Cybersecurity actors in the EU

Cyberattack numbers have surged in recent years, leading to the formation of entities at all levels to prevent attacks or mitigate the harm they may cause. An efficient EU-level response requires coordination and the timely exchange of information. Several bodies and networks have been set up to this end; this paper explains their respective roles.

Introduction

Nowadays, cybersecurity is embedded in public and private sector organisations to protect their vital interests and offer strategies to mitigate possible cyberattacks. Whereas national security, including cybersecurity, remains a national government prerogative, the potential cross-border impact of cyber incidents implies the need for cooperation and a common EU response. This need is increasingly reflected in EU legal acts defining new entities – at both EU and national level – to analyse threats and respond to cyber incidents. On top of that, Member States have been taking their own initiatives for cooperation at supranational level, both inside the EU and beyond (for instance within the North Atlantic Treaty Organisation (NATO) and the Organisation for Security and Co-operation in Europe (OSCE), and bilaterally, for example with the US). In view of the extent and speed of these legislative and organisational developments, this publication outlines the main actors at EU level and illustrates the complexity of the EU cyber landscape.

European Commission agencies and bodies

Several agencies are working with the European Commission and its directorates-general to build up EU cybersecurity capabilities and cooperation. Since 2004, the EU has had a dedicated agency for cybersecurity (**ENISA**). ENISA was strengthened by the EU cybersecurity act, which gave it a permanent mandate, more responsibilities and more resources to improve its ability to help achieve a high common level of cybersecurity across Europe. The agency's role is to support and ensure a framework for operational cooperation, in particular in preparation for significant cross-border cyberattacks, to assist Member States with ad hoc cybersecurity-related issues, and to implement the relevant legislation. A number of EU legislative acts that are currently pending – such as the cyber resilience act –will enhance ENISA's role and give the agency new responsibilities.

The European Cybersecurity Competence Centre (**ECCC**), established in 2021, is responsible for EU cybersecurity capacity building and competitiveness. The centre, which became operational in May 2023, aims to improve technological sovereignty through strategic cybersecurity investments; it works together with the network of national coordination centres. Its work is powered by artificial intelligence and complemented by the EU supercomputing infrastructure developed under the European high-performance computing joint undertaking.

CERT-EU is the computer security incident response team for all the EU institutions, bodies and agencies. It was set up in 2011 and formally established through an interinstitutional agreement in 2018. CERT-EU's role is to prevent, detect, mitigate and respond to cyberattacks against EU institutions, bodies and agencies. It also serves as a hub for cybersecurity information exchange for its constituents.

The European Cybercrime Centre (**EC3**) was set up by Europol in 2013 to strengthen the law enforcement response to cybercrime in the EU. Since its establishment, it has helped to fight cybercrime and thus protect European citizens, businesses and governments.

Structured cooperation between Member States: European cyber networks

The directive on measures for a high common level of security of network and information systems across the Union (referred to as the NIS Directive) established the **Network and Information Systems (NIS) Cooperation Group** to ensure strategic cooperation and information exchange between Member States and contribute to the development of trust and confidence. The group is composed of representatives of

Author: Polona Car, Members' Research Service

PE 757.594 – January 2024

the Member States, the European Commission and ENISA. Among other things, it carries out coordinated security risk assessments of critical supply chains, discusses cases and requests from Member States for mutual assistance, provides strategic guidance for the activities of the computer security incident response teams (CSIRTs) Network and the European Cyber Crises Liaison Organisation Network (EU-CyCLONe), and provides guidance and exchanges information and best practices on issues falling within its remit.

The NIS Directive established (and the NIS2 Directive later strengthened) the **CSIRTs Network** to promote effective operational cooperation on specific cybersecurity incidents and the sharing of information on cybersecurity risks. The network is composed of Member State-appointed CSIRTs, CERT-EU, and the European Commission as an observer, with ENISA providing the secretariat and support as needed.

The NIS2 Directive formally established **EU-CyCLONe**, which was launched in 2020. EU-CyCLONe is a cooperation network for Member States' national authorities in charge of cyber crisis management. Supported by ENISA, the network aims to collaborate and develop timely information sharing and situational awareness, and to intervene in the event of large-scale cybersecurity incidents and crises; it supports the coordination and management and assesses the impacts of such incidents. As such, it provides a bridge between the technical (in the form of the CSIRTs Network) and political levels, which is tested through regular exercises. It cooperates with the CSIRTs Network on the basis of procedural agreements.

The prosecution of cyber criminals and enforcement of cyber legislation is crucial in the fight against cybercrime. Therefore, the European Judicial Cybercrime Network (**EJCN**) was established in 2016 to promote cooperation among cybercrime professionals and contribute to swifter prosecution of cybercrime offences. On the enforcement side, the European Union Cybercrime Task Force (**EUCTF**) was established in 2010 within Europol. EUCTF is a network – composed of the heads of Member States' national cybercrime units and representatives from Europol, the Commission, the EU Agency for Criminal Justice Cooperation (Eurojust) and the EU Agency for Law Enforcement Training (CEPOL). It provides a forum in which to identify, discuss and prioritise the key challenges and actions in the fight against cybercrime. Detection and prevention of any form of cybercrime is its first objective.

Council and European External Action Service (EEAS) tools and defence cooperation

As the EU's diplomatic service, the **EEAS** steers the EU's cyber diplomacy and strategic communication. The Strategic Compass provides a plan of action for strengthening the EU's security and defence policy by 2030. In 2022, the High Representative, in line with the objectives of the Strategic Compass, established the EEAS crisis response centre (**CRC**) as a permanent crisis response capability and the single entry point on all crisis-related issues in the EEAS. The CRC brings together diplomatic, security and intelligence capabilities to increase the EU's capability to respond to security and consular crises abroad.

The Council has several information sharing and coordination bodies. These include the **Horizontal Working Party on Cyber Issues**, which coordinates the Council's cyber policy and legislative activities. In the event of a major incident, however, a fast and collective response is crucial to reassure citizens and international partners. The Integrated Political Crisis Response Mechanism (**IPCR**) provides the necessary protocols and procedures for rapid and coordinated decision-making by the EU and is the Council Presidencies' tool to coordinate the political response to major crises. The IPCR works in close cooperation with the EEAS CRC to ensure a coherent and coordinated EU approach and response to crises. The cyber diplomacy toolbox provides a framework for a joint EU diplomatic response to malicious cyber activities and a legal framework for sanctions against cyberattacks. The revised implementing guidelines of the cyber diplomacy toolbox define the practical implementation of the toolbox in a step-by-step process.

Today, cyber threats are just as threatening to national security as physical ones. It goes without saying that the defence community has intensified its efforts to fight them, and the European Defence Agency (**EDA**) supports Member States in developing cyber resilience. In 2017, the Council established a framework for permanent structured cooperation (**PESCO**) to boost **cooperation on defence** among participating Member States. The EDA and EEAS are both part of the PESCO secretariat. Countries participating in PESCO have established several projects dedicated to cyber defence: cyber rapid response teams (CRRTs), the Cyber Ranges Federation (CRF) and the Cyber Threats and Incident Response Information Sharing Platform (CTIRISP), to name just a few. Projects include a varying number of Member States that participate in PESCO, and are coordinated by one or more of these countries.

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.