EUROPEAN UNION AGENCY
FOR CYBERSECURITY

2020 REPORT ON CSIRT-LE COOPERATION

A study of the roles and synergies among selected EU Member States/EFTA countries

JANUARY 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and) EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

Contact

For queries about this paper, please email CSIRT-LE-cooperation@enisa.europa.eu
For media enquiries about this paper, please email press@enisa.europa.eu

Authors (in alphabetical order by surname)

Philip Anderson, François Beauvois, Sandra Blanco Bouza, Smaragda Karkala (ENISA), Gregoire Kourtis, Alexandra Michota (ENISA), Andreas Mitrakas (ENISA), Catalin Patrascu, Silvia Portesi (ENISA), Václav Stupka.

Acknowledgements

ENISA would like to thank the following people and organisations:

- The following subject matter experts, selected from the List of Network and Information Security (NIS) Experts compiled following the ENISA Call for Expressions of Interest (CEI) (ref. ENISA M-CEI-17-C01):
  - Philip Anderson, François Beauvois, Sandra Blanco Bouza, Catalin Patrascu and Václav Stupka, who, together with the ENISA project team, collected the data and drafted the report;
  - Maria Bada, who provided input to the development of the methodology and the desk research;
  - Silvia Signorato and Koen Van Impe, who contributed as reviewers.

- The subject matter experts/organisations who took the time to be interviewed and who provided valuable data for this report, including but not limited to:
  - Alexandre Dulaunoy, CIRCL.LU, Luxembourg;
  - Beng Hägglund, CERT-SE, Sweden;
  - Catalin Zetu, Central Cybercrime Unit, Romanian Police, Romania;
  - Dan Cimpean, CERT-RO, Romania;
  - François-Xavier Masson, French Cybercrime Unit, France;
  - Gabriel Ene, CERT-RO, Romania;
  - Jacques Martinon, Mission for the Prevention and Fighting of Cybercrime, Ministry of Justice, France;
  - Magnus Rødseth, National Criminal Investigation Service, National Cybercrime Centre, Norway;
  - Markus Hartmann, Central Cybercrime Department, Germany;
  - Nelu Munteanu, CERT-RO, Romania;

- Øystein Andreassen, National Criminal Investigation Service, National Cybercrime Centre, Norway;
- Pedro Verdelho, Prosecution Service, Portugal;
- Robert Fleckhammer, Directorate for Investigating Organised Crime and Terrorism, Romania;
- Robert Jonsson, CERT-SE, Sweden;
- Rogerio Bravo, Department of Digital Investigations, Cyber-attacks and Serious Crimes, Criminal Police of Portugal, Portugal;
- Rogerio Gil Raposo, CERT-PT, Portugal;
- Tomáš Foldyna, Prosecutor General's Office, Czechia;
- Section BL 23 – IT Security and Law, Federal Office for Information Security (BSI), Germany;
- Section OC 24 – CERT-Bund, BSI, Germany;
- additional experts from computer security incident response teams (CSIRTs), law enforcement agencies and/or the judiciary communities from Czechia, France, Germany and Sweden who also provided input.

- All of the subject matter experts/organisations who, in addition to ENISA and two CEI experts, peer reviewed the report or parts of the report, including:
  - Eric Romang, GOVCERT.LU, Luxembourg;
  - Europol's European Cybercrime Centre (EC3);
  - Iulian Alecu, CERT-RO, Romania;
  - Tomáš Minárik, National Cyber and Information Security Agency, Czechia;
- Gregoire Kourtis, who provided input to the drafting of the report and graphical representations;
- The ENISA colleagues who provided input and reviewed the report, in particular Andrea Dufkova and Jo De Muynck.

Legal notice

Copyright notice

ISBN: 978-92-9204-404-6
DOI: 10.2824/786524

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The purpose of this report is to further explore and support the cooperation between computer security incident response teams (CSIRTs), in particular national and governmental (n/g) CSIRTs, and law enforcement agencies (LEAs) and their interactions with the judiciary (prosecutors and judges).

This report follows a number of previous reports published by the European Union Agency for Cybersecurity (ENISA), including *Tools and methodologies to support cooperation between CSIRTs and law enforcement* (ENISA, 2017), *Improving cooperation between CSIRTs and law enforcement: legal and organisational aspects*, *Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary* (ENISA, 2017a), *An Overview on Enhancing Technical Cooperation between CSIRTs and LE* (ENISA, 2019a) and *Roadmap of the cooperation between CSIRTs and LE* (ENISA, 2019b).

This report proposes a methodology to analyse the legal and organisational framework, the roles and duties of CSIRTs, LEAs and the judiciary, and their required competences, as well as synergies and potential interferences in their activities related to their responses to cyber incidents and fight against cybercrime, respectively. In addition, this report aims to present a detailed analysis focusing on some Member States (MSs) and European Free Trade Association (EFTA) countries, namely Czechia ([1]), France, Germany, Luxembourg, Norway, Portugal, Romania and Sweden.

The data for this report were collected via desk research and interviews with subject-matter experts. The data collected showed, among other things, that:

- The communities make efforts to avoid interferences where possible and attempt to create effective partnerships and take advantage of their synergies to support each other in the fight against cybercrime; however, some interferences might occur during incident handling and cybercrime investigations.
- There are examples of joint training activities, mainly involving two communities (CSIRTs and LEAs or LEAs and the judiciary, especially prosecutors) and, more rarely, involving all three communities, in particular in the form of joint exercises. These joint training activities help enhance overall the competences required to respond to cybercrime.
- There has been no significant impact of the coronavirus disease 2019 (COVID-19) pandemic on cooperation and interaction between the three communities and their ability to function. In some instances, interaction among the communities has increased, with even daily interactions, to ensure that each community is kept up to date. As the COVID-19 pandemic has continued, the use of online tools to facilitate meetings and events has become the norm.

This report, the 2020 handbook and the 2020 toolset on CSIRT and LE (law enforcement) cooperation (ENISA, 2021) are a set of deliverables complementing each other as follows:

- The report analyses roles, duties, competences, synergies and potential interferences across the three communities (CSIRTs, LE and judiciary).
- The handbook helps a trainer explain these concepts through scenarios.
- The toolset contains exercises for trainees based on these scenarios.

([1]) Czechia has been the short-form name for the Czech Republic since 2016.

1. INTRODUCTION

1.1. BACKGROUND OF THE REPORT

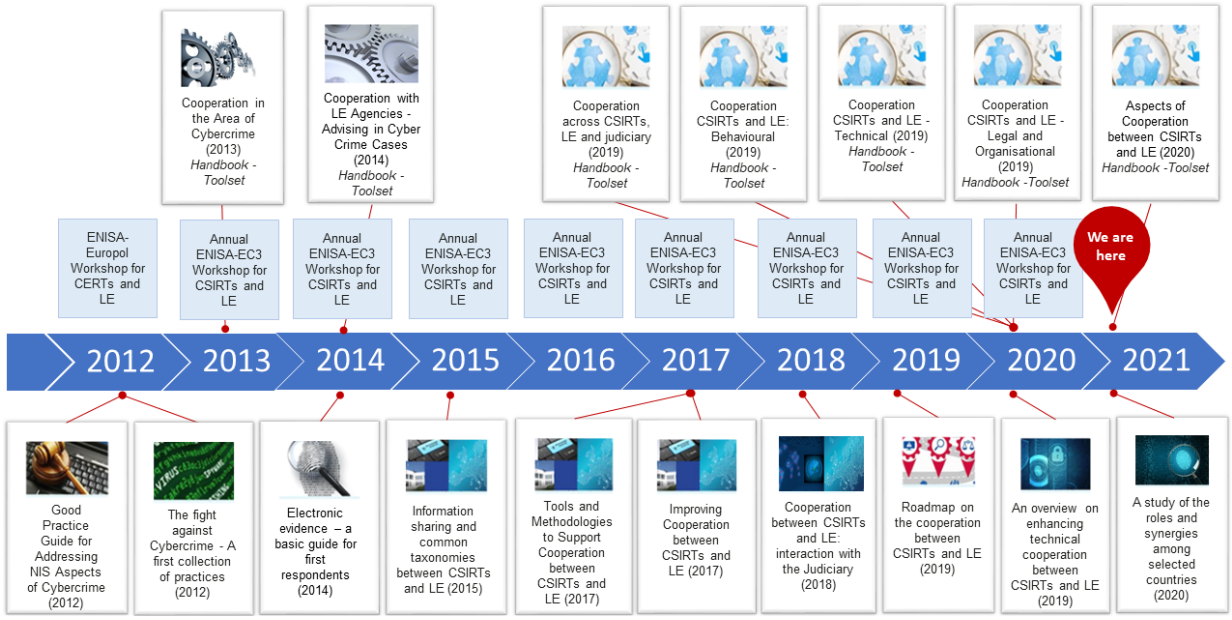
This report follows up previous work in the area of Computer Security Incident Response Teams (CSIRTs) and law enforcement (LE) cooperation. With the view of enhancing the response to cyberattacks and supporting the fight against cybercrime, this report aims to continue to facilitate cooperation between the CSIRT and the LE communities and the extensions that this collaboration may have to other communities, especially the judiciary. The *ENISA Programming Document 2020–2022* (ENISA, 2019) includes Objective 4.2 – Community building and operational cooperation. Under this objective, Output O.4.2.2 – Support the fight against cybercrime and collaboration across CSIRTs, LEA and other operational communities anticipates as one of the deliverables a report on a topic emanating from the 2019 report on cooperation between CSIRTs and LE.

The report presented here originates in particular from one of the recommendations of the 2019 report on cooperation between CSIRTs and LE entitled "*An Overview on Enhancing Technical Cooperation between CSIRTs and LE*" (ENISA, 2019a), namely:

- 'To promote the use of Segregation (or separation) of Duties (SoD) matrices to avoid overlapping duties across CSIRTs, LE and the judiciary in relation to the sharing information' (ENISA, 2019a, p. 35).

An overview and timeline of the previous work carried out by the European Union Agency for Cybersecurity (ENISA) in the area of CSIRT and LE cooperation is presented in the figure below ([2]).

Figure 1: Overview and timeline of previous ENISA work on CSIRT–LE cooperation



([2]) All reports and training materials are available on the ENISA website under publications (www.enisa.europa.eu/publications) and training resources (www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material).

This report, the 2020 handbook and the 2020 toolset on CSIRT and LE (law enforcement) cooperation (ENISA, 2021) are a set of deliverables complementing each other as follows:

- The report analyses roles, duties, competences, synergies and potential interferences across the three communities (CSIRTs, LE and judiciary).
- The handbook helps a trainer explain these concepts through scenarios.
- The toolset contains exercises for trainees based on these scenarios.

1.2. REPORT OBJECTIVES

The main objectives of this report are to:

- propose a **methodology** to analyse:
  - the legal and organisational framework defining the **roles and duties** ([3]) of CSIRTs, LEAs and the judiciary;
  - the **required competences** ([4]) of LEAs and CSIRTs, especially national and governmental CSIRTs;
  - **synergies and potential interferences** in their activities related to their responses to incidents of a criminal nature and their fight against cybercrime.
- present, focusing on some Member States/European Free Trade Association (EFTA) countries, a **detailed analysis of the roles and duties** of CSIRTs and LEAs and **required competences**, showing **synergies and potential interferences** in their activities related to their responses to incidents of a criminal nature and their fight against cybercrime.

This report is meant to provide a basis for a further, more comprehensive analysis covering additional Member States and EFTA countries. The methodology proposed could be used, with some adaptation, for further analysis of candidate countries, potential candidate countries ([5]) and neighbouring countries of the EU ([6]), as well as other countries.

1.3. REPORT SCOPE

The report focuses on the cooperation of national and governmental (n/g) CSIRTs ([7]) with LEAs, although most of the analysis is largely applicable to CSIRTs in general (i.e. other than n/g CSIRTs).

No specific sector is targeted in this report; the results are applicable to the different levels of cooperation between the three communities in response to incidents of a criminal nature and in the fight against cybercrime in all sectors (from finance to energy and from transport to health).

([3]) The term 'duties', as used here, as well as in the SoD matrix and in other parts of the reports, is synonymous to the term 'tasks'.
([4]) 'Competency' refers to a 'combination of skills, knowledge, attributes and behaviours that enables an individual to perform a task' (IAEA, n.d., p. 5) For more information on competences see also (UN, n.d., p. 6) and (OECD, 2014).
([5]) For a list of candidate countries and potential candidate countries see https://ec.europa.eu/neighbourhood-enlargement/countries/check-current-status_en
([6]) For a list of neighbourhood countries see https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/international-economic-relations/enlargement-and-neighbouring-countries/neighbouring-countries-eu_en
([7]) 'National/government (n/g) CSIRTs' refers to teams 'that serve a country's government by helping to protect its critical information infrastructure. N/g CSIRTs play a key role in coordinating incident management with the relevant stakeholders at national level. They also bear responsibility for cooperation with other countries' national and governmental teams (ENISA, n.d.d)]" (ENISA, 2019c, p. 9).

Following the methodology presented in this report (see Chapter 3), an analysis of the roles and duties, required competences, and synergies and potential interferences has been conducted and is presented in Chapter 4.

The general geographical scoping of the report is limited to EU/EFTA countries. The analysis presented in Chapter 4 focuses in particular on:

- Czechia;
- France;
- Germany;
- Luxembourg;
- Norway;
- Portugal;
- Romania;
- Sweden.

This selection of countries was based on the following criteria:

- geographical balance;
- balance of different legal systems;
- balance in terms of size (area and population) of the countries;
- balance in terms of maturity of the CSIRT–LE cooperation.

This report does not seek to provide an exhaustive analysis; rather, it focuses on a small number of topics affecting cooperation – in particular roles and duties, synergies and possible overlaps and interferences, required competences – as might be of interest in cross-border investigations.

In the future, this report is likely to be followed up with an extended version covering additional countries.

1.4. TARGET AUDIENCE

The intended target audience of this report is:

- CSIRTs, in particular n/g CSIRTs;
- LE ([8]);
- the judiciary (in this report this refers both to prosecutors ([9]) and to judges ([10]));
- individuals and organisations with an interest in cybersecurity.

Policymakers and lawmakers may also benefit from particular aspects of the analysis presented in this report as they prepare policies and legislation to enhance cooperation between operational communities in responding to cyberattacks and fighting cybercrime, including CSIRTs, LEAs and the judiciary, in the Member States and in jurisdictions interested in cooperating with the EU in their transition to and affirmation of the rule of law.

([8]) Similarly to previous ENISA reports, law enforcement (LE), law enforcement agencies (LEAs), police and police agencies are used synonymously; see, for instance, (ENISA, 2018).
([9]) On the status and role of prosecutors, see (UNODC, 2014).
([10]) On judges and principles to ensure their competence, independence and impartiality, see the European Charter on the Statute for Judges (Council of Europe, 1998).

2. DATA COLLECTION METHODS

This chapter describes the methods used to collect data for this report, starting with the desk research that was undertaken using publicly available sources such as legislative acts, policy reports, training programmes and other country-specific material. This is followed by a description of the interviews that were conducted, which were semi-structured and guided by a questionnaire, while allowing interviewees to discuss issues and topics pertinent to them and provide additional information. Finally, a description is provided of the SoD matrix that was used to collect additional data during the interviews to further support the research.

Qualitative research ([11]) was conducted for this report. A combination of research methods was used to collect data for analysing CSIRT, LE and judiciary cooperation, roles and duties, required competences, synergies and potential interferences in the selected Member State/EFTA countries, in particular:

- desk research;
- subject matter expert interviews;
- SoD matrix.

Desk research was also conducted to develop the methodology presented in Chapter 3, which was also used to collect data for the analysis of the eight EU Member States and EFTA countries presented in Chapter 4 and proposed for expanding the analysis to other countries.

The cut-off date for data collection was 31 August 2020; however, some input received at the beginning of October 2020 has also been integrated in this report.

