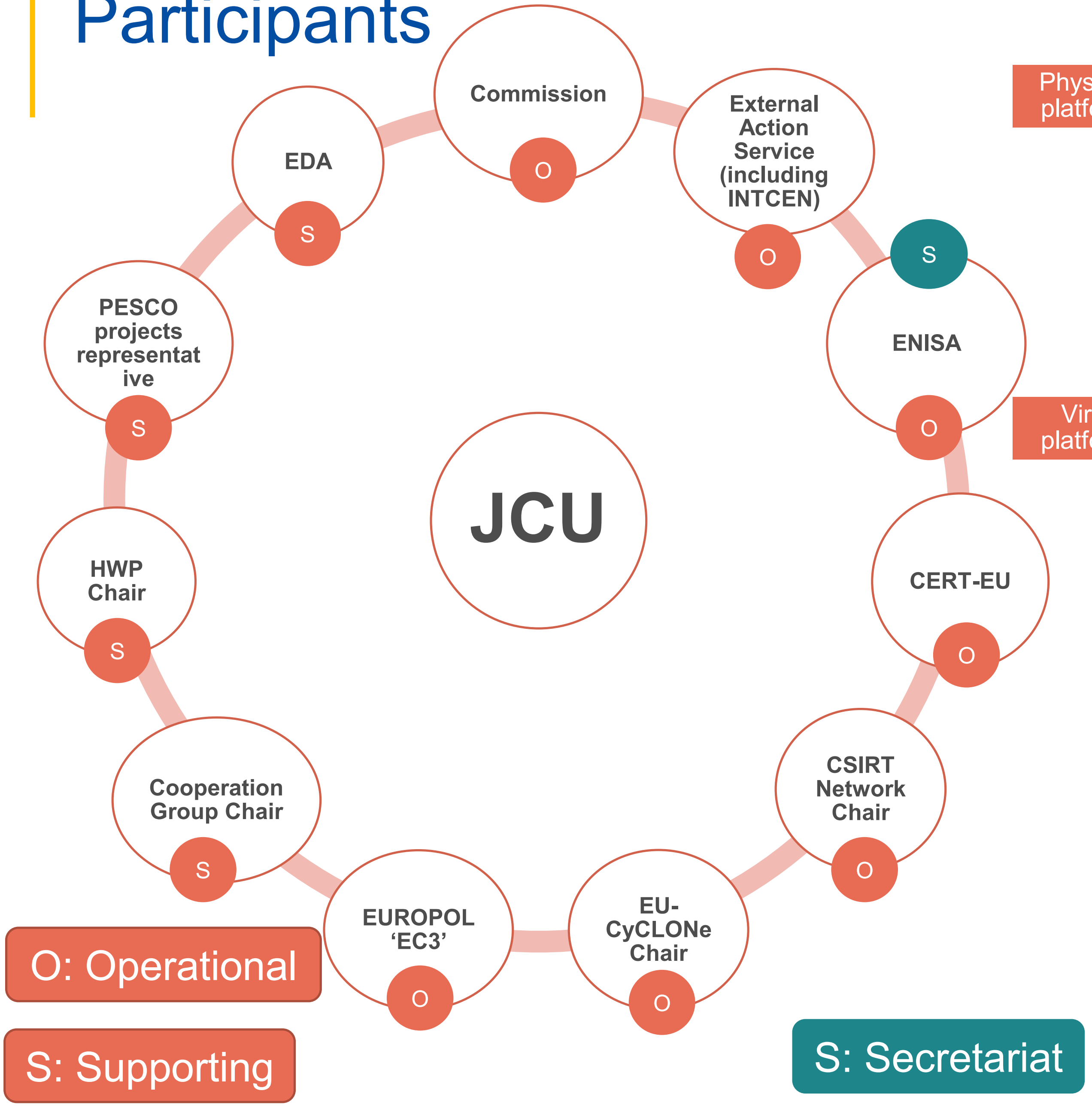
Incremental co-creation process between EUIBAs and MS

- Preparatory process to be completed by **working group** (co-chaired by EC, HR, MS representative)
- **Roles and responsibilities to be defined** based on working group assessment

Enables mutual assistance

- Coherently with NIS Directive and **Article 222 of TFEU**
- **Without prejudice to Article 42(7)** of TEU
- Cooperation and mutual assistance agreements through **Memoranda of Understanding**

Participants



JCU

Commission O

External Action Service (including INTCEN) O

ENISA S O

CERT-EU O

CSIRT Network Chair O

EU-CyCLONe Chair O

EUROPOL ‘EC3’ O

Cooperation Group Chair S

HWP Chair S

PESCO projects representative S

EDA S

O: Operational

S: Supporting

S: Secretariat

Physical platform

- Space where cybersecurity experts can, in case of need, come together to conduct joint operations, share knowledge and exercises.
- Built around **ENISA – CERT-EU adjacent Brussels office**

Virtual platform

- Composed of collaboration and secure information sharing tools
- Possible to use **existing infrastructure** (e.g. ‘SIENA’) to support the exchange of operational information, possibly including confidential material.
- Leveraging the wealth of information gathered through the **European Cyber-Shield**, notably through Security Operation Centres (‘SOCs’) and Information Sharing and Analysis Centres (‘ISACs’).

