European Commission

JOINT CYBER UNIT

23 June 2021

#DigitalEU
#Cybersecurity

Why do we need the Joint Cyber Unit?

The Commission proposed to build a new Joint Cyber Unit to tackle the rising number of major malicious cyber incidents impacting the life of businesses and citizens across the European Union. The Joint Cyber Unit aims to bring cybersecurity communities together in a platform to foster cooperation and to enable the existing networks to realise their full potential.

This will fill the gap that currently exists: a common space for all cybersecurity communities to work together to tackle common threats.

What is the Joint Cyber Unit?

The **Joint Cyber Unit** is a new platform that aims to strengthen cooperation among EU Institutions, Agencies, Bodies and the authorities in the Member States, for example civilian communities, law-enforcement, diplomatic and cyber defence ones, to **prevent**, **deter** and **respond** to cyberattacks. It will be built gradually and in close co-operation with Member States.

Goals of the Joint Cyber Unit

Ensure an **EU coordinated response** to large-scale cybersecurity threats, incidents and crises.

Improve **situational awareness** and communication to the general public.

Guarantee **joint preparedness**.

Role of the Joint Cyber Unit

The Joint Cyber Unit will support participants to:

Create **an inventory** of operational and technical capabilities available in the EU;

Produce **integrated EU cybersecurity situation reports**, including information and intelligence about threats and incidents;

Deliver the **EU Cybersecurity Incident and Crisis Response Plan**, based on national plans proposed in the revised NIS Directive (NIS2);

Conclude **memoranda of understanding** for cooperation and mutual assistance;

Establish and mobilise EU **Cybersecurity Rapid Reaction Teams**;

Share information and conclude operational cooperation agreements with private sector companies.

How the Joint Cyber Unit will work

A **physical platform** – a physical space where cybersecurity experts can, in case of need, come together to conduct joint operations, share knowledge and work together.

A **virtual platform** for collaboration and secure information sharing, leveraging the wealth of information gathered through monitoring and detection capabilities (European Cyber Shield).

It will work on two levels:

1. technical

2. operational

The Joint Cyber Unit will be physically located next to the Brussels office of the EU Agency for Cybersecurity (ENISA) and the Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU).

Timeline

With the Joint Cyber Unit, the relevant EU institutions, bodies and agencies together with the Member States will build a European framework for solidarity and assistance to counter large-scale cyberattacks. The Commission has proposed to build the Unit through a **gradual and transparent process in 4 steps**:

by 31 December 2021

1. Assess the organisational aspects and identify EU operational capabilities.

by 30 June 2022

2. Prepare national incident and crisis response plans and roll out joint preparedness activities.

Based on the results of the assessments carried out by the participants of the JCU, the Commission and the High Representative will **draw up a report on the roles and responsibilities** of participants within the Joint Cyber Unit, to be transmitted to the Council of the European Union for endorsement.

by 31 December 2022

3. Operationalise the Joint Cyber Unit by mobilising EU Rapid Reaction teams, along the lines of procedures defined in the EU Incident and Crisis Response Plan.

by June 2023

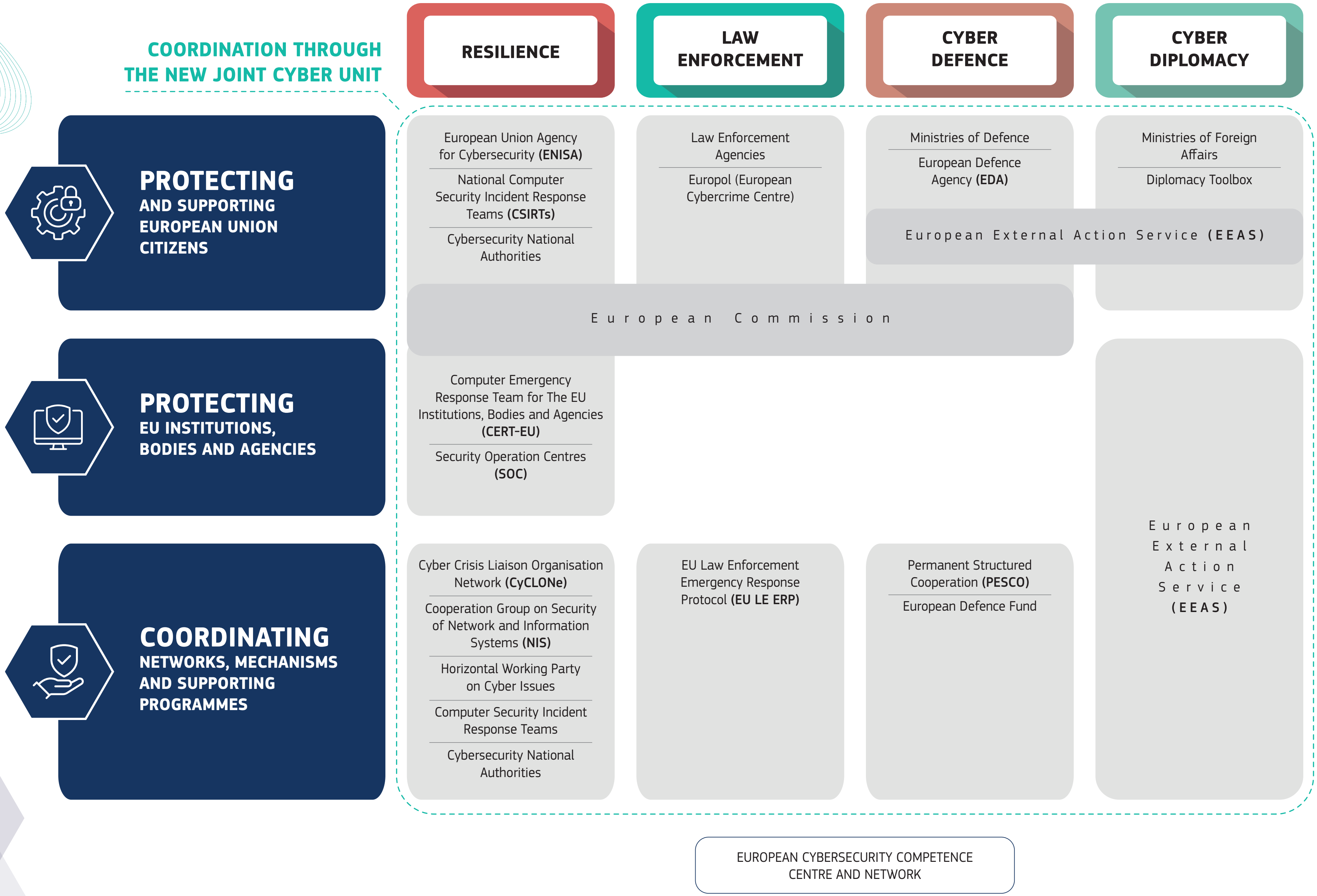
4. Involve private sector partners, users and providers of cybersecurity solutions and services, to increase information sharing and to be able to escalate EU coordinated response to cyber threats.