2.1. DESK RESEARCH

Initially, desk research was conducted based on publicly available information sources such as legislative acts, policy reports, training programmes and country-specific sources, including ENISA publications.

The first findings from this desk research were particularly useful for:

- developing the methodology (presented in Chapter 3); and
- drafting the questionnaire to support the interviews.

Additional desk research was carried out focused on specific topics considered relevant by the project team following the analysis of the data collected during the initial desk research and the interviews. For instance, some additional desk research was conducted on the role of certain national bodies or joint initiatives mentioned during the interviews.

Desk research was also conducted to collect information on the included countries; the main sources consulted for each country are listed in Annex A.

Some legal material (EU and national legal acts, but also legislation-related legal assessments, policies and legal literature) covering areas such as principles of criminal procedure,

([11]) Qualitative research is focused on explaining the reasons for people's behaviour and understanding their opinions and options while quantitative research aims to quantify attitudes, opinions or other defined variables to generalise results from a population (Bryman & Bell, 2011). Interviewing is the most common format used for data collection in qualitative research while the questionnaire is the research instrument that is used most widely for both quantitative and qualitative approaches.

comparative criminal law and procedure, and European law was consulted. No specific thorough case law research was conducted on the role of CSIRTs in supporting the fight against cybercrime; however, from the limited research undertaken, it appears that such case law is rare and/or not publicly available.

In addition, documents such as the Cybersecurity Strategy of the EU and specific country National Cyber Security Strategies (NCSSs) ([12]) were reviewed.

Regarding aspects of cooperation and coordination between CSIRTs, LE and the judiciary, in addition to previous ENISA reports and projects, some reports by the European Commission, the European Union Agency for Law Enforcement Cooperation (Europol), the European Union Agency for Criminal Justice Cooperation (Eurojust), the Council of Europe and Interpol were also reviewed.

Academic publications were reviewed focusing on aspects such as the cybersecurity culture of CSIRTs and their effectiveness, capacity building and international cooperation, as well as national criminal justice practices.

Several course offerings and training programmes for CSIRTs, LE and the judiciary, as well as joint training initiatives, were reviewed, including, but not limited to, those provided by:

- ENISA: 'Trainings for Cybersecurity Specialists (ENISA, n.d.);
- Task Force on Computer Security Incident Response Teams (TF-CSIRT): 'TRANSITS training: High-quality training for computer security teams' (GÉANT, n.d.);
- Forum of Incident Response and Security Teams (FIRST): 'Trainings' (FIRST, n.d.);
- European Union Agency for Law Enforcement Training (CEPOL): 'Education and training' (CEPOL, n.d.);
- Europol European Cybercrime Centre (EC3): 'Training and capacity building' (Europol , n.d.);
- European Judicial Training Network (EJTN, n.d.a);
- Council of Europe: 'Cybercrime Programme Office (C-PROC)' (Council of Europe, n.d.a);
- Academy of European Law (ERA) (ERA, n.d.);
- ENFORCE Project ([13]) (CIRCL.LU, n.d. a).

Examples of the course offerings and training programmes reviewed are presented in Annex B.

Several different sources were also consulted to collect country-specific information.

The main sources consulted for the drafting of this report are listed in Annex C, grouped according to the following categories:

- legal framework-related material;
- policy reports;
- ENISA reports in the area of CSIRT and LE cooperation;

([12]) The ENISA NCSS Interactive Map lists all of the documents of the NCSSs in the EU, together with their strategic objectives and good examples of implementation. The map is available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

([13]) 'ENFORCE is an 18-month European project co-funded by the European Commission in the framework of the Internal Security Fund – Police.' The project was concluded in May 2020. 'The ENFORCE project aims at designing, setting-up, and disseminating a cybercrime training curriculum at the European level. This curriculum will be validated during a training exercise allowing different European public (e.g. law enforcement agencies and CSIRTs) and private actors fighting cybercrime to train together using state-of-the-art training technology. ENFORCE project is coordinated by CEIS and a partnership between CIRCL, French Ministry of Interior and CEIS' (CIRCL.LU, n.d. a).

- training-related material;
- country-specific material;
- academic papers;
- other material.

The search for policy reports took place from April to June 2020 using the following keywords: cybercrime, cybersecurity, national cybersecurity strategy, CSIRT, cybercrime legislation, criminal code, Budapest Convention, law enforcement, prosecutors, judiciary, criminal court, training, e-evidence.

2.2. INTERVIEWS

A questionnaire was designed to collect data through semi-structured interviews with experts from the selected countries.

The questionnaire was developed through several rounds of internal reviews to ensure that it was appropriate and relevant. The questionnaire was piloted and following the pilot interviews a few changes, mainly editorial, were made.

The questionnaire was divided into the following sections:

- Section 1: General and organisational aspects;
- Section 2: Possible synergies and potential interferences;
- Section 3: Challenges;
- Section 4: Competences and training;
- Section 5: Impact of the COVID-19 pandemic;
- Section 6: Certification of forensic tools.
- Section 7: Any additional information and comments

The questionnaire consisted of 14 open questions; in one question the interviewees were asked to fill in a SoD matrix (further details on the SoD matrix are provided in section 2.3). The interviewees were given the possibility of providing additional input and comments as free text.

The questionnaire was sent to the interviewees before the interviews.

Twenty interviews were conducted. The interviewees were carefully selected to ensure that the data collected would be as consistent as possible across the different communities (CSIRTs, LE and the judiciary) and countries. One representative each from a CSIRT, LE and the judiciary from each country was identified, mostly in a top/middle management role and with a good understanding or experience of cooperation between communities within their own country and possibly across the EU.

The interviews took place between June and August 2020. Unless the interviewees asked for an interview in person, the interviews were conducted by telephone. Interviews lasted for approximately 1 hour. To ensure that the data collected were of the highest quality, two members of the project team – in most cases at least one ENISA expert and one Call for Expressions of Interest (CEI) subject matter expert ([14]) – participated in the interviews and took detailed notes. After the interviews these detailed notes were sent to the interviewees for validation.

2.3. SOD MATRIX

In addition to the desk research and interview questions, a SoD matrix was used to collect data. The interviewees were sent the matrix, together with the questionnaire, before the interviews.

([14]) For more information on CEI Experts see Section 2.4.

During the interview they were asked to identify which actor(s) in their country for each of the given duties is Responsible, Supporting (if applicable), Informed (if applicable) and Consulted (if applicable). Some interviewees preferred to fill in the matrix after the interview and send it back by email.

SoD is a control that is used to ensure compliance with laws and regulations; it is already well known in financial accounting systems. In particular, regulatory mandates such as the Sarbanes–Oxley (SOX) Act of 2002 (US Congress, 2002) and the Gramm–Leach–Bliley Act (GLBA) (US Congress, 1999) introduced the concept of SoD and associated it with information technology (IT) organisation.

The importance of roles and duties has also been highlighted more recently in the General Data Protection Regulation (GDPR) (European Parliament and Council of the European Union, 2016a). The SoD is also presented in the ISO 27001 standard (ISO, n.d.) as one of the potential controls used for ensuring implementation and operation of information security within the organisation (control A.6.1.2 from Annex A of the ISO 27001 standard). Conflicting duties and areas of responsibilities should be segregated to reduce the risk of exposure to unauthorised or unintentional modification or misuse.

Thus, applying a SoD is a crucial aspect of an effective risk management strategy. In the context of CSIRT and LE cooperation, the risks that the communities may be exposed to are:

- reciprocal interference in the performances of duties;
- duplication of efforts because of overlapping duties;
- delays during a cybercrime investigation because of improper allocation of duties;

which could lead to:

- ineffective management of a cybersecurity incident and/or loss of information important for the investigation or of electronic evidence to prove the crime.

The SoD approach mandates a separation between actors performing different duties. Detected conflicts can be better managed as the actors, i.e. the CSIRTs, LE and judiciary, will be aware of the other communities' duties.

The SoD approach for the CSIRT, LE and judiciary communities was proposed in the 2018 ENISA report *Cooperation between CSIRTs and LE: interaction with the judiciary* (ENISA, 2018). In 2019, this matrix was developed further and the updated version was published in the 2019 report *An overview on enhancing technical cooperation between CSIRTs and LE* (ENISA, 2019a) and the *Roadmap on the cooperation between CSIRTs and LE* (ENISA, 2019b). Indicative examples of completed SoD matrices are provided in the 2019 ENISA Training material on CSIRT and LE cooperation (ENISA, n.d.c). It should be noted that the content of this framework was validated by the Member States during the 8th ENISA/EC3 Workshop that took place in November 2019 (ENISA, n.d.n); the workshop participants provided feedback and their views have been considered in the version of the SoD matrix presented in this report.

The SoD matrix used to collect data for this report and proposed as a methodology to collect data on CSIRT and LE cooperation is presented in more detail in Section 3.3. This SoD matrix is inspired by COBIT ([15]) methodology, in particular COBIT 5 (ISACA, n.d.), especially by the

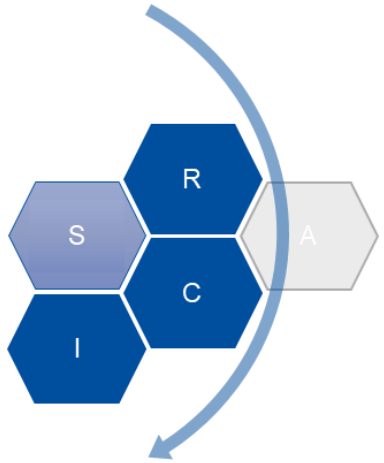
([15]) COBIT ('Formerly known as Control Objectives for Information and related Technology (COBIT); with this iteration used only as the acronym') is 'a broad and comprehensive I&T governance and management framework and continues to establish itself as a generally accepted framework for I&T governance' (ISACA, n.d.). This SoD matrix is inspired by COBIT 5 (released in 2012); however, it should be noted that there is a newer version of COBIT, COBIT 2019. 'Earlier versions of COBIT – [including COBIT 5] – focused on IT, whereas COBIT 2019 focuses on information and technology aimed at the whole enterprise, recognizing that I&T has become crucial in the support, sustainability and growth of enterprises'. For more information see (ISACA, n.d. a).

'RACI' charts (for more information on RACI charts, see, for instance, (Tomczack, 2014)). In COBIT 5 methodology the RACI charts are introduced to ensure the correct allocation of tasks within an organisation, with RACI denoting Responsible, Accountable, Consulted and Informed. The use of a responsibility assignment matrix such as the RACI charts, which describe participation in different roles, allows more detailed input than the symbols that have been used in previous ENISA studies on CSIRT and LE cooperation. Although responsibility assignment matrices are offered by various frameworks, the role distinction presented in COBIT 5 seemed to better fit the needs of this project. It should be noted that the COBIT 5 framework was not implemented in this study; however, the methodology used for collecting data was inspired by its RACI charts.

In the SoD matrix used to collect data for this report and proposed as a methodology to collect data on CSIRT–LE cooperation, namely 'RSCI', the four possible roles for CSIRTs, LE, prosecutors and judges concern the performance of duties related to (supporting) cybercrime-fighting activities: Responsible (R), Supporting (S) (if applicable), Consulted (C) (if applicable), and informed (I) (if applicable).

Figure 2 depicts the roles that can be assigned to the communities when they perform their duties, comparing them with those presented in the COBIT 5 RACI charts. The roles that were used to collect data for this project are highlighted in blue. The new role that replaced 'accountable' in COBIT 5 is highlighted in light blue. It should be noted that when a community is 'responsible' for a specific duty its representatives are also accountable when performing this duty.

Figure 2: RSCI method used to collect data



The SoD matrix has been converted to a Malware Information Sharing Platform (MISP) Galaxy 'matrix' format and made available on GitHub, together with some additional documentation ([16]). For this project, a JSON file ([17]) was created that can be easily converted to the data format that is supported not only by MISP but also by other sharing platforms that are accessible by both CSIRTs and LE. As mentioned in the 2019 ENISA report on technical cooperation between CSIRTs and LE (ENISA, 2019a), MISP seems to be the most popular information sharing platform used by both communities. 'MISP Galaxy is a simple method used to express a large object called cluster that can be attached to MISP events or attributes' (GitHub, n.d.). MISP Galaxies and Clusters can be added to MISP events and attributes for additional context and clarification. For instance, they can be used in MISP instances where LEAs/CSIRTs carry out joint threat research.

([16]) See https://github.com/enisaeu/CSIRTLEA/tree/main/SoD-Matrix
([17]) 'JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is easy for humans to read and write. It is easy for machines to parse and generate' (JSON.ORG, n.d.).

2.4. CONTRIBUTION BY SUBJECT MATTER EXPERTS

ENISA selected nine external subject matter experts, of whom eight were selected from the List of Network and Information Security (NIS) Experts compiled following the ENISA CEI (ref. ENISA M-CEI-17-T01) (ENISA, n.d.m).

Of these nine experts, five contributed to this report by supporting data collection (interviews and desk research) and report drafting; one contributed in particular to the desk research and the development of the methodology; one acted as the editor and coordinator of the input; and two reviewed the report over several rounds, including the first draft in April 2020, the intermediate draft in June 2020 and the final draft in August 2020 (these reviews were in addition to the reviews by ENISA reviewers and other external reviewers).

All nine contributed on an individual basis by their expertise in NIS aspects of cybercrime, including but not limited to technical, legal, organisational and behavioural aspects of CSIRT and LE cooperation.

3. PROPOSED METHODOLOGY

This chapter presents in detail the methodology suggested for the analysis of roles, synergies and potential interferences between CSIRT, LE and judiciary cooperation in specific countries in the desk research. This methodology has been piloted and used for the data collection for the current report and can be used for analysing additional countries.

The description of the desk research is followed by a description of the questionnaire to collect data via semi-structured interviews. Finally, the SoD matrix is proposed to support and/or complement the semi-structured interviews.

3.1. DESK RESEARCH

The desk research aims to collect information on:

- roles and duties;
- synergies and potential interferences;
- required competences.

To collect this information, **with a focus on specific countries**, the following sources are proposed to be consulted:

- **national laws and other legal acts**, including but not necessarily limited to:
  - constitutions;
  - criminal codes;
  - criminal procedural codes;
  - other laws specific to cybercrime and e-evidence, including laws implementing relevant EU law ([18]) and laws implementing the Council of Europe Convention on Cybercrime (Council of Europe, 2003);
- **NCSSs**;
- **policy documents**;
- **official websites of national and governmental CSIRTs, including their RFC2350 ([19])**;
- **official police websites**, especially the pages dedicated to fighting cybercrime activities;
- **official websites of prosecution offices**, especially the pages dedicated to fighting cybercrime activities;
- **official websites of criminal courts**, especially the pages dedicated to fighting cybercrime activities;
- **information dedicated to the different countries on the following portals/web pages**:
  - **ENISA National Cyber Security Strategies – Interactive Map** (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map);

([18]) For an overview of the relevant EU legal framework see (ENISA, 2017a).
([19]) An RFC2350 (where 'RFC' stands for Request for Comments) provides basic information about a CSIRT, its channels of communication and its roles and responsibilities. For more details on RFC2350 see (Brownlee & Guttman, 1998).

- **ENISA CSIRTs by Country – Interactive Map** (https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map);
- **FIRST members** (https://www.first.org/members/map);
- **Trusted Introducer (TI) European database of CSIRTs ([20])** (https://www.trusted-introducer.org/directory/index.html);
- **Europol website** (https://www.europol.europa.eu/partners-agreements/member-states);
- **Eurojust website** (http://www.eurojust.europa.eu/about/background/Pages/History.aspx);
- **Council of Europe website** (https://www.coe.int/en/web/portal/47-members-states);
- **e-Justice Portal** (https://e-justice.europa.eu and https://beta.e-justice.europa.eu – beta version);
- **European Judicial Network (EJN)** (https://www.ejn-crimjust.europa.eu/ejn/Ejn_Home/EN) and in particular the following pages:
  - 'Info about national systems' (https://www.ejn-crimjust.europa.eu/ejn/ejn_infoaboutall.aspx);
  - 'e-Evidence' (https://www.ejn-crimjust.europa.eu/ejn/EJN_DynamicPage/EN/83);

- **courses and training** for CSIRTs, LE, prosecutors and judges, focusing on preventing and fighting cybercrime.