Operations
EU coordinated response

The establishment, training, testing and coordinated deployment of **EU Cybersecurity Rapid Reaction Teams**

The coordinated deployment of a **virtual and physical platform**

The creation and maintenance of an inventory **of operational and technical capabilities available in the EU** across cybersecurity communities

The reporting experience gained in **cybersecurity operational cooperation activities** within and across cybersecurity communities

Operations
Shared situational awareness and preparedness

The development of the **Integrated EU Cybersecurity Situation report**

- Building on the ENISA Technical situation report

The use secure **tools** for rapid information-sharing

The **exchange of information and expertise**

The development, management and testing of **EU Cybersecurity Incident and Crisis Response Plan**

- Based on **national plans introduced under NIS2**
- Testing through cross-community exercises and trainings

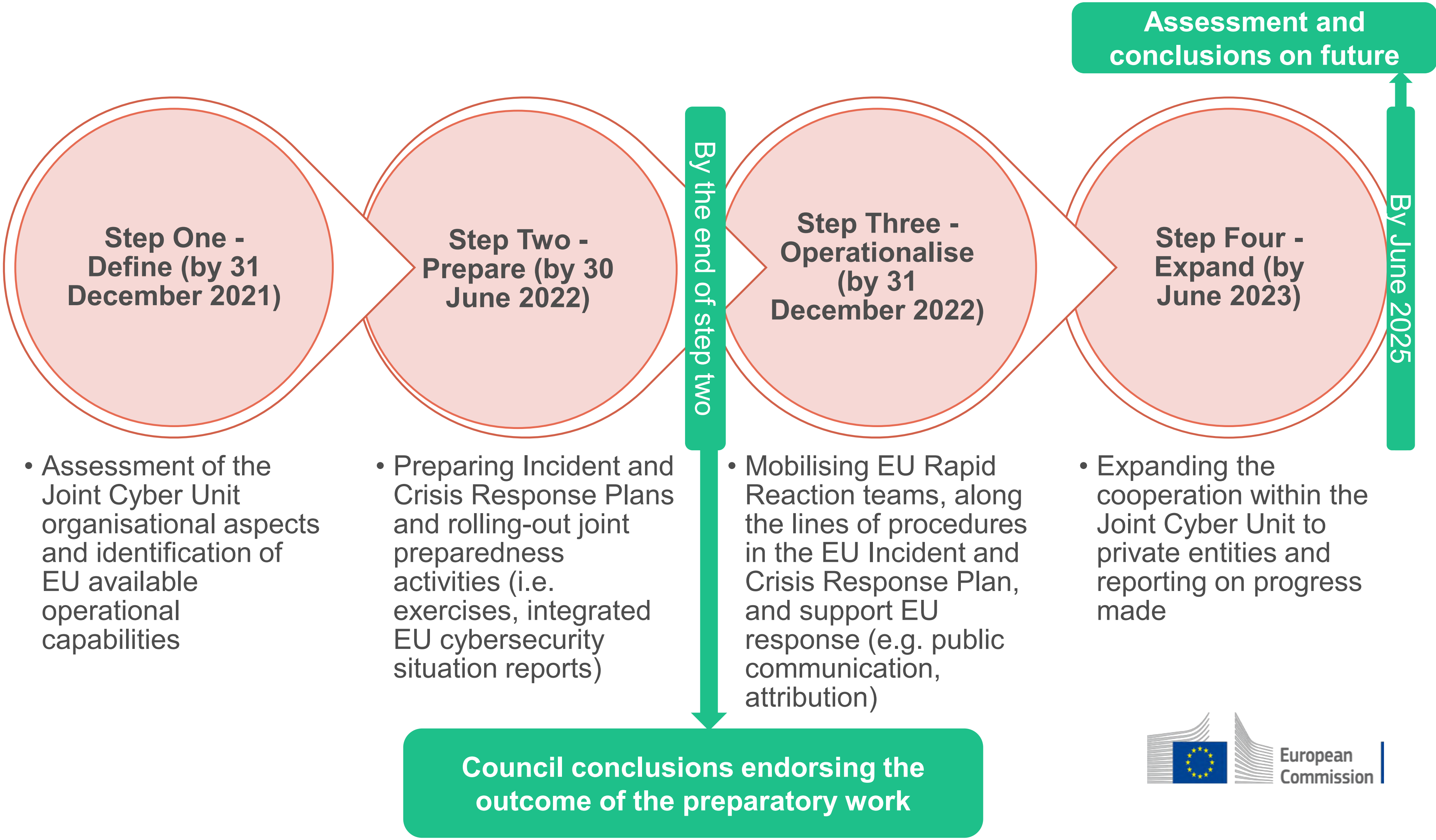
Conclusion of information-sharing and operational cooperation agreements with **private sector entities**