Publications Office
of the European Union

BOOK KK-03-21-298-EN-C ISBN 978-92-76-39111-1 doi:10.2759/886652
PDF KK-03-21-298-EN-N ISBN 978-92-76-39110-4 doi:10.2759/32126

Updated 2021-03-22

EU CYBERSECURITY ECOSYSTEM



COORDINATION THROUGH THE NEW JOINT CYBER UNIT

	RESILIENCE	LAW ENFORCEMENT	CYBER DEFENCE	CYBER DIPLOMACY
PROTECTING AND SUPPORTING EUROPEAN UNION CITIZENS	European Union Agency for Cybersecurity **(ENISA)** National Computer Security Incident Response Teams **(CSIRTs)** Cybersecurity National Authorities	Law Enforcement Agencies Europol (European Cybercrime Centre)	Ministries of Defence European Defence Agency **(EDA)**	Ministries of Foreign Affairs Diplomacy Toolbox
			European External Action Service **(EEAS)**	
	European Commission			
PROTECTING EU INSTITUTIONS, BODIES AND AGENCIES	Computer Emergency Response Team for The EU Institutions, Bodies and Agencies **(CERT-EU)** Security Operation Centres **(SOC)**			European External Action Service **(EEAS)**
COORDINATING NETWORKS, MECHANISMS AND SUPPORTING PROGRAMMES	Cyber Crisis Liaison Organisation Network **(CyCLONe)** Cooperation Group on Security of Network and Information Systems **(NIS)** Horizontal Working Party on Cyber Issues Computer Security Incident Response Teams Cybersecurity National Authorities	EU Law Enforcement Emergency Response Protocol **(EU LE ERP)**	Permanent Structured Cooperation **(PESCO)** European Defence Fund	

EUROPEAN CYBERSECURITY COMPETENCE CENTRE AND NETWORK

MAIN ACTORS AND NETWORKS OF COOPERATION INVOLVED IN THE JOINT CYBER UNIT

Resilience

European Union Agency for Cybersecurity (ENISA)

A centre of expertise on cybersecurity in the EU: it contributes, among other tasks, to operational cooperation in the Union, capacity building, awareness raising and education.

Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU)

Composed of IT security experts from the main EU Institutions.

National Computer Security Incident Response Teams (CSIRTs)

Composed of technical cybersecurity experts from EU Member States' appointed CSIRTs and CERT-EU: it promotes swift and effective cooperation.

EU Cyber Crisis Liaison Organisation Network (CyCLONe)

Composed of crisis management operational experts from Member States: it ensures that information effectively flows from technical level to political decision-makers.

Cooperation Group on Security of Network and Information Systems

Composed of representatives of Member States, the Commission, and the ENISA: it facilitates strategic cooperation on cybersecurity policies in the EU.

Security Operation Centres (SOC)

An information security team that monitors, analyses and addresses cybersecurity incidents and risks of an organisation, whether public or private. It combines human and technology resources and procedures. SOCs often closely cooperate with computer emergency response teams to ensure that cybersecurity incidents are addressed effectively.

Law enforcement

The European Cybercrime Centre ('EC3')

Established under Europol, it includes the Joint Cyber Crime Taskforce ('J-CAT') and acts as the focal point in the fight against cybercrime in the Union.

Diplomacy

European External Action Service (EEAS)

Contributes to the promotion and protection of a global, open, stable and secure cyberspace. Through the "Cyber Diplomacy Toolbox" provides support in using the full range of diplomatic measures, notably as regards public communication, supporting shared situational awareness and engagement with third countries in the event of a crisis.

Horizontal Working Party on Cyber Issues

A forum that discusses, among other topics, the use of measures under the Cyber Diplomacy Toolbox: a framework for a joint EU diplomatic response to malicious cyber activities.

Defence

Permanent Structured Cooperation (PESCO)

A framework and a process to deepen defence cooperation, including on cybersecurity, between those EU Member States who are capable and willing to do so.

European Defence Agency (EDA)

It supports Member States in developing their cyber defence capabilities, defined as the ability to detect, withstand and recover from any cyberattack; supports Member States in defining EU-level priorities for cyber defence, leveraging also synergies with other EU cyber-related efforts.