The desk research aims to collect data on the competences that are needed for CSIRTs, LE and the judiciary to perform their roles and duties related to fighting cybercrime. Special focus should also be given to training initiatives to facilitate cooperation across the communities.

3.2. QUESTIONNAIRE

The following questionnaire can be used to support semi-structured interviews to collect data on roles and duties, required competences, synergies and potential interferences:

Section 1 – Questions on general legal/organisational aspects

1. What is the role of your organisation in fighting cybercrime activities?
2. Does your legal framework support the cooperation between CSIRT/LEA and the interaction/information flow with the judiciary (prosecutors and judges) in cybercrime
3. Regarding cybercrime cases, could you briefly describe how information is shared between CSIRTs – national and governmental in particular – LEAs, prosecutors and judges?

Segregation of duties (SoD) matrix

4. Referring to the SoD matrix that was sent to you before this interview […], could you fill it out by identifying for each duty which actor (CSIRT, LE, Prosecutors, Judges) in your country is:
   - Responsible (R): responsible for performing this duty, is the decision-maker
   - Supporting (S): providing support when performing this duty (if applicable)
   - Consulted (C): consulted during the performance of this duty (if applicable)
   - Informed (I): informed when performing this duty? (if applicable)

([20]) The Trusted Introducer (TI) maintains the European database of CSIRTs (also known as CERTs) and security teams. See https://www.trusted-introducer.org

Section 2 – Questions on possible synergies and potential interferences

5. In your opinion, which are the possible synergies across CSIRT/LE and judiciary during the performance of their fighting cybercrime-related duties? Have you seen in reality such synergies taking place? Could you give us an example?
6. In your opinion, which are the potential interferences across CSIRT/LE and judiciary during the performance of their fighting cybercrime-related duties? Have you seen in reality such interference taking place? Could you provide an example?

Section 3 – Questions on challenges

7. Are there any specific challenges that you would like to mention about cooperation across the CSIRT/LE and judiciary communities? If yes, what kind of challenges (e.g. legal, organisational, technical, cultural)?
8. Are there any challenges that you would like to mention in particular regarding digital forensics and electronic evidence (e-evidence)?

Section 4 – Questions on competences and training

9. What are the competencies that your organisation/community has and could share with the other communities (in particular CSIRT with LE/judiciary, LE with CSIRT, and judiciary with CSIRT)?
10. Which competencies do you feel are lacking/could be improved in your organisation/community and you might improve by learning from another community (e.g. CSIRT from LE/judiciary, LE from CSIRT, and judiciary from CSIRT)?
11. Does your organisation organise and/or participate in joint training across CSIRTs, LEAs and judiciary (prosecutor and judges) communities? If yes, do you find them useful?

Section 5 – Question on covid-19 pandemic crisis

12. Has the COVID-19 pandemic crisis changed the way CSIRT/LE/judiciary work together? If yes, how so? Could you provide an example? (e.g. fewer meetings in person, but on the other hand more communication via email and over the phone)

Section 6 – Question on cybersecurity certification of forensic tools

13. Do you think that a cybersecurity certification of forensic tools would help the CSIRT/LE/judiciary cooperation? (e.g. if CSIRTs use certified tools, the LE and Judiciary might trust more the data provided by CSIRT and use them more easily as evidence in court)

Section 7 – Question on any additional information or comments

14. Would you like to share any additional information or provide us with any comment?

The complete questionnaire is presented in Annex E.

3.3. SOD MATRIX

To complement and support data collection using the desk research and the semi-structured interviews, the SoD matrix in Table 1 is proposed to be used to collect data on the different roles of CSIRT, LE and judiciary, in the different phases of a cybercrime investigation. The development of this SoD matrix is described in Section 2.3, while a detailed description of the different roles and guidelines on how to fill in the matrix are provided below.

Table 1: SoD matrix used to collect data by implementing the RSCI method

Version 1.6 of 5 June 2020

- **Responsible (R)**: Who is responsible for performing this duty? Who is the decision-maker?
- **Supporting (S)**: Who is providing support when performing this duty? (if applicable)
- **Consulted (C)**: Who is consulted during the performance of this duty? (if applicable)
- **Informed (I)**: Who is informed when performing this duty? (For instance, if CSIRT should report a crime to LEA; this means that LEA is informed) (if applicable)

COLUMN 1	COLUMN 2	COLUMN 3	COLUMN 4	COLUMN 5	COLUMN 6	COLUMN 7
Duties related to (supporting) cybercrime fighting activities	**CSIRTs**	**LE**	**Prosecutors**	**Judges**	**Training topics (e.g. technical skills etc.)**	**ADDITIONAL COMMENTS (including information on Possible synergies and potential interferences)**
Prior to incident/crime						
1. Delivering training						
2. Participating in training						
3. Collecting cyber threat intelligence						
4. Analysing vulnerabilities and threats						
5. Issuing recommendations for new vulnerabilities and threats						
6. Advising potential victims on preventive measures against cybercrime						
During the incident/crime						
7. Discovering of the cyber security incident/crime						
8. Identifying and classifying the cyber security incident/crime						
9. Identifying the type and severity of the compromise						
10. Collecting data that may be evidence/evidence						
11. Providing technical expertise						
12. Preserving the evidence that may be crucial for the detection of a crime in a criminal trial						
13. Advising the victim to report/obligation to report a cybercrime to law enforcement (LE)						
14. Informing the victim of a cybercrime						
15. Informing other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)						
16. Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling						
17. Mitigating a cybersecurity incident						
18. Conducting the criminal investigation						

19. Leading the criminal investigation						
20. In the case of disagreement, having the final say for a criminal investigation						
21. Authorizing the investigation carried out by the LE						
22. Ensuring that fundamental rights are respected during the investigation and prosecution						
Post incident/crime						
23. Advising on systems recovery						
24. Protecting the constituency						
25. Preventing and containing cyber security incidents from a technical point of view						
26. Analying and interpreting collected evidence						
27. Requesting testimonies from CSIRTs and LE						
28. Admitting and assessing the evidence						
29. Judging who committed a crime						
30. Assessing cyber security incident damage and cost						
31. Reviewing the response and updating policies and procedures						

As it was the case for the data collection for this report, the matrix in Table 1 can be sent to interviewees along with the questionnaire before the interviews.

Some explanations on the matrix are provided below:

- At the top of the SoD matrix the four possible roles that each actor (CSIRTs, LE, prosecutors and judges) may play are listed and explained: Responsible (R), Supporting (S) (if applicable), Consulted (C) (if applicable), and informed (I) (if applicable).
- In the rows, the duties are listed and numbered for convenience (e.g. 10. Collecting data that may be evidence/evidence collection). It should be noted that ‘duties’ refers to the tasks performed by the communities during the cybercrime investigation phases.
- Columns 2–5 refer to the key actors throughout the cybercrime investigation life cycle: CSIRTs, LE, prosecutors and judges.
- In this matrix, the interviewees were asked to indicate which role(s) each actor (CSIRTs, LE, prosecutors, judges) plays in the performance of duties during a cybercrime (supporting)-fighting activity. In particular, the interviewees were asked to identify whether the CSIRT, LE, the prosecutor or the judge ‘Responsible’ for a particular duty and, if applicable, which other actor is responsible for ‘Supporting’ the performance of that duty, and who is ‘Consulted’ or ‘Informed’ during the performance of that duty.
- Column 6 (optional) is used to capture information on training topics that need to be covered for the communities to be able to successfully perform their tasks. It should be noted that the training needs are directly linked to the competences required for the performance of the specific duties.
- Column 7 is used for any additional information an interviewee might provide, with the aim of recording possible synergies and potential interferences, especially for those cases where a task is performed by more than one community.

An example of how to fill in the SoD matrix using the RSCI method is presented in Table 2. A LEA has been asked to indicate the roles that each community plays when 'collecting data that may be evidence'.

- The LEA is Responsible (R) for evidence collection while the CSIRT is Supporting (S) this cybercrime-fighting activity, as it also collects evidence that may be useful for LE.

- The prosecutor may be Consulted (C) and Informed (I) during the evidence collection phase to provide guidance on the types of data that need to be collected and to confirm if these data are admissible in criminal proceedings. Judges do not participate in this activity.

Table 2: Example of completed information related to one duty in the SoD matrix

- **Responsible (R): Who is responsible for performing this duty? Who is the decision-maker?**
- **Supporting (S): Who is providing support when performing this duty? (if applicable)**
- **Consulted (C): Who is consulted during the performance of this duty? (if applicable)**
- **Informed (I): Who is informed when performing this duty? (For instance, if CSIRT should report a crime to LEA; this means that LEA is informed) (if applicable)**

COLUMN 1	COLUMN 2	COLUMN 3	COLUMN 4	COLUMN 5	COLUMN 6	COLUMN 7
Duties related to (supporting) cybercrime fighting activities	**CSIRTs**	**LE**	**Prosecutors**	**Judges**	**Training topics (e.g. technical skills etc.)**	**ADDITIONAL COMMENTS (including information on Possible synergies and potential interferences)**
Prior to incident/crime						
10. Collecting data that may be evidence/Evidence collection	S	R	I C		Digital forensics	Prosecutor depending on the specific case may be informed or consulted, in other words requested to provide guidance.

4. COUNTRY FOCUS

This chapter presents the analysis of the data collected using the methodology outlined in Chapter 3 for the following MSs/EFTA countries:

- Czechia;
- France;
- Germany;
- Luxembourg;
- Norway;
- Portugal;
- Romania;
- Sweden.

For each country, first, an analysis of the roles and duties of CSIRTs, LE and the judiciary is provided. This is followed by a description of synergies and potential interferences. Finally, some examples of existing training programmes are provided.

The country profile analysis was based on desk research and interviews with CSIRTs, LE and some judiciary representatives. Contributions from the interviewees are acknowledged in the report. However, the following points should be noted:

- For consistency, the names of those interviewed are not provided, as some interviewees requested not to be named in the report.
- Interviewees provided their contributions based on their knowledge and expertise and were not acting as representatives of their country.

In each country section, a subsection is dedicated to the 'roles and duties' of competent authorities and departments that perform duties related to preventing and fighting cybercrime. The tables of competent authorities and departments provided are not exhaustive but rather aim to present the reader with a quick overview. Additional information on the authorities and departments and their roles and duties can be found in the subsections that follow these tables. It should be noted that each country has its own organisations in terms of CSIRTs, including national and governmental CSIRTs (as well as other CSIRTs), and also LE and judiciary authorities.

4.1. CZECHIA

Czechia is a 'parliamentary republic with a head of government, the prime minister – and a head of state, the president. The country is divided into 14 regions, including the capital, Prague' (European Union, n.d.a).

In the following subsections, an overview of the main authorities involved in the response to cybercrime in Czechia is provided, synergies and possible interferences are discussed and examples of relevant training are provided. More information on the relevant Czech legal framework can be found in Annex C.

In 2014 Czechia adopted its NCSS for 2015–2020 (NBÚ, 2015) (ENISA, n.d.e)). Cybersecurity has been regulated by the Cyber Security Act since 2014 (NCKB, 2014). The Cyber Security Act regulates the rights and obligations of persons, as well as the powers and competences of public authorities, in the field of cybersecurity. It also implements relevant EU provisions

(transposing, for example, the NIS Directive (European Parliament and Council, 2016)) and regulates the security requirements for electronic communications networks and information systems.

4.1.1. Roles and duties

In Czechia, the following authorities and departments play a role in and perform duties related to preventing and fighting cybercrime.

Name of the authority/department in English	Name of the authority/department in the original language	Abbreviation/short name in the original language (if applicable)
National Cyber and Information Security Agency (NCISA)	Národní úřad pro kybernetickou a informační bezpečnost	NÚKIB
National Cyber Security Centre (NCSC)	Národní centrum kybernetické bezpečnosti	NCKB
GovCert.CZ: Government CERT of the Czech Republic	GovCERT.CZ: Vládní CERT České republiky	GovCERT.CZ
National CSIRT of the Czech Republic	Národní CSIRT České republiky	CSIRT.CZ
Police of the Czech Republic – National Centre Against Organized Crime – Unit of Special Activities	Národní centrála proti organizovanému zločinu – Útvar zvláštních činností	NCOZ – ÚZČ
Supreme Public Prosecutor's Offices and Judges	Nejvyšší státní zastupitelství České republiky	

4.1.1.1. National cyber security agency

The **National Cyber and Information Security Agency** (NCISA) is responsible for the implementation of the NCSS in Czechia. It is 'the central administrative body for cyber security, including the protection of classified information in the field of information and communication systems and cryptographic protection' (NÚKIB, n.d.). It can also act as an 'expert' on cybersecurity issues for LE and provide technical help in criminal investigations. NCISA 'operate[s] the government security team, the so-called Government CERT of the Czech Republic (GovCERT.CZ)' (NÚKIB, n.d. a). It also engages in dialogue with the other EU Member States. NCISA cooperates with other national and foreign CSIRTs, supports education and research and development in the field of cybersecurity, performs security audits and exercises, and engages in international cooperation and policy work. It also offers legal and policy support in the field of cybersecurity to other governmental bodies and their CSIRTs.

4.1.1.2. CSIRTs

In Czechia, there are officially two nationwide CSIRT teams recognized by the Cyber Security Act: the governmental CERT (**GovCERT.CZ**) and a national CSIRT (**CSIRT.CZ**).

GovCERT.CZ is a public entity operated by the executive section of NCISA. GovCERT.CZ's 'goal is to help [the critical information infrastructure and the state bodies] to effectively face security challenges, react on the incidents, coordinate actions to solve them and effectively prevent them' (NÚKIB, n.d.). Its 'constituency are public sector institutions and critical information infrastructure of the Czech Republic' (NCBK, 2015, p. 8). Operators of these infrastructures are required by law to report cybersecurity incidents to NCISA. GovCERT.CZ is therefore responsible for the evaluation of, and coordination of the response to, severe incidents and the sharing of relevant information about incidents or threats with relevant authorities, operators of relevant infrastructures and the public. GovCERT.CZ/NCISA may require regulated

entities to implement reactive or preventive measures in reaction to specific cybersecurity incidents and threats.

CSIRT.CZ is a private entity operated by the Czech domain registry CZ.NIC on the basis of a public contract arranged with NCISA. CSIRT.CZ fulfils the role of a national CSIRT, as defined in the Cyber Security Act. It collects mandatory reports of cybersecurity incidents from operators of important networks and digital services, coordinates the response to them and shares data and information with GovCERT.CZ.

There are three main reasons why there are two nationwide CSIRTs in Czechia. The first reason is because of the principle of the minimisation of state intervention – it is not necessary for the state to strictly regulate all operators of information infrastructures; therefore, GovCERT.CZ deals only with the most important infrastructures in terms of national security and provides other infrastructures with the opportunity to cooperate through the national CSIRT. The second reason is that private infrastructure operators are more willing to cooperate with another private entity than with the state; therefore, a greater intensity and scope of cooperation between the infrastructure operators and the private national CSIRT is expected. The third reason is that a public institution can do only what the law expressly allows, whereas the private national CSIRT can be much more creative in coordinating and organising the response to cybersecurity incidents, as it can act *praeter legem* and can do anything that the law does not explicitly prohibit it from doing (Government of the Czech Republic, 2020).