Synergies with national, sectoral and cross-border **monitoring and detection capabilities** (e.g. SOCs)

Assistance in crises **management**

- supporting diplomatic action (use of Cyber-diplomacy toolbox)
- political attribution as well as attribution in the context of criminal investigations
- aligning public communication and facilitating incident recovery

Steps to build the Joint Cyber Unit



Step One - Define (by 31 December 2021)

- Assessment of the Joint Cyber Unit organisational aspects and identification of EU available operational capabilities

Step Two - Prepare (by 30 June 2022)

- Preparing Incident and Crisis Response Plans and rolling-out joint preparedness activities (i.e. exercises, integrated EU cybersecurity situation reports)

By the end of step two

Council conclusions endorsing the outcome of the preparatory work

Step Three - Operationalise (by 31 December 2022)

- Mobilising EU Rapid Reaction teams, along the lines of procedures in the EU Incident and Crisis Response Plan, and support EU response (e.g. public communication, attribution)

Step Four - Expand (by June 2023)

- Expanding the cooperation within the Joint Cyber Unit to private entities and reporting on progress made

By June 2025

Assessment and conclusions on future

European Commission

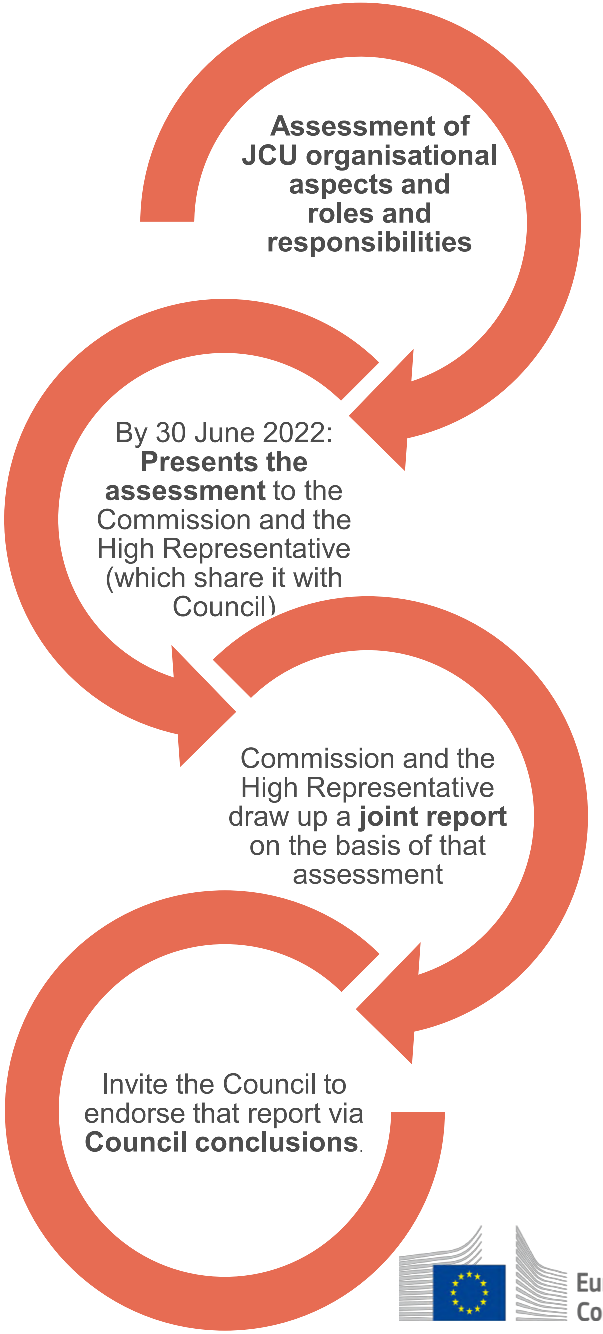
Working Group

Co-chaired by Commission High Representative Member States representative

Convened by the Commission

Composed of operational and supporting participants

Tasked with completing the preparatory work (first two steps)



Assessment of JCU organisational aspects and roles and responsibilities

By 30 June 2022: **Presents the assessment** to the Commission and the High Representative (which share it with Council)

Commission and the High Representative draw up a **joint report** on the basis of that assessment

Invite the Council to endorse that report via **Council conclusions**.

Thank you

European
Commission