

Legal and cooperation frameworks between CSIRTs and law enforcement agencies

 vanimpe.eu/2021/08/08/legal-and-cooperation-frameworks-between-csirts-and-law-enforcement-agencies/

August 8, 2021

For a recent assignment, I had to summarise some of the legislation and cooperation frameworks that exist between CSIRTs and law enforcement agencies. This list is certainly not complete but already gives you an overview of what's available. I first list the **frameworks** and then provide an overview of some of the existing **cooperation mechanisms**.

Legal Frameworks



Council of Europe Convention on Cybercrime (Budapest, ETS No 185)

2001 – International

This convention, also known as the **Budapest Convention** is the first international treaty to address Internet and computer crime. The treaty focused on harmonising laws and increasing cooperation across borders so that cybercrime could be prosecuted in the countries affected. The treaty had three main objectives

- harmonising national laws that dealt with cyber-related crime;
- supporting the investigation of cyber-related crimes;
- increase the international cooperation in the fight against cybercrime.

Full text can be found at coe.int.

Directive on attacks against information systems (2013/40)

2013 – Europe

This directive imposes new obligations, tasks and expectations on certain key stakeholders, including CERTs/CSIRTs, LEAs, security specialists, telecommunications service providers. These relate mainly to the operation of the existing 24/7 contact points (introducing a

response deadline obligation within 8 hours), improving criminal justice/police cooperation, and the obligation to strengthen statistical data collection in order to support accountability and rational policy making.

The Directive is well known because it establishes the criminalisation of certain tools for committing offenses

This is a directive, which needs to be transposed into national law in all individual member states of Europe.

Full text can be found at eur-lex.europa.

Directive on processing personal data for prevention, investigation, detection or prosecution of criminal offences (2016/680)

2016 – Europe

This directive regulates the processing of data by police and criminal justice authorities in the EU. The Directive requires the data collected by law enforcement authorities to be processed lawfully and fairly, collected for specified, explicit and legitimate purposes. The data can also only be kept in a form that allows identification of the individual for no longer than is necessary. The Directive requires that the law enforcement authorities make a clear distinction between the data of different categories of persons.

This is a directive, which needs to be transposed into national law in all individual member states of Europe.

Full text can be found at eur-lex.europa.

General Data Protection Regulation – GDPR (2016/679)

2016 – Europe

The GDPR is the privacy data law that is designed to harmonise and update data protection requirements in the European Union. The primary objectives of the GDPR are to give control of personal data to EU citizens and residents. GDPR also simplifies the regulatory environment for international business within the EU.

Contrary to a directive, a regulation does not need to be transposed into national law, it immediately applies.

Full text can be found at eur-lex.europa.

Directive on Security of Network and Information Systems – NIS (2016/1148)

2016 – Europe

The EU's NIS Directive (Directive on security of network and information systems) is the first piece of EU-wide cyber security legislation. It aims to achieve a high common level of network and information system security across the EU's critical infrastructure. It sets a range of network and information security requirements which apply to operators of essential services and digital service providers (DSPs).

This is a directive, which needs to be transposed into national law in all individual member states of Europe.

Full text can be found at [eur-lex.europa](https://eur-lex.europa.eu).

EU's Cybersecurity Strategy for the Digital Decade (JOIN/2020/18)

2020 – Europe

The EU Cybersecurity Strategy focusses on building the operational capacity to prevent, deter and respond to cyber incidents. One of the major focal points to increase the operational capacity is to establish a Joint Cyber Unit (JCU) to speed up information sharing between different cybersecurity communities in the EU. It also focusses on increased cooperation and strengthening collective capabilities to respond to major cyberattacks.

Full text can be found at [eur-lex.europa](https://eur-lex.europa.eu).

Cooperation Mechanisms



CSIRTs Network (CNW)

The CSIRTs Network is a network composed of EU Member States' appointed CSIRTs and CERT-EU. The European Commission participates in the network as an observer. ENISA is tasked to actively support the CSIRTs cooperation, provide the secretariat and active support for incident coordination upon request. The CSIRTs Network provides a forum where members can cooperate, exchange information and build trust. Members will be able to improve the handling of cross-border incidents and even discuss how to respond in a coordinated manner to specific incidents.

European Union Cybercrime Task Force (EUCTF)

The EUCTF is a trust based network which meets twice yearly at Europol and provides a forum for the heads of the EU cybercrime units and associated countries (Denmark, Iceland, Norway and Switzerland), together with EUROPOL, CEPOL, EUROJUST and DG HOME to identify, discuss and prioritise the key challenges and actions in the fight against cybercrime. The mission statement of EUCTF is to develop and promote a harmonised approach within the European Union to the criminal misuse of information and communication technology and the fight against cybercrime.

Joint Cybercrime Action Taskforce (J-CAT)

The Joint Cybercrime Action Taskforce (J-CAT), launched in September 2014 helps fighting cybercrime within and outside the EU. J-CAT's objective is to drive intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the joint identification, prioritisation, preparation, initiation and execution of cross-border investigations and operations by its partners. It consists of 9 EU Member States, 7 non-EU partner countries and Europol.

European Judicial Cybercrime Network (EJCN)

The European Judicial Cybercrime Network (EJCN) was established in 2016 to foster contacts between practitioners specialised in countering the challenges posed by cybercrime, cyber-enabled crime and investigations in cyberspace, and to increase the efficiency of investigations and prosecutions. Eurojust is a key partner of the EJCN, especially in situations in which the Network deals with the numerous challenges related to the genuinely borderless nature of cybercrime.

24/7 Points of Contact Network

This network was constructed under the Council of Europe Convention on Cybercrime

Joint Cyber Unit

The JCU is part of the new EU Cybersecurity Strategy and has as goal to speed up information sharing between different cybersecurity communities in the EU.