4.1.1.3. LE

The **National Centre against Organized Crime** (Národní centrála proti organizovanému zločinu – NCOZ) was established in 2016 by merging the Organized Crime Detection Unit (Útvar pro odhalování organizovaného zločinu – ÚOOZ) and the Corruption and Financial Crime Detection Unit (Útvar pro odhalování korupce a finanční criminality – ÚOKFK). It currently plays a key role in the fight against cybercrime in Czechia. As a central body, it specialises in the fight against organised and large-scale cybercrime and cybercrime against critical and important information infrastructures. NCOZ also plays a coordinating role and a role in the preparation of standard and recommended procedures for cybercrime investigations.

The **Unit of Special Activities** (Útvar zvláštních činností – ÚZČ) of the Police of the Czech Republic intercepts and records telecommunication traffic, conducts surveillance of persons and objects, and collects digital evidence and carries out other specialised actions aimed at securing such evidence.

At the regional level there are information crime units at each of the regional criminal police directorates. These units include specialists and have technical equipment for investigating cybercrime and securing electronic evidence. They conduct investigations and provide support and technical equipment in cybercrime investigations to lower organisational units.

4.1.1.4. Judiciary

'The Supreme Public Prosecutor's Office of the Czech Republic is the competent central authority in the pre-trial stage of criminal proceedings whereas the Ministry of Justice of Czechia is the competent central authority for the trial stage of criminal proceedings and when the execution of sentences is concerned' (Council of Europe, n.d.b).

A network of prosecutors specialising in cybercrime has been formally established at the national level (Council of the European Union, 2017).

At the level of the Public Prosecutor's Office and courts, an informal expert group has been set up at the Supreme Public Prosecutor's Office, which focuses on computer crime.

Judges in Czechia are independent in the performance of their duties and there is no specialisation of judges in criminal chambers. Cases are therefore assigned to judges according to a random key and it is up to each judge to educate themselves on the issue at hand. However, because of the increasing number of cybercrime cases, as well as cases in which familiarisation with the issue of electronic evidence is necessary, there is an increased interest in this area on the part of the judges. There is also a clear effort on the part of prosecutors and the police to provide relevant information on the context of, and to explain the technical details of, cases, including in cooperation with CSIRTs, academia and other members of the professional public.

Czechia cooperates with Eurojust and is a member of Eurojust's Cybercrime Network.

4.1.2. Synergies and potential interferences

As in most countries, useful synergies and also at the same time reciptocal potential interferences in the activities of individual communities can be identified. In general, representatives of these communities agreed that, if the activities of individual communities are coordinated, they are significantly more effective. In such cases, individual communities can support each other and share specific competences, powers, knowledge, information and equipment.

Over the last few years, many steps have been taken to strengthen the effectiveness of intercommunity cooperation. The Cyber Security Act has been adopted, regulating the obligation to provide information and formulating the powers of NCISA and national and governmental CSIRTs; a memorandum was concluded between NCISA and the police; the position of liaison officer to enable police and CSIRT coordination was established; and cooperation mechanisms have been set up and implemented. These steps have led to many synergistic effects. In particular, they enable the immediate and effective bilateral transfer of information on threats and incidents between LE and CSIRTs, the mutual use of professional and technical capabilities of individual communities, mutual assistance in actions to fulfil relevant obligations, and cooperation with other communities. One synergistic effect specifically identified during the interviews is that CSIRTs share with LE information obtained from a constituency or cooperating alliances that would otherwise be unavailable to LE. However, although these synergies are particularly evident between CSIRTs and LE, they are relatively new in the case of the judiciary.

There are also some interferences that may occur between the communities. According to the interviewees the most important potential interference relates to the collection of digital evidence and stems from the differences between the goals and approaches of the different communities. Activities of CSIRTs focused on the mitigation of cyber incidents may seriously hinder collection of the evidence necessary for a criminal investigation, or even destroy it or render it inadmissible at court. In addition, one of the limitations of cooperation identified during the interviews is the effort made by CSIRTs to maintain trust within their constituencies. Although CSIRTs recommend that victims of cybercrime report incidents to and cooperate with LEAs, they sometimes refuse to do so for different reasons. In such cases CSIRTs are discouraged from sharing information about relevant incidents with LE because they fear a loss of trust on the part of their constituency. Another limitation identified is the lack of understanding, specifically between CSIRT and LE community technical experts and the judiciary.

During the interviews, the following recommendations were formulated by the interviewees:

- provide more coordination of activities – through training, more precise legal and procedural regulation and cooperation mechanisms;
- provide transparent information-sharing mechanisms;

INTERCOMMUNITY COOPERATION

Cooperation mechanisms have been set up and implemented [enabling] immediate and effective bilateral transfer of information on threats and incidents between LE and CSIRTs.

- strengthen cooperation with the judiciary (CSIRT–LE cooperation is mostly already in place);
- provide better descriptions of individual groups/units, so that everyone knows who to contact and when;
- implement sustainable and trustworthy cooperation routines for all the institutions involved;
- involve all of the communities in training; the training should be focused on the ability to rapidly share information between all communities.

4.1.3. Examples of training

The Action Plan of the Cyber Security Strategy of Czechia (NCKB) considers promoting the development of Czechia's police capabilities with regard to cybercrime. It mainly aims to:

- reinforce the personnel of individual police cybercrime departments;
- modernise the technological equipment of specialised police departments;
- develop cooperation with foreign counterparts;
- provide professional education and training to police specialists, including language training.

The Conception of the Development of Capabilities of the Police of Czechia to Investigate Cybercrime was drafted by the Police Presidium of Czechia and adopted by the National Security Council in October 2015 (Council of the European Union, 2017).

Actions aimed at the prevention and public awareness of cybercrime are carried out by several authorities within Czechia, such as the National Cyber Security Centre, LEAs, the private sector, academia and non-governmental organisations.

The National Cybersecurity Competence Centre (NC3) (National Cybersecurity Competence Centre , n.d.) at Masaryk University, Brno (Masaryk University , n.d.), has developed a special tool, KYPO (Kybernetický polygon), which is a cyber range platform (KYPO, n.d.), and built a laboratory that is used to organise cybersecurity exercises. These consist of large-scale exercises held two to four times a year, with smaller exercises taking place a couple of times a month, and are offered to public authorities, businesses and education providers. NC3 offers training to judicial and police academies, investigators and public prosecutors. NCISA, in cooperation with NC3, also organises the annual Cyber Czech exercise using KYPO and its laboratory ([21]).

Law enforcement and judicial authorities are provided with professional training on cybercrime. The aim is to establish standard practices and knowledge for the detection and investigation of cybercrime, with the main focus being to secure digital traces and evidence. Certain educational activities on dealing with cybercrime also take place at Secondary Police Schools of the Ministry of the Interior. Participation in national and international exercises in the field of cybersecurity, organised by GovCERT.CZ, also serve as professional training.

The Police Academy (The Police Academy of the Czech Republic, n.d.) also takes cybercrime into account in its lifelong training for officers. These training activities are organised with CEPOL and many of the courses are the result of the EMPACT initiatives (Europol, n.d.d).

The Judicial Academy (The Judicial Academy, n.d.) organises training activities for LE and prosecutors on cybercrime and electronic evidence in cooperation with the Police Academy.

([21]) This is the main cybersecurity exercise organised by Czechia – it is focused mainly on technical issues, but also deals with cooperation, legal and organisational issues. It involves the simulation of cooperation between CSIRTs, the police, the media, data protection authorities, users, other infrastructure operators, etc. For more information see https://csirt.muni.cz/projects/cyber-czech.

Finally, tabletop exercises take place between CSIRTs and LE and help to improve communication.

4.2. FRANCE

France is 'a semi-presidential republic with a head of government, the prime minister, appointed by the president who is the directly elected head of state. France's territory consists of 18 administrative regions – 13 metropolitan (i.e. European France) and 5 overseas regions' (European Union, n.d.f).

In the following subsections, an overview of the main authorities involved in the response to cybercrime in France is provided, synergies and possible interferences are discussed and examples of relevant training are provided. More information on the relevant French legal framework can be found in Annex C.

France adopted its updated NCSS in 2015 (ANSSI, n.d.) (ENISA, n.d.h). 'An initial cybersecurity strategy was developed in France in early 2010 and was published in early 2011' (Prime Minister of France, 2015, p. 7).

4.2.1. Roles and duties

In France, the following authorities and departments, in particular, are responsible for preventing, analysing and fighting cybercrime.

Name of the authority/department in English	Name of the authority/department in the original language	Abbreviation/short name in the original language (if applicable)
National Agency for the Security of Information Systems	Agence Nationale de la Sécurité des Systèmes d'information	ANSSI
- **French government computer emergency response team**	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques	CERT-FR
National Police	Police Nationale	
- **Directorate-General of the National Police**	Direction Générale de la Police Nationale	DGPN
- **Central Directorate of the Judicial Police**	Direction Centrale de la police judiciaire	DCPJ
○ **Sub-directorate for ICT-related offences established for the fight against cybercrime**	Sous-Direction de Lutte contre la Cybercriminalité	SDLC
▪ **Central Office for Combating Information and Communication Technology Crime**	Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication	OCLCTIC
▪ **CSIRT of the Judicial Police**	CSIRT Police Judiciaire	CSIRT PJ
▪ **E-evidence Unit**	Division de la preuve numérique	
National Gendarmerie	Gendarmerie Nationale	
- **Directorate-General of the National Gendarmerie**	Direction Générale de la Gendarmerie Nationale	DGGN
○ **Centre for Fighting Digital Offences**	Centre de lutte contre les criminalités numériques	C3N
Paris Police Prefecture	Préfecture de police	

- **Cybercrime Unit**	Brigade de lutte contre la cybercriminalité	BL2C
Directorate-General for Internal Security	Direction générale de la sécurité intérieure	DGSI
Public Prosecutors and Judges	Magistrats du parquet (Ministère public) and Juges	

4.2.1.1. National cyber security agency

The National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information – ANSSI) is responsible for implementing the NCSS in France. 'The role of ANSSI is to foster a coordinated, ambitious, pro-active response to cybersecurity issues in France, to drive raising-awareness actions, as well as to spread French vision and expertise, and European values, abroad' (ANSSI, n.d. a).

4.2.1.2. CSIRTs

France has an officially recognised national CSIRT, CERT-FR (French government CERT, Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques).

CERT-FR is part of ANSSI. 'Its mission is to coordinate and investigate IT security incident response for the French government, critical national infrastructure operators and operators of essential services as defined by the French law.

CERT-FR's missions cover prevention, detection, response and recovery by:

- Helping to prevent security incidents by setting up necessary protection measures;
- Detecting vulnerabilities on networks and systems;
- Managing incident response, with the support of trusted partners if necessary;
- Organizing trusted networks of CSIRT' (ANSSI, 2018).

As a national CSIRT it is the preferred international contact point for any cyber-related incident affecting France. It operates 24 hours a day, 7 days a week..

CERT-FR is a member of well-known networks of CSIRTs such as the CSIRTs Network, the FIRST and it participates in the TF-CSIRT activities. CERT-FR also creates a French initiative to structure the national incident response ecosystem called InterCERT-FR. As part of ANSSI, CERT-FR also work closely with the CyCLONe's officers.

CSIRT of the Judicial Police (CSIRT Police Judiciaire – CSIRT-PJ) is the CSIRT of the Central Directorate of the Judicial Police, operating under the Cybercrime Centre (CSIRT-PJ, n.d.). CSIRT-PJ aims to provide LE with CSIRT-like services: incident response, threat intelligence, and malware analysis tooling. It is a member of TF-CSIRT (listed) and belongs to the French CSIRT community called InterCERT-FR.

4.2.1.3. LE

The National Police (Police nationale) has the principal mission of fighting against any form of criminality and delinquency including cybercrime. One of the directorates of the National Police is the Central Directorate of the Judicial Police (Direction centrale de la police judiciaire – DCPJ), which performs investigative tasks and supports the prosecution service in cybercrime cases. Within the DCPJ, a sub-directorate for ICT-related offences has been established for the fight against cybercrime (Sous-direction de lutte contre la cybercriminalité – SDLC), which includes the Central Office for Combating Information and Communication Technology Crime

(Office Central de lutte contre la Criminalité liée aux Technologies de l'iInformation et de la Communication – OCLCTIC) ([22]), a cyber-intelligence unit.

The National Gendarmerie (Gendarmerie nationale) is a branch of the French Armed Forces that is placed, as far as its civilian role goes, under the jurisdiction of the Ministry of the Interior. The Central Criminal Intelligence Service of the National Gendarmerie (Service central de renseignement criminel de la Gendarmerie nationale – SCRCGN) is responsible for providing information and a precise understanding of organised and mass crime, to guide actions in the fight against crime in the pre-judicial and judicial phases. In parallel, within the SCRCGN, the Centre for the Fight against Digital Crimes (Centre de lutte contre les criminalités numériques – C3N) aims to conduct or coordinate investigations of national scope relating to cybercrime, and to carry out permanent surveillance of the internet, to detect and collect evidence of any offences that may be committed there.

Under the structure of the Paris Police Prefecture (Préfecture de police), the Cybercrime Unit (Brigade de lutte contre la cybercriminalité – BL2C) is assigned with cybercrime investigation tasks, in the capacity of judicial police (CSIRT-PJ, n.d.).

The Directorate-General for Internal Security (Direction générale de la sécurité intérieure – DGSI), among other duties, has jurisdiction over investigations into cyberattacks with a national security component. More precisely, the DGSI has exclusive judicial competence to carry out cybercrime investigations related to attacks against critical infrastructure, national institutional networks and operators of essential services (Ministère de l'Interieur, 2019).

4.2.1.4. Judiciary

The French judicial system consists of ordinary courts, which include the criminal courts, and administrative courts. The Court of Cassation (Cour de Cassation) is the supreme court in the French judicial system of ordinary courts. The public prosecutor is the authority exercising prosecution tasks, referring cases to the 'investigative judge' (*juge d'instruction*) and overseeing the criminal investigation process and the judicial police (European Union, n.d.g) (Ministère de la Justice, 2012).

Within the public prosecutor's offices, 'an internal organisation has been set up to include a "specialist judge" (*magistrat référent*) for cybercrime, who can provide technical support to colleagues involved in cybercrime cases' (Council of the European Union, 2015).

The Prosecutor of Paris now has national jurisdiction for cybercrime cases. As was highlighted during one of the interviews, the prosecutor can evoke any case on national territory. This approach provides better management of expertise as judges are specialised and handle a great number of cases. The Prosecutor of Paris has a cell of three magistrates who specialise in cybercrime.

One of the interviewees reported that the Mission against Cybercrime was established in 2015 within the French Ministry of Justice. This mission has a more strategic role. The following information emerged in this interview: 'The tasks undertaken are not at an operational level but directly at the ministry level, to analyse the phenomenon, represent the ministry and provide official guidelines to handle relevant cases. An example of its work is to issue official guidelines for Prosecutors to treat and prosecute some cases, such as a document to centralize judicial treatment of ransomware. Public policy on the fight against cybercrime is elaborated at the level of this Mission to support the judiciary.'

([22]) The SLDC responds to the need to develop a global policy to combat cybercrime. It defines the strategies to be implemented in the operational, training and prevention areas for the general public and the financial sector. Strategic coordination of SDLC activities is handled by the OCLCTIC.

France cooperates with Eurojust and is a member of Eurojust's Cybercrime Network.

4.2.2. Synergies and potential interferences

As emerged from the interviews 'ANSSI/CERT-FR and FR law enforcement perimeters and mandates are complementary. As part of the national authority on cybersecurity, ANSSI/CERT-FR has the expertise on many cyber-related topics.' ANSSI/CERT-FR helps both LE and the judiciary 'by sharing […] expertise in cybersecurity and […] knowledge on threats'. As was stated during one of the interviews, 'There are different directions [of interaction] between CSIRTs and LE but also the judiciary from the administrative and the operational side. ANSSI […], according to French law, […is] a public agency [and] has the obligation to inform the competent authorities in the event of a suspicious criminal case'. Therefore, ANSSI informs the Prosecutor Office when it becomes aware of a crime. On the other hand, the prosecutors can also ask for 'help from ANSSI (e.g. on particular infrastructure data and on modus operandi), but this is still quite rare. There are [indeed] rather few cases […where] the judiciary has initiated a contact with the CSIRTs to handle a case.'

Usually, ANSSI is informed of an attack on its constituency (critical infrastructure operators) directly or the victim files a complaint to LE. ANSSI teams collect evidence in a legally sound manner and begin remediation. LE then receives and processes the evidence and conducts its analysis (on network logs, for example). The objective of LE is different from that of ANSSI: ANSSI is looking for every details of intrusion while LE is looking for identification information. Thus, ANSSI is able to suggest efficient remediation actions to the victim. In addition, as the interviewees noted, 'a liaison officer has been appointed between the ANSSI/CERT-FR and the Ministry of [the] Interior and a dedicated process has been set up to share information on incidents that are reported to ANSSI and are relevant for [French] LE entities'.

Nevertheless, according to the interviewees, restrictions on information sharing may occur, such as 'when an investigation is launched on a […] case [that is under judicial examination]'. In such cases, 'ANSSI/CERT-FR has to follow strict rules on information sharing with its other partners in order to respect the confidentiality of investigations'. Eventually, ANSSI may request authorisation from the judiciary for information sharing with other members of the CNW for prevention purposes; a known C2 IP can help other CSIRTs protect their constituency. As emerged from the interviews, the information-sharing process with international partners could therefore be delayed in some cases. As 'threats are international but the law enforcement administration is national', the main challenge identified is to address these delays. Furthermore, as one of the interviewees highlighted, another challenge that may arise is to have the victim 'file a legal complaint, in order to allow LE to take over before [launching the] remediation actions that could potentially alter the evidence'.

To better understand each other's work, some public prosecutor's offices have regular formal meetings with specialised police investigation services. In addition, such meetings help to clarify which investigative tasks can be requested of local police to avoid overloading the specialised services. Indeed, the communities are committed to a 'continuous improvement of the close relations' that they have established.

In addition, under the framework of the French cyber defence strategy entitled "La Revue stratégique de cyberdéfense", a public–private initiative was launched in 2017 to raise awareness of the risks of cyberattacks to society and to support the victims of such attacks. The initiative is handled by the Public Interest Group for Action against Malicious Cyber Activities (Le Groupement d'Intérêt Public Action contre la Cybermalveillance (GIP ACYMA). The state actors involved are ANSSI, the Ministry of the Interior, the Ministry of Justice, the Ministry of Economy and Finance and the Secretary of State in charge of the digital sector. Civil society is also represented in this Public Interest Group through consumer associations or victim support entities, as well as trade and labour unions. This public–private initiative also handles the online cybersecurity platform Cybermalveillance.gouv.fr, which was put in place to guide individuals,

EXAMPLE OF SYNERGY – THE CSIRT-PJ

The CSIRT Police Judiciaire is part of French LE. It supports investigations into cybercrime. As full member of the CSIRT community, it is a privileged actor in terms of cooperation and information exchange.

small businesses and local authorities in taking preventive steps against cyberattacks and addressing malicious events once they occur (Cybermalveillance.gouv.fr, 2019).

4.2.3. Examples of training

ANSSI offers free cybersecurity training to public organisations, among them LEAs, covering a wide variety of topics and expertise levels. A lot of the training addresses basic security for end users, as well as system administrators. It also deals with a wide range of advanced topics such as security audits, network security, security certificate management and implementation of cybersecurity certification. Finally, it provides training on very specialised topics such as radio security against TEMPEST attacks.

As discussed during the interviews, the communities could benefit from joint training, as this would 'be useful to help strengthen the relationship between the CERT-FR/ANSSI and the LE [and] judiciary [communities]'. Moreover, the communities could benefit from learning more about each other's counterparts in the 'international cooperation process, [the] mechanisms and [the] main players [involved]' to overcome the difficulties that occur in identifying competent actors and the actions to be expected.

Trainees at police, gendarmerie and judicial academies receive basic training on cybercrime. These courses are often complemented by conferences or scientific and technical police workshops.

The OCLCTIC of the National Police organises on an annual basis a training course for French judges and investigators entitled 'Approach to cybercrime', focusing on legal aspects related to cybercrime and the special investigation techniques. It also organises a 'first responder' training course aimed at police officers who have to carry out basic cybercrime-related investigative procedures (Council of the European Union, 2015).

The BL2C, part of the Paris Police Prefecture, participates in private sector training and provides two approved training courses to the judiciary and customs officers on digital police investigations.

The Information Systems Security Training Centre (CFSSI) is the main point of contact for ANSSI for the training of various agencies. It is also involved in the definition and implementation of the training policy.

CECyF, also called F-CCENTRE, is the French Expert Centre against Cybercrime. CECyF started in the context of the European project 2Centre (Cybercrime Centres of Excellence Network for Training Research and Education). CECyF provides support to LE researchers from both academia and the private sector and educational institutions to create projects that contribute to training, education and research on cybercrime (CECyF, n.d.).

Finally, the French National School for the Judiciary (Ecole nationale de la magistrature – ENM) provides multidisciplinary training to French and foreign judges, police officers, gendarmerie and customs officers on recent legislative developments, as well as specific aspects of digital investigations and the judicial handling of cybercrime.

4.3. GERMANY

Germany is 'a federal, parliamentary republic, with a head of government, the chancellor, and a head of state, the president, whose primary responsibilities are representative. The country comprises of sixteen federal States (Länder), which each have their own constitution and are largely autonomous regarding their internal organisation' (European Union, n.d.c.). Power is distributed between the federal and the state governments. Considering the state structure in

the country, preventing and responding to cybercrime require close cooperation at the federal and Länder levels.

In the following subsections, an overview of the main authorities involved in the response to cybercrime in Germany is provided, synergies and possible interferences are discussed and examples of relevant training are provided. More information on the relevant German legal framework can be found in Annex C.

Germany adopted its NCSS initially in 2011 (BMI, 2011); this was updated in 2016 (ENISA, n.d.f).

4.3.1. Roles and duties

In Germany, the following authorities and departments in particular, are responsible for preventing, analysing and fighting cybercrime.

Name of the authority/department in English	Name of the authority/department in the original language	Abbreviation/short name in the original language (if applicable)
Federal Office for Information Security	Bundesamt für Sicherheit in der Informationstechnik	BSI
- **CERT-Bund (part of BSI)**	CERT-Bund	CERT-Bund
National Cyber Response Centre	Nationale Cyber-Abwehrzentrum	Cyber-AZ
Federal Criminal Police Office	Bundeskriminalamt	BKA
- **Division CC – Cybercrime**	Abteilung 'Cyber-crime'	CC
Federal Police	Bundespolizei	BPOL
Criminal police offices of the federal states (Länder)	Landeskriminalämter	LKAs
The Federal Public Prosecutor General and the Federal Court of Justice	Der Generalbundesanwalt beim Bundesgerichtshof and Bundesgerichtshof	GBA and BGH
Public Prosecutor's Offices and Courts of the federal states (Länder)	Die Staatsanwaltschaften der Länder and Landgerichte	Individual per federal state

4.3.1.1. National cyber security agency

The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) is the federal cybersecurity authority that 'shapes information security in digitization through prevention, detection and reaction for government, business and society' (BSI, n.d.). Its 'goal […] is to promote IT security in Germany. The BSI is first and foremost the central IT security service provider for the federal government in Germany' (BSI, n.d.). CERT-Bund is part of the BSI. The mandate and competences of the BSI are provided by the Act on the Federal Office for Information Security of 2009, last amended on 2017 (BSI, 2017).

The National Cyber Response Centre (Nationale Cyber-Abwehrzentrum – Cyber-AZ) has been set up to 'optimize operational cooperation between all state authorities and improve the coordination of protection and response measures'. Different governmental agencies are part of this centre (BSI, BKA, BW-KdoCIR, BBK, BPOL, BfV, MAD and BND). 'Cooperation in the National Cyber Response Centre […] strictly observe[s] the statutory tasks and powers of all authorities involved on the basis of cooperation agreements.'

4.3.1.2. CSIRTs

As mentioned, **CERT-Bund** is part of the BSI. CERT-Bund is the national CSIRT and 'acts as the central point of contact regarding IT-security incidents concerning the German government. In addition it provides services to critical infrastructure, industry and SME [small and medium-sized enterprises] as well as citizens. Germany's national IT Situation Centre and the national Cyber Response Centre are supported by CERT-Bund' (BSI, n.d. a). CERT-Bund is therefore responsible for a large constituency and handling IT security incidents related to government institutions, federal authorities, critical infrastructures and organisations.

The services that CERT-Bund offers are:

- '24-hour on-call duty in cooperation with the IT Situation Centre;
- analysis of incoming incident reports;
- creation of recommendations derived from incidents;
- support during IT security incidents;
- operation of a warning and information service;
- active alerting of the Federal Administration in case of imminent danger' (CERT-Bund, n.d.).

CERT-BPOL ([23]) is part of the Federal Police (Bundespolizei). 'After an attack in 2017, the CERT-BPOL was founded as the cyber attack analysis and defense center and has been reinforced continually ever since. The team comprises IT security staff from the Federal Police. The team consists of IT experts from the Federal Police supported by experts from industry and science. In order to detect and investigate incidents in the German Federal Police infrastructure, intrusion prevention systems are operated and infrastructure vulnerabilities are identified by CERT-BPOL. Liaison officers from CERT-BPOL represent the Federal Police Headquarters at the […] Cyber-AZ' (Bundespolizei, 2017).

4.3.1.3. LE

As of 1 April 2020, the German Federal Criminal Police Office (Bundeskriminalamt - BKA, n.d.) includes a separate division dealing with cybercrime, named Division CC – Cybercrime (Abteilung 'Cyber-crime'). This division emerged from the Cybercrime and Information and Communication Crime (ICT) group of the Serious and Organised Crime (SO) Department.

The main tasks of the Division CC – Cybercrime are to investigate cybercriminals and provide support to other departments, analyse information, protect federal institutions and critical infrastructures against cyberattacks and provide training to non-specialist employees of the BKA, as well as provide advice on relevant legal provisions (BKA-CC, n.d.).

The BKA is in communication with prosecutors and judges. The BSI has appointed a CSIRT-LE liaison officer to the BKA.

([23]) CERT-BPOL is listed in the ENISA inventory: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#team=CERT-BPOL

The German Federal Police is a (primarily) uniformed federal police force (Bundespolizei, n.d.). It is subordinate to the Federal Ministry of the Interior (Bundesminister des Innern, für Bau und Heimat (BMI), n.d.).

LE authority is also exercised at the state level: the criminal police offices of the *Länder* (Landeskriminalämter – LKAs) are independent LEAs in all 16 states (*Länder*) and are subordinate to the Ministry of the Interior. The state police are known as the *Landespolizei*. They are the main points of contact for cybercrime for most of the *Länder*. The '16 federal states (*Länder*) [have] the authority to maintain their own police forces within their territory, along with the right to pass legislation and exercise police authority' (BMI, n.d.).

4.3.1.4. Judiciary

Following the federal structure of Germany, 'the court system is also structured federally. Jurisdiction is exercised by federal courts and by the courts of the sixteen federal states (*Länder*). The main workload of the administration of justice lies with the *Länder*' (European Union, n.d.b).

The BGH (Federal Court of Justice) is at the head of the local, regional and higher regional courts and functions as a court of appeal for both civil and criminal cases. In general its interpretations of the law are adopted by all regional courts and therefore do have far-reaching effects on German jurisdiction in general.

'The prosecution offices are set up at every regional court' and 'are competent to investigate all kinds of criminal offences except of offences against the state and other offences falling withinthe competence of the Federal Public Prosecution Office'. […] 'On the federal level there is only one prosecution office, the Federal Public Prosecution Office which has its seat in Karlsruhe. In the area of investigation and prosecution of crimes, the Federal Public Prosecution Office is competent to investigate and prosecute crimes against the state and terrorist crimes as well as other cases, if they involve serious crime that goes beyond individual Länder borders' (EJN, n.d.a).

Certain State Prosecutor's Offices, such as the one in North Rhine-Westphalia, have a central cybercrime unit dealing 'with significant cybercrime proceedings' (Council of the European Union, 2017a, p. 28).

'There are no courts with specific jurisdiction in most of the Länder. In North Rhine-Westphalia, however, Cologne regional court has a criminal division with special jurisdiction on account of the Central Cybercrime Unit and Contact Point located at Cologne Public Prosecution office' (Council of the European Union, 2017a, p. 28). Indeed, as was also highlighted during one of the interviews conducted, 'Certain major courts have created special chambers with judges specifically trained in cybercrime cases (example of Chamber in the High Regional Court of Cologne).' For more information on this point see (Landgericht Köln, pp. 90, section 242, subsections c) and d)).

Germany cooperates with Eurojust and is a member of Eurojust's Cybercrime Network.

4.3.2. Synergies and potential interferences

As emerged from both the desk research and the interviews, there are several synergies between the communities, and the Cyber-AZ plays an important role in bringing the communities together and facilitating their synergies. For instance, as one of the interviewees explained, the different agencies that are part of this centre (BSI, BKA, BW-KdoCIR, BBK, BPOL, BfV, MAD and BND) have 'a daily interaction and coordination on handling and treating cases'. In addition, the agencies involved collaborate in 'producing situation reports to cover the different aspects of an incident, from the perspective and within the limits of each agency's [competence]'.

As emerged from the interviews, 'There is a daily flow of exchange of information [between CSIRTs and LE] for ongoing investigations and in the framework of analysing projects and indicating prevention measures.' For instance, the BSI may 'recover data and information from suspected systems', which could also be used to support LE investigations and 'be presented in Court as testimonies by BSI experts'.

As one of the interviewees explained, the current legal framework does not anticipate having CSIRT personnel permanently assigned to prosecution authorities. Instead, according to the German Code of Criminal Proceedings, the role that CSIRTs may play is either that of a witness or that of an expert. The CSIRT community can help prosecution authorities when there is a need for a qualified technical expert. Indeed, 'Even if the CSIRTs contacted do not have the specific qualified technical experts within their team, they can still support the prosecution authorities as they have many links in the technical community.' Moreover, CSIRTs can provide support to prosecution authorities by reaching out to civil organisations and non-governmental organisations, as they are in a better position to perform this task.

As one of the interviewees highlighted, 'The major field of interference during an investigation [between the different communities] is how to deal with the incident. The prosecution service aims at gathering proper judicial evidence, while the CSIRTs aim at dealing with the incident and fixing the issue. From the prosecutor's perspective, gathering evidence takes much longer time than the CSIRTs would want. In any major case the usual discussion is what can be done to gather evidence and close the collection process as soon as possible in order to proceed with the CSIRT activity of unlocking the system.'

AN EXAMPLE OF FACILITATING SYNERGIES

The **Nationales Cyber-Abwehrzentrum** (National Cyber Response Centre) plays an important role in bringing the communities together and facilitating their synergies.

4.3.3. Examples of training

The BKA has developed various national training programmes on cybercrime, including in the field of information and communication technology (ICT) forensics. The BKA is also responsible for training experts in the Federation and the *Länder*. As part of this training, it is possible to specialise in specific operating systems, networks/internet, mobile forensics and cryptology. The BKA also organises an internal basic training course on cybercrime once a year (Council of the European Union, 2017a).

Courses on cybercrime are offered at all levels, from basic to advanced/specialised, for all police officers and court experts in Germany.

The German Judicial Academy (Deutsche Richterakademie) also offers further training on criminal law and the internet on an annual basis and organises conferences and training on criminal law, forensics, criminal proceedings and investigative measures for judges and public prosecutors who are involved in combating internet crime (German Judicial Academy, n.d.).

The Brandenburg Judicial Academy (Justizakademie des Landes Brandenburg) organises regular training sessions for senior judiciary who handle cybercrime cases (Brandenburg Judicial Academy, n.d.). In addition, at a local level, training is organised (e.g. by the Joint Judicial Examination Office of the *Länder* of Berlin and Brandenburg) on combating cybercrime, including topics such as preservation of computer evidence, data network investigations, including a cross-border dimension, the challenges presented by big data and data protection-related issues.

At the Länder level, various training initiatives are offered for LE officers and prosecutors, such as in North Rhine-Westphalia, which organises 'a joint training programme for specialists from the Land police force and public prosecutors'. However, practices such as working meetings and exchange of information are more common between the police and the public prosecutor's offices on different aspects of combating cybercrime (Council of the European Union, 2017a). .

As emerged from the interviews, joint training takes place between the CSIRTs and LE, and, in particular, the Quick Reaction Force (QRF), with judiciary representatives also invited to participate in this training as observers.

As an interviewee explained, 'In a joint exercise/practical training on critical infrastructures, which was held with the support of a private company, a representative from the prosecution office was invited to actively participate and the prosecutor was then on call during the real-life scenario.' As another interviewee underlined, 'The judges are usually not involved in such joint trainings, also due to [their] obligation to remain neutral/impartial (e.g. there could be a conflict if a training is organised by a private entity or an exercise hosted in a company's premises).'

In addition, it should be noted that, as stated by one of the interviewees, the 'Prosecution team has the responsibility for providing State justice academy trainings to LE officials. Regarding the CSIRT community, prosecutors actively engage in seminars and training sessions also involving the BSI. Through these, they are trying to share the information by inviting CSIRT experts in such events or participating respectively in trainings of the CSIRT community.'

However, what emerged from the interviews is that CSIRTs and LE work closely together on a daily basis and that they 'have managed to learn from each other and understand each entity's role and actions'. Since CSIRTs and the judiciary – because of their mandates and the legal framework – do not have many opportunities to work so closely together, the judiciary could 'benefit greatly' if the CSIRT community could provide training for prosecutor and judges to further improve their technical skills.

4.4. LUXEMBOURG

Luxembourg 'is a parliamentary constitutional monarchy (Grand Duchy) with a head of government, the prime minister, and a head of state, the Grand Duke. The country is divided into 4 […] regions, 12 […] cantons and 105 communes' (European Union, n.d.d.).

In the following subsections, an overview of the main authorities involved in the response to cybercrime in Luxembourg is provided, synergies and possible interferences are discussed and examples of relevant training are provided. More information on the relevant Luxembourg legal framework can be found in Annex C.

Luxembourg adopted its NCSS in 2018 for the period 2018–2020 (ENISA, n.d.g).

4.4.1. Roles and duties

In Luxembourg, the following authorities and departments, in particular, are responsible for preventing, analysing and fighting cybercrime.

Name of the authority/department in English	Name of the authority/department in the original language	Abbreviation/short name in the original language (if applicable)
National Agency for the Security of Information Systems	Agence nationale de la sécurité des systèmes d'information	ANSSI
CERT.LU	CERT.LU	CERT.LU
Computer emergency response team of the Government of the Grand Duchy of Luxembourg	Équipe Gouvernementale de Réponse aux Urgences Informatiques	GOVCERT.LU
Computer Incident Response Center Luxembourg	Computer Incident Response Center Luxembourg	CIRCL

National CERT Luxembourg	National CERT Luxembourg	NCERT.LU
Grand-Ducal Police	Police Grand-Ducale	
High Commission for National Protection	Haut-Commissariat à la Protection Nationale	HCPN
Cybersecurity Board		CSB
Public Prosecution and Judges	Ministère de la Justice	

4.4.1.1. National cyber security agency

The National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information – ANSSI) is part of the High Commission for National Protection (Haut-Commisariat à la Protection nationale – HCPN) and is responsible for establishing information security policies and guidelines on non-classified information within the Luxembourg state bodies (ministries, state departments and administrations). ANSSI assists these bodies with risk analysis in the domain of information security, in order to help build up a culture of risk-based governance within the Luxembourg state, as required by the general information security policy. Furthermore, ANSSI is in charge of promoting information security awareness and may advise the Luxembourg state's training institute on training programmes in the domain of information security.

4.4.1.2. CSIRTs

National CERT Luxembourg (NCERT.LU), the CERT of the Government of the Grand Duchy of Luxembourg (Équipe gouvernementale de réponse aux urgences informatiques – GOVCERT.LU) and the Computer Incident Response Center Luxembourg (CIRCL) are the main actors responsible for the detection of and response to incidents.

NCERT.LU**,** run by GOVCERT.LU, is the national CSIRT (GOVCERT.LU, n.d.b). NCERT.LU gathers and disseminates information about security incidents that affect information and communication systems in Luxembourg. It also serves as interlocutor for natural and legal persons, entities and bodies, both national and international. Once it has received information, NCERT.LU must convey it to the CERTs in charge of the affected victim's sector or, if no sectorial CERT exists, directly to the victim. NCERT.LU also advises about the specific points of contact according to the targeted sector.

CERT.LU, run by SECURITYMADEIN.LU, is the Cyber Emergency Response Community Luxembourg (CERT.LU, n.d.). It is an initiative to enhance collaboration between public and private CERTs in Luxembourg. The objective is to create a community of all of the major actors for sharing expertise.

GOVCERT.LU**,** the governmental CSIRT, 'is the single point of contact dedicated to the treatment of all computer related incidents jeopardising the information systems of the government and defined critical infrastructure operators, whether they are public or private' (GOVCERT.LU, n.d.). The services provided by GOVCERT.LU include incident handling, coordination and resolution, and also proactive services such as notification of malware and vulnerabilities, as well as compromised (infected) systems, among others. 'The Constituency of GOVCERT.LU is made of:

- all ministries, administrations and services of the Luxembourgish government

- military organizations and administrations using a military system of the Luxembourgish government (e.g. embassies)
- critical infrastructure operators of the Grand-duchy of Luxembourg
- some major players in sensitive sectors within the Grand-duchy of Luxembourg' (GOVCERT.LU, n.d.a).

CIRCL 'is a government-driven initiative designed to gather, review, report and respond to computer security threats and incidents' (CIRCL.LU, n.d.). 'CIRCL is the CERT for the private sector, communes and non-governmental entities for the Grand Duchy of Luxembourg' (CIRCL.LU, n.d. b).

CIRCL provides incident response capacities and remediation to national ICT users. It also takes a coordinator's role during incidents involving multiple actors, both national and international. It is also charged with collecting information about incidents to enhance future responses. CIRCL also handles vulnerability management and disclosure and incident response training (CIRCL, 2020).

CIRCL has created a large number of tools applicable to forensics, incident responses, network analysis, dark web monitoring and threat intelligence. The most successful of these tools is MISP (Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing), which is a threat intelligence database with very large information-sharing capabilities. It is used by more than 6000 entities worldwide and is becoming a de facto standard in the CSIRT community.

CIRCL already has a strong LE cooperation culture through frequent informal exchanges and training programmes, such as the Horizon 2020 ENFORCE project and the NEOLEA initiative (CIRCL.LU, n.d. a).

The HCPN is a coordinating mechanism for responding to serious cyberattacks (HCPN, n.d.). It also includes a Cybernetic Risk Evaluation Cell (Cellule d'Evaluation du Risque Cybernétique) known as CERC (The Luxembourg Government, 2018).

4.4.1.3. LE

The Grand-Ducal Police (Police Grand-Ducale, n.d.) is the primary LEA in Luxembourg.

The Directorate of the Judicial Police Service (SPJ) 'is responsible, inter alia, for the Coordination of judicial activities at the national and international level. It is also responsible for defining and managing, in collaboration with the judicial authorities, judicial investigations.' Within the SPJ the Department of Property Crime has a section on cybercrime (OSCE, n.d.a). The SPJ is composed of two units:

- Cybercrime Unit. This unit deals with pure cybercrime mainly against ICT systems. It handles felonies such as data theft, modification and erasure, as well as cyberbullying and property scam. It is the international point of contact for Europol, Interpol and 24/7 networks.
- High Tech Analysis Unit. This unit provides forensic support to other police units. It handles lawful evidence collection, interception management and maintenance for audio/video special equipment.

To prevent and combat cybercrime, LE in Luxembourg cooperates with the following authorities:

- Principal Public Prosecutor's Office (mutual legal assistance);
- Public Prosecutor (investigation and prosecution)/Parquet général;
- Office of the Examining Magistrate (preparatory enquiries and enforcement action);

- Financial Intelligence Unit (financial crime using new technologies);
- criminal courts.

4.4.1.4. Judiciary

The judicial system of Luxembourg is 'divided into a judicial branch', including the criminal courts, 'and an administrative branch' (European Union, n.d.e).

Some magistrates from the Public Prosecutor's Office and a magistrate at the level of the Financial Intelligence Unit are responsible, among other duties, for cybercrime cases.

Luxembourg also cooperates with Eurojust and is a member of Eurojust's Cybercrime Network.

4.4.2. Synergies and potential interferences

The different communities in Luxembourg have a strong tradition of cooperation and collaboration. The CSIRT/LE and judiciary cybercrime working group brings together national authorities (Public Prosecutor's Office, LE and CSIRTs) to exchange information regularly, for instance on their interactions with service providers.

The police rely on mutual legal assistance instruments and the direct exchange of information with Europol and Interpol, but also on the voluntary sharing of information by communication service providers.

An interesting case of synergies was mentioned during the interviews. This was a case 'where the LE performed a significant data interception, that CSIRTs were not allowed to do but onwards CSIRTs supported in analysing this data package. Similarly, [synergies are achieved] in cases of seizing of equipment performed by the LE, later on, analysed with the support of CSIRTs.'

An example of synergies in developing training was also provided during the interviews, in the context of the ENFORCE project (CIRCL.LU, n.d. a) during the training, CSIRT technologies were shown and feedback from the LE received and improvements in tools.

CSIRTs (such as CIRCL) can provide technical pre-investigation and investigation support before LE intervention. They also support requests from the judiciary and other LEAs for technical assistance.

Information sharing is carried out automatically using MISP, using sharing groups to implement information sharing rules. Specific information regarding financial fraud is shared with the judiciary.

Main synergies occur through cooperation between CSIRTs and LEAs. LEAs have legal tools to enable data acquisition by seizing and intercepting servers. Other synergies can be handled during training (see below).There is a memorandum of understanding between CSIRTs and LE.

Potential interferences can occur when LEAs and CSIRTs come into conflicts. LEAs may disturb CSIRT monitoring operations when seizing a piece of infrastructure studied by CSIRTs.

Outside the EU, the use of Mutual Legal Assistance Treaty (MLAT) can cause extensive delays and impede cooperation.

Another challenge is the discrepancy in data-handling capacities. CSIRTs generate a lot of data, for example in the field of child abuse. Since LEAs works on a case-by-case model, they cannot handle large numbers of data without predefined agreements.

TRADITION OF ACHIEVING SYNERGIES

The different communities in Luxembourg have a strong tradition of cooperation and collaboration.

The final challenge is to improve evidence handling by MISP: large data sets need to be handled in such a way as to preserve the chain of custody.

One way to improve synergies would be to share information in real time. This is legally challenging but would be more profitable for all entities.

4.4.3. Examples of training

'Law enforcement officers are trained at the Police school of the Grand-Ducal Police. […]. In addition, the Police school is responsible for managing the continuing education of the personnel of the Grand-Ducal Police' At the Police School, cybercrime is covered during basic training and professional development for police officers and investigators (OSCE, n.d.a).

To increase opportunities to provide specialised training to IT forensic experts and investigators working on cybercrime cases, the SPJ arranges training in coordination with neighbouring police agencies. It is also common practice for personnel attending external training to pass on their knowledge to others by organising internal training sessions.

Luxembourg 'does not have a specific institution or school for the training of its judges and prosecutors, therefore, the Ministry of Justice has reached an agreement with the French Ecole Nationale de la Magistrature and the German Judicial Academy' (Deutschen Richterakademie) (EJTN, n.d.).

In addition, the New Technologies Section of the SPJ provides training for judges, especially on new tools and methods used by cybercriminals (darknet, bitcoin, etc.).

In the interviews, further examples of training were discussed. For example, when customers share their issues and needs in the field of cybercrime, this helps CSIRTs understand the requirements of cybercrime investigations. Further, the Prosecutor's Office also provides training related to the four ways of filing a complaint for a CSIRT's constituency.

As emerged from the interviews, 'There is a set of training that is already provided by CSIRTs to LE, i.e. for OSINT [open-source intelligence], cryptographic keys ([…] published under the ENFORCE project) and forensic tools, including forensics acquisition. There are cases of prosecutors and judges that joint such trainings, as they had a demonstrated interest in the field'

LE and CSIRTs also participate in training exercises provided by the ENFORCE Project. The ENFORCE project is a 'European project co-funded by the European Commission in the framework of the Internal Security Fund – Police. […]. The ENFORCE project aims at designing, setting-up, and disseminating a cybercrime training curriculum at the European level. This curriculum will be validated during a training exercise allowing different European public (e.g. law enforcement agencies and CSIRTs) and private actors fighting cybercrime to train together using state-of-the-art training technology'. CEIS, the coordinator of the ENFORCE Project, also co-organizes a cybercrime training with the Luxembourgian CIRCL and the French National Police" (CEIS, n.d.). This training material specifically addresses aspects of cooperation.

According to the data collected during the interviews, CSIRTs have received training from the Customs Authority. This was in the form of a workshop, where the Customs Authority shared concerns related to cybercrime and was able to discuss how CSIRTs can help (e.g. when seizing equipment at the borders and how this should be handled before being submitted for analysis

4.5. NORWAY

Norway is a constitutional monarchy and a member country of EFTA and a signatory to the European Economic Area (EEA) Agreement (EFTA, n.d.a), (EFTA, n.d.).

In the following subsections, an overview of the main authorities involved in the response to cybercrime in Norway is provided, synergies and possible interferences are discussed and examples of relevant training are provided. More information on the relevant Norwegian legal framework can be found in Annex C.

Norway adopted a new NCSS in 2019; this is the fourth edition of the NCSS, with the first strategy published in 2003 (ENISA, n.d.i) (Norwegian Ministeries, n.d.).

4.5.1. Roles and duties

In Norway, the following authorities and departments, in particular, are responsible for preventing, analysing and fighting cybercrime.

Name of the authority/department in English	Name of the authority/department in the original language	Abbreviation/short name in the original language (if applicable)
Norwegian Computer Emergency Response Team		NorCERT
National Criminal Investigation Service	Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet	Kripos
Norwegian National Security Authority	Nasjonal sikkerhetsmyndighet	NSM
Norwegian National Cyber Security Centre	Nasjonalt cybersikkerhetssenter	NCSC
National Authority for Investigation and Prosecution of Economic and Environmental Crime	Den sentrale enhet for etterforsking og påtale av økonomisk kriminalitet og miljøkriminalitet	Økokrim
Norwegian Police Security Service	Politiets sikkerhetstjeneste	PST
Norwegian Prosecuting Authority	Påtalemyndigheten	
Judicial system		
Joint Cyber Coordination Centre	Felles cyberkoordineringssenter	FCKS
Norwegian Data Protection Authority	Datatilsynet	
Norwegian Communications Authority	Nasjonal kommunikasjonsmyndigheit	Nkom

4.5.1.1. National cyber security agency

The Ministry of Justice and Public Security is primarily the responsible authority for network and information security in Norway. The Norwegian National Security Authority (Nasjonal sikkerhetsmyndighet – NSM) is the national organisation focusing on cybersecurity in the country. Under the NSM, organisations run different functions related to cybersecurity and cybercrime, such as the Norwegian CERT (NorCERT) and the Norwegian National Cyber Security Centre (Nasjonalt cybersikkerhetssenter – NCSC) (NSM, n.d.).

4.5.1.2. CSIRTs

Norway has an officially recognised national and governmental CSIRT (NSM, n.d.). The NSM is responsible for NorCERT.

The main activities of NorCERT are “response to cyber threats in our technical threat operation centre 24/7; operate and organise a national sensor network on the internet to detect data breaches in critical infrastructure across sectors; reverse engineering, forensics, network analysis and counterintelligence” (NCSC, n.d.).

In addition, Norway has different sectorial CSIRTs, such as:

- HelseCERT, which supports the Norwegian healthcare sector (HelseCERT, n.d.)
- UNINETT CERT, of the UNINETT ‘ICT infrastructure company in Norway’ (UNINETT, n.d.) (UNINETT , n.d a).
- UiO-CERT, the University of Oslo’s CSIRT (UiO-CERT, n.d.);
- FinansCERT, the CSIRT supporting the Norwegian financial sector (FinansCERT, n.d.).

4.5.1.3. LE

The Norwegian Police Security Service (Politiets sikkerhetstjeneste – PST) is the national security service of Norway. The activities of the PST are assigned by the Police Act and it reports directly to the Ministry of Justice and Public Security.

The main aim of the National Criminal Investigation Service (Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet – Kripos) is to prevent and combat serious organised crime. Its main functions are criminal investigations, forensic investigations, gathering criminal intelligence and undertaking international police cooperation (Politiet, n.d.). The National Cybercrime Centre (NC3) falls under Kripos. The main activities of NC3 fall under the following areas: cybercrime investigations, digital forensics, internet investigations and internet crimes against children (Politiet, n.d. a). Within Kripos there is also a high-tech crime division that acts as a 24/7 point of contact.

The National Police Directorate is the highest police authority in Norway and ‘falls under the Ministry of Justice and Public Security’. The National Police Directorate supports police bodies and special units and provides expertise (Politiet, n.d.c)

As emerged from one of the interviews conducted, in relation to cybercrime, the role of the national police in Norway, in particular Kripos, is prevention and investigation and intelligence gathering. For LEAs in Norway, fighting cybercrime is no different from fighting other crimes.

Prosecutors are integrated into LEAs, sharing the same offices with LE personnel; hence, there is a seamless exchange of information and close cooperation between the two. On the legal framework side a specific Police Act allows police to share information with the national CERT to prevent criminal activities.

4.5.1.4. Judiciary

The Norwegian Prosecuting Authority (Påtalemyndigheten) is the competent authority for legal prosecutions in Norway. It handles investigations and prosecutions of criminal cases.

The Norwegian Prosecuting Authority is divided into the following levels:

- the Director of Public Prosecutions (DPP);
- the Regional Public Prosecution Offices (PPO);
- the Prosecuting Authority in the Police (Higher Prosecuting Authority, n.d.)

The National Authority for Investigation and Prosecution of Economic and Environmental Crime (Den sentrale enhet for etterforsking og påtale av økonomisk kriminalitet og miljøkriminalitet – Økokrim) provides services as a police unit but also as a prosecution authority with specific expertise in computer crime and fraud (Økokrim, n.d.).

In Norwegian judicial system, the supreme court 'is the highest court in Norway […] and has an authority in all areas of the law' (Domstol, n.d.). Judicial cooperation in criminal matters with EU Member States is based on the principles of mutual recognition and direct contact between the judicial authorities.

Norway also cooperates with Eurojust and is a member of Eurojust's Cybercrime Network.

4.5.2. Synergies and potential interferences

As mentioned above, Økokrim, because of its dual nature as a police unit and a prosecution authority, cooperates with a number of other authorities, such as surveillance authorities, the business sector, in combating economic and environmental crime.

In addition, the Joint Cyber Coordination Centre (Felles cyberkoordineringssenter – FCKS) is a key collaborative hub that consists of representatives from the NSM, the Norwegian Intelligence Service, the PST and Kripos. The FCKS is also coordinated by the NSM (FCKS, n.d.).

NC3 cooperates closely with public and private security entities in Norway and abroad, especially regarding the exchange of information (Politiet, n.d.b). Cooperation mechanisms have also been established between LE and NorCERT.

The interviews showed that a lot of synergies are established in tactical operations and at strategic levels. There are cases of LEAs and national CERTs attending crime scenes together and conducting investigations together, to complement each other's capabilities. For instance, if information is discovered by LE that is deemed important for a national CERT, this information is passed on to the CERT. Joint reports are prepared and submitted to the government in the field of cybercrime, including on risks. Another example is LEAs and CERTs discussing and analysing the issues together. Through the Joint Cyber Coordination Centre, prosecutors hold monthly meetings with the legal officers of the CERT communities.

ESTABLISHED SYNERGIES

Through the Joint Cyber Coordination Centre, prosecutors hold monthly meetings with the legal officers of the CERT communities.

However, as emerged in the interviews, there are also potential interferences. In one example, in the early stages of cooperation the national CERT found a CC server abroad and passed the information to the hosting country. The hosting country could have decided to shut down the server, which may have been problematic for the LEA and its operational plan.

4.5.3. Examples of training

"The Norwegian Police University College (/Politihøgskolen – (NPUC) 'is the central educational institution for the police service in Norway. Basic training for police officers is a three-year university college education aimed at providing a broad practical and theoretical foundation'. The college provides education in areas such as 'policing, crime investigation and prevention, and prosecution and administrative responsibilities' (OSCE, n.d.b.).

The college also provides training in areas such as:

- international civil crisis management;
- Schengen Border and Immigration Service;
- Nordic Baltic Police Academy (NPUC, n.d.) (OSCE, n.d.b.).

The NPUC is also a member of the European Cybercrime Training and Education Group (ECTEG) (ECTEG, n.d. a).

The Norwegian Center for Cyber and Information Security (CCIS) develops cybersecurity competences for Norwegian agencies, companies and academia. It is supported by the Ministry of Justice and Public Security and members of its board of directors come from authorities such as the NSM, the Police Directorate and the NPUC, among others (CCIS, n.d.).

From the data collected in the interviews, it emerged that the different communities (CSIRTs, LE and judiciary) participate in shared exercises with the North Atlantic Treaty Organization (NATO), as well as other national exercises held by private partners. LEAs also participate in such training activities along with the private sector, mostly in the telecoms field.

NC3 organises training for LEAs as well as prosecutors.

4.6. PORTUGAL

Portugal is 'a semi-presidential republic with a head of government, the prime minister, and a head of state, the president, who has power to appoint the prime minister and other government members. The country is administratively divided into 308 municipalities, subdivided into 3 092 civil *parishes'* (European Union, n.d.i.).

In the following subsections, an overview of the main authorities involved in the response to cybercrime in Portugal is provided, synergies and possible interferences are discussed and examples of relevant training are provided. More information on the relevant Portuguese legal framework can be found in Annex C.

Portugal adopted its first NCSS in 2015. In 2019, the Portuguese government issued the NCSS for 2019–2023 (ENISA, n.d.j).

4.6.1. Roles and duties

In Portugal, the following authorities and departments, in particular, are responsible for preventing, analysing and fighting cybercrime.

Name of the authority/department in English	Name of the authority/department in the original language	Abbreviation/short name in the original language (if applicable)
CERT.PT	CERT.PT	CERT.PT
CC-CRISI, Portuguese Armed Forces	CC-CRISI, Estado Maior General das Forças Armadas	CC-CRISI, EMGFA
Portuguese National Cybersecurity Centre	Centro Nacional de Cibersegurança	CNCS
National Communications Agency	Autoridade Nacional de Comunicações	ANACOM ([24])
Judicial Police	Polícia Judiciária	PJ
Public Security Police	Polícia de Segurança Pública	PSP
National Unit to Combat Cybercrime and Technological Crime	Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica	UNC3T

([24]) For a description of the role of ANACOM see below Section 4.6.2.

Internal Intelligence Service	Serviço de Informações de Segurança	SIS
Prosecutor General's Office	Procurador-Geral da República	PGR
Public Prosecution Service	Ministério Público	MP
Central Department of Criminal Investigation and Prosecution	Departamento Central de Investigação e Ação Penal	DCIAP
Judicial system		

4.6.1.1. National cyber security agency

The Portuguese National Cybersecurity Centre (Centro Nacional de Cibersegurança – CNCS) (CNCS, n.d.) monitors and coordinates the implementation of the NCSS and is the single point of contact. Its main focus is informing and raising the awareness of not only public entities and critical infrastructures but also the business sector and civil society.

4.6.1.2. CSIRTs

Portugal has an officially recognised national CSIRT, CERT.PT (CNCS, n.a.a). CERT.PT 'is a service integrated in the Portuguese National Cybersecurity Centre that coordinates the response to incidents involving State entities, operators of Critical infrastructures, operators of essential services, digital service providers and, in general, the national cyberspace, including any device belonging to a network or address block attributed to an operator of electronic communications, institution, collective or singular person based, or physically located, in Portuguese territory' (CNCS, n.a.a). Its mission is to enhance national capacity in cybersecurity by creating new CSIRTs and developing the capacities of existing ones. CERT.PT is a member of the National CSIRT Network and a national representative in the CNW.

CC-CRISI is the CSIRT for the Portuguese Armed Forces Estado Maior General das Forças Armadas – EMGFA) (EMPFGA, n.d.).

4.6.1.3. LE

The Judicial Police (Polícia Judiciária, n.d.) investigates violent crime, organised crime and financial crime. It is 'a higher criminal police force falling under the Ministry of Justice. Its mission is to assist judicial and prosecuting authorities with investigations and to develop and foster preventive, detection and investigative actions, falling within its remit or entrusted with by the competent judicial and prosecuting authorities. […]. Polícia Judiciária is also responsible for ensuring the operation of the Europol National Unit and the Interpol National Central Bureau, within the framework established by national legislation" (Europol, n.d.b).

With the aim to fight against cybercrime, the Judicial Police established in February 2017 the National Unit to Combat Cybercrime and Technological Crime (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica), also known as UNCT3. A specialised team within the UNCT3 supports criminal investigations with technical and legal aspects (Polícia Judiciária , n.d.).

The Public Security Police (Polícia de Segurança Pública – PSP) is responsible for maintaining security and public order and investigating non-organised crimes and violent crimes (PSP, n.d.).

The Internal Intelligence Service (Serviço de Informações de Segurança – SIS, (SIS, n.d.) produces security intelligence to assist political decision-makers in fighting cybercrime, among other crimes. To accomplish its mission, the SIS is supported by all of the security and LEAs and public authorities in general.

According to the data collected in the interviews, the organisation in Portugal in charge of cybercrime is Judicial Police, the police force that deals with anti-corruption, counter-terrorism, drug prevention and serious cybercrime.

Since the transposition of the NIS Directive, a new national law (Cybersecurity law) mentioned the needs of cooperation between the Portuguese CERT (the Portuguese national CERT is within the Cyber Centre) and other national CSIRTs. In addition, there is a clause in the law stating that the CNCS and the national criminal police should cooperate. This group involves four entities (known as G4): (1) the CNCS, (2) the Judicial Police, (3) the Cyber defence and (4) intelligence services. The G4 group collaborates with cyber diplomacy, a body within the Ministry of Foreign Affairs, which is also tasked with supporting national services with information exchange in the EU space.

However, magistrates are not part of the G4 group because they have their own powers and can act directly/ask LE and the CNCS for services and information. They are therefore not explicitly mentioned in the legal act. Members of the G4 group have regular meetings and occasionally, if needed, undertake joint operations.

4.6.1.4. Judiciary

The Portuguese judicial system 'has two separate sets of courts, the civil courts and the administrative courts. Provision is also made for other courts, such as the Constitutional Court. In the civil sphere, the ordinary courts with civil and criminal jurisdiction are the judicial courts' (European Union, n.d.j).

The Public Prosecution Service (Ministério Público – PPS) (PPS, n.d.) is the Portuguese prosecution authority. Within the PPS, the Prosecutor General's Office (Procurador-Geral da República – PGO) (PGO, n.d.) acts as the central authority for international judicial cooperation in criminal matters. In addition, within the PPS, the Central Department of Criminal Investigation and Prosecution (Departamento Central de Investigação e Ação Penal – DCIAP) (DCIAP, n.d.) is a body entrusted with the coordination of the investigation of organised crime, as well as crime prevention.

Portugal cooperates with Eurojust and is a member of Eurojust's Cybercrime Network.

4.6.2. Synergies and potential interferences

'The National Cybersecurity Centre is the operational coordinator and the Portuguese national authority specialised in cybersecurity working in this field with State entities, operators of Critical Infrastructures, operators of essential services and digital service providers, ensuring that the cyberspace is used as an area of freedom, security and justice, for the protection of all the sectors of society that materialize national sovereignty and the Democratic State under the rule of law' (CNCS, n.d.b).

ANACOM (National Communications Authority, Autoridade Nacional de Comunicações) is the regulator, supervisor and representative of the communications sector in Portugal. The authority is responsible for ensuring compliance with the Electronic Communications Law (ANACOM, n.d.). In terms of criminal investigations, there is close cooperation between ANACOM, the Judicial Police and the Prosecutor General's Office on combating cybercrime and obtaining digital evidence (ANACOM, n.d a).

As highlighted by one of the interviewees, 'Nothing prevents the cooperation between CSIRTs, LE and […judiciary]. However, there are no particular laws in place'. 'CSIRTs officers have the obligation to report malicious/suspicious events to the prosecution service', which derives from the general rule stating that all 'public institutions have the obligation to cooperate with the LE and the prosecution service during criminal investigations'.

CERT-PT 'coordinates the response to incidents involving State entities, operators of essential services, operators of national critical infrastructures and digital service providers'. In addition, the National Unit to Combat Cybercrime and Technological Crime (UNC3T) collaborates and directly supports the actions of prevention, detection and mitigation developed by national entities (Polícia Judiciária , n.d.). Finally, the Internal Intelligence Service (SIS, n.d.) collaborates closely with LEAs and public authorities, as well as providing support when this is requested.

As emerged from the interviews, one example of synergy is the sharing of methodologies: both CSIRTs and LEAs run regular laboratories and/or joint exercises and share methodologies. Another example is the sharing of information: LEAs frequently share indicators of compromise or indicators of threat with the other G4 members through the communication channel to verify the information. There are also synergies across the different communities with regard to training: the police provide lectures to the school of magistrates and criminal police schools, as well as annual lectures to magistrates and the academic community.

SYNERGIES IN MULTIPLE LEVELS

Examples of synergies include sharing of methodologies, sharing of information and training activities.

Nevertheless, addressing cybersecurity means dealing with the global security of cyberspace and sometimes there is an overlap between the CNCS and the police. For example, if a CSIRT decides to bring down ('takedown procedure') a botnet without consulting a LEA that may be in the process of investigating it, this can cause disruptions. The G4 group was created to try and avoid conflicts and overlapping activities, and weekly meetings increase the levels of communication between the parties.

4.6.3. Examples of training

The CNCS ensures that suitable training activities are provided to the CSIRT community, including but not limited to training sessions for CSIRT operators and coordination of national cybersecurity exercises and participation to international cybersecurity exercises. In addition, the CNCS supports the establishment of new CSIRTs, defines the required capabilities and circulates best practices for the handling of cybersecurity incidents (CNCS, n.d.c.).

In terms of LE training, the PSP offers both training/teaching courses at a basic level and specialised courses. The courses are taught by the Higher Institute of Police Sciences and Internal Security (Instituto Superior de Ciências Policiais e Segurança Interna – ISCPSI) (ISCPSI, n.d.) and the Police Training School (Escola Prática de Polícia). The Police Training School provides training in criminal investigations. In addition, UNC3T is responsible for ensuring collaboration and direct participation in initial and ongoing training on cybercrime for staff involved in criminal investigations and in supporting the Judicial Police.

The Centre for Judiciary Studies (Centro de Estudos Judiciários – CEJ) (CEJ, n.d.) provides training for the judiciary on cybercrime and digital evidence, as well as on cyber components of the penal code and criminal investigations, aiming to provide to all judges and prosecutors a minimum level of knowledge and information on cybercrime. As reported during one of the interviews, "The judiciary community has established initiatives that usually try to involve experts from the other communities in their training activities (provided for prosecutors, judges, sometimes lawyers and LE). This is a common practice as they have observed the benefits of such an exchange.' This will also help 'to ensure that judiciary experts provide guidance to CSIRTs'.

The interviews revealed that CSIRTs and LE carry out joint exercises; however, in 2020 any planned training was not held because of the coronavirus disease 2019 (COVID-19) pandemic. The judiciary (prosecutors and judges) do not currently participate in such activities. The interviewees noted that CSIRTs and LE want to find a common approach. Once this is accomplished, they will expand the training to the judiciary community as well.

From the data collected in the interviews, it emerged that LE personnel participate in civil postgraduate programmes (legal or engineering programmes). Efforts are also being made to

provide more engineering courses to legal actors and more legal knowledge to engineers and set up links with the academic community. This is something that LE supports heavily through liaising with professors and students to inspire collaborations. LE participates in lectures on cybercrime law, digital forensics, ethics, etc.

As indicated in the interviews, the CNCS delivers such training online along with awareness courses for the public. LEAs receive training provided by the school of magistrates and criminal police schools, with the CNCS also providing annual lectures to magistrates.

4.7. ROMANIA

Romania is 'a semi-presidential republic with a head of government – the prime minster – and a head of state – the president. The country is divided into 41 counties and the municipality of Bucharest' (European Union, n.d.h).

In the following subsections, an overview of the main authorities involved in the response to cybercrime in Romania is provided, synergies and possible interferences are discussed and examples of relevant training are provided. More information on the relevant Romania legal framework can be found in Annex C.

Romania adopted its NCSS in 2013 (ENISA, n.d.k) and legislation that transposes the EU NIS Directive (Law No 362/2018) in 2018 (CERT RO, 2020).

4.7.1. Roles and duties

In Romania the following authorities and departments, in particular, are responsible for preventing, analysing and fighting cybercrime.

Name of the authority/department in English	Name of the authority/department in the original language	Abbreviation in the original language (if applicable)
Romanian National Computer Security Incident Response Team	Centrul Național de Răspuns la Incidente de Securitate Cibernetică	CERT-RO
Cyber Security Incident Response Center	Centrul de Răspuns la Incidente de Securitate Cibernetică	CERT-MIL
Operational Response Centre for Security Incidents	Centrul Operațional de Răspuns la Incidente de Securitate	CORIS-STS
National Cyberint Center	Centrul Național Cyberint	
General Inspectorate of Romanian Police	Inspectoratul General al Poliţiei Române	IGPR
Directorate for Investigating Organised Crime and Terrorism	Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism	DIICOT
Judicial system		

4.7.1.1. National cyber security agency

The implementation of the NCSS in Romania is coordinated by the Chancellery of the Prime Minister.

In Romania, there are multiple cybersecurity authorities. Currently, the Romanian National Computer Security Incident Response Team (Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO) (CERT-RO, n.d.) no longer operates under the Ministry of Communication and Information Society (MCSI), but is coordinated by the Chancellery of the Prime Minister (Portal Legislativ, n.d.). According to the law transposing the NIS Directive (Law No 362/2018), CERT-RO is the national competent authority for network and information systems and has an operational role (CERT RO, 2020).

4.7.1.2. CSIRTs

Romania has an officially recognised national CSIRT: **CERT-RO** 'is the National CERT of Romania, established as an independent structure for research, development and expertise in the field of cyber-security. It is a specialized organization responsible for preventing, analysing, identifying and reacting to cyber incidents. CERT-RO is the national contact point for similar structures. CERT-RO is responsible for elaborating and distributing public politics for prevention and counteracting the incidents that occur within national cyber infrastructures' (CERT-RO, n.d. a).

CORIS-STS (Operational Response Centre for Security Incidents, Centrul Operațional de Răspuns la Incidente de Securitate) is the Romanian governmental CSIRT and is part of the Romanian Special Telecommunications Service (STS). This CERT 'is designated to prevent and respond to security incidents related to information and communications systems of the Special Telecommunications Service and its clients' (CORIS-STS, n.d.).

CERT-MIL (Cyber Security Incident Response Center, Centrul de Răspuns la Incidente de Securitate Cibernetică) (CERT-MIL, n.d.) is the Romanian Military CSIRT, under the Ministry of Defence CSIRT, and is responsible for the management of cybersecurity incidents in the relevant cyber infrastructures, ensuring their detection, investigation and response in accordance with the regulations and procedures in force under the Ministry of National Defence. It was established in 2007 within the Ministry of National Defence and since 2020 has been the responsibility of the Cyber Defence Command.

The **National Cyberint Centre** (Centrul Național Cyberint) is the cyber intelligence centre of the Romanian Intelligence Service (SRI). Its main focus is on counter-espionage, economic security, transnational threats and the protection of classified information. The SRI focuses on cyberattacks, including those that originate in other states, and cybercrime groups, which may also be associated with terrorist organisations or extremists (hacktivists) (SRI, n.d.).

4.7.1.3. LE

The Central Cybercrime Unit within the **Romanian Police** (Politia Romana, n.d.) is the primary LEA dealing with cybercrime, with local capacities as well. More specifically it deals with:

- online fraud and fraud committed with electronic payment instruments;
- digital forensics;
- online child abuse;
- computer-related crimes (crimes against/through computer systems; unauthorised computer/data access or data transfer).

It is a specialised unit (Politia Romana, n.d.a), with general territorial competence, that is involved in combating and coordinating the fight against organised crime, including cybercrime, at the national level. The activities carried out by the Directorate for Combating Organized Crime include*:*

- Operational activity
- Control, support and guidance decisive in obtaining results at territorial level
- Information and decision support
- International representation/training (Politia Romana, n.d.a).

The challenges facing this specialised unit in 2020 are phishing campaigns/mobile malware distribution related to COVID-19, ransomware attacks on health facilities/hospitals, attacks against critical infrastructure holding personal data on COVID-19 patients, online fraud and SIM SWAP scams (Council of Europe, 2020).

4.7.1.4. Judiciary

The supreme court in Romania is the High Court of Cassation and Justice. The judicial authorities are divided by the regional and specialised jurisdiction (European e-Justice Portal , n.d.)

In Romania, the issuing and execution of the request for international judicial cooperation in criminal matters is under the competence of the courts and prosecution offices (EJN, n.d.a).

The Ministry of Justice, the Prosecutor's Office of the High Court of Cassation and Justice and the Ministry of Internal Affairs have responsibility for international judicial cooperation in criminal matters (EJN, n.d.).

Romania cooperates with Eurojust and is a member of Eurojust's Cybercrime Network.

4.7.2. Synergies and potential interferences

'National cyber security system (NSCC) is the general framework of cooperation which brings together public authorities and institutions with responsibilities and capabilities in the field in order to ensure coordination of actions at national level for cyberspace security, including through cooperation with academia and business, professional associations and organizations NGOs' (CERT-RO, n.d.b).

Romania has developed official programmes for cybersecurity interagency cooperation and information sharing, with CERT-RO playing a major role. CERT-RO has 'signed a Memorandum of Understanding (MoU) and Protocols with public institutions in the cybersecurity field' (ITU, n.d.).

The Romanian CSIRT, LE and judiciary are cooperating on cybercrime cases under the national legal framework, which is expected to be updated to provide further support for this kind of cooperation, for example to stipulate in the criminal procedure code that CERT-RO could be called to provide expertise to the Prosecutor's Office and in court.

One example of this cooperation is the Romanian CSIRT, LE and judiciary working together to fight banking/financial malware (botnets) affecting Romanian citizens and financial institutions.

In terms of synergies, CERT-RO and the Romanian Police are working together to continuously adapt the framework for information exchange and cooperation. One important aspect of this is the tools needed to support the cooperation framework, and here CERT-RO has made important steps recently by implementing a National Cybersecurity Services Platform (NCSP) that can be used by all stakeholders: LEAs, CSIRTs, internet service providers, public and private partners, and other authorities.

Another common objective is to assure that technical training is provided for those who work in the areas of cybersecurity and cybercrime. CERT-RO also has a leading role here by organising regular technical workshops and seminars for all relevant stakeholders.

SYNERGIES IN FIGHTING CYBER THREATS

The Romanian CSIRT, LE and judiciary cooperate in fighting cyber threats affecting the national IT infrastructure, citizens and organisations.

Possible interferences have been reduced drastically as a result of recent developments in implementation of an optimal cooperation framework between the CSIRT, police and judiciary. Some interferences may still occur in cybercrime investigations, mainly because of the different focuses that these communities have, i.e. incident mitigation (CSIRTs) compared with evidence preservation and criminal prosecution (LE and judiciary).

4.7.3. Examples of training

Since 2017, a national cyber exercise called CyDEX has been organised by the SRI through its National Cyberint Center, in cooperation with the national CSIRT (CERT-RO), the Ministry of Defence, the Military Technical Academy, the STS, the Protection and Guard Service and organisations form different private sectors. The latest exercise included participants from more than 90 organisations in the public and private sector, including CSIRTs, LE and the judiciary.

Training for LE at a foundational level and at advanced levels is provided by the Police Academy and the Police Officers School in Romania.

The training of judges and public prosecutors is the responsibility of the Ministry of Justice. Since 2004, the Ministry of Justice, through its website, has made available guides and useful information on judicial cooperation, such as handbooks and manuals, for Romanian judges and prosecutors (Romanian Ministry of Justice, n.d.).

In addition, the Romanian Centre of Excellence for Cybercrime Investigation (CYBEREX-RO) offers training to those organisations working to combat cybercrime in Romania, such as CERT-RO, the General Inspectorate of Romanian Police (Inspectoratul General al Poliţiei Române – IGPR) – Fraud Investigations Directorate (GIRP-FID, n.d.), the Prosecutor's Office attached to the High Court of Cassation and Justice (POHCCJ, n.d.), the National Institute for Magistracy (NIM, n.d.), the Police Academy and others (European Commission, n.d.).Currently, there are no examples of joint training between the three communities.

4.8. SWEDEN

Sweden is 'a constitutional monarchy and parliamentary democracy with a head of government – the prime minister – and a head of state – the monarch. Sweden is a unitary state, divided into 20 counties and 290 municipalities' (European Union, n.d.k.).

In the following subsections, an overview of the main authorities involved in the response to cybercrime in Sweden is provided, synergies and possible interferences are discussed and examples of relevant training are provided. More information on the relevant Swedish legal framework can be found in Annex C.

Sweden adopted its NCSS in 2017, followed by a comprehensive cyber security action plan for the period 2019–2022 (ENISA, n.d.l) (Swedish Government, n.d.).

4.8.1. Roles and duties

In Sweden the following authorities and departments, in particular, are responsible for preventing, analysing and fighting cybercrime.

Name of the authority/department in English	Name of the authority/department in the original language	Abbreviation in the original language (if applicable)
CERT-SE	Sveriges nationella Computer Security Incident Response Team	CERT-SE
Swedish Civil Contingencies Agency	Myndigheten för samhällsskydd och beredskap	MSB
National Defence Radio Establishment	Försvarets radioanstalt	FRA
Swedish Defence Materiel Administration	Försvarets materielverk	FMV
Swedish Armed Forces	Försvarsmakten	FM
Swedish Post and Telecom Authority	Post-och telestyrelsen	PTS
Swedish Police Authority	Polismyndigheten	
Swedish Security Service	Säkerhetspolisen	SÄPO
Swedish Prosecution Authority	Åklagarmyndigheten	
Swedish Economic Crime Authority	Ekobrottsmyndigheten	
Swedish National Courts Administration	Domstolsverket	

4.8.1.1. National cyber security agency

The Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskaps – MSB) is the responsible authority for network and information security in Sweden (MSB, n.d.). The cybersecurity action plan of Sweden contains measures that the MSB will undertake, along with the authorities mentioned above in Section 4.8.1.

4.8.1.2. CSIRTs

CERT-SE is the officially recognised national and governmental CSIRT (CERT-SE, 2015). The MSB is the authority that operates the national CERT.

CERT-SE also collaborates with the military CERT of Sweden, Försvarsmakten FM-CERT (FM-CERT, n.d.) (Council of the European Union, 2017b).

SUNet-CERT is the Swedish University Network CERT. It supports academic and educational institutions as well as other organisations connected to the SUNET network (SUNet-CERT, n.d.).

4.8.1.3. LE

The Swedish Police Authority (Polismyndigheten) (Polisen, n.d.) falls under the Ministry of Justice. The LEAs listed below undertake cybercrime investigation tasks, among other types of criminal investigations, and are overseen by the Swedish Police Authority:

- the Swedish Cybercrime Centre (SC3);
- the National Fraud Centre;
- the National Forensic Centre (Nationellt forensiskt centrum – NFC);
- the National Operations Department (Nationella operativa avdelningen – NOA).

The SC3 was established 'to investigate all forms of cybercrime. [SC3] is responsible for detecting, preventing and averting serious cybercrime'. The SC3 shares information on threats, as well as technical methods to combat cybercrime, with partner agencies (Council of the European Union, 2017b); see also (Polisen, n.d. a).

The main tasks of the NFC are to conduct forensic investigations and analyses for the judicial authorities (NFC, n.d.). The National Fraud Centre has a coordinating and supportive role. The centre supports investigators regionally and locally and shares best practices. It collaborates with the NFC and the SC3 (Council of the European Union, 2017b) (Polisen, n.d. a).

The NOA has a leading role in operational activities. The International Affairs Division within the NOA acts as the National Unit of Europol and is the national point of contact for international police cooperation (Polisen, n.d. a).

4.8.1.4. Judiciary

The Swedish Prosecution Authority (Åklagarmyndigheten) and the Swedish Economic Crime Authority (Ekobrottsmyndigheten) are the national authorities that carry out public prosecution tasks (Council of the European Union, 2017b) (Åklagarmyndigheten, n.d.) (Ekobrottsmyndigheten, n.d.).

The Swedish Prosecution Authority comprises the following offices:

- the National Anti-Corruption Unit, which deals with corruption;
- the National Unit for Environment and Working Environment Cases, which deals with the environmental crimes;
- the National Security Unit, which deals with security-related cases;
- the National Unit against Organised Crime, which deals with organised cross-border crime.

Cybercrime and criminal investigations fall under the responsibility of the general prosecution service. In addition, the Swedish Prosecution Authority has developed a network of prosecutors who deal with cybercrime in the different regions of the country (Council of the European Union, 2017b).

The Swedish judicial system has "two parallel types of courts: Ordinary courts, which deal with criminal and civil cases, and general administrative courts, which deal with cases relating to public administration" (European Union, n.d.l.).

"Cybercrime acts are dealt with by the general courts […] in the same manner as other criminal acts" (Council of the European Union, 2017b). The Swedish National Courts Administration (Domstolsverket) (Swedish National Courts Administration, n.d.) is the coordinating organisation for the Swedish courts.

Judicial cooperation in criminal matters with EU Member States is based on the principles of mutual recognition and direct contact between judicial authorities.

Sweden also cooperates with Eurojust and is a member of Eurojust's Cybercrime Network.

4.8.2. Synergies and potential interferences

'The SC3 and the Civil Contingencies Agency are developing cooperation mechanisms at operational as well as at strategic level' (Council of the European Union, 2017b).

Cooperation mechanisms have also been established between LE and the CERT-SE. In addition, collaboration between the private sector and financial institutions and LE has been established, mainly based on information sharing.

As indicated in the interviews with competent experts, there is a frequent exchange of information between the CSIRT and LE communities as part of monthly meetings established to support their cooperation. In addition, there is 'spontaneous communication on a daily basis' under the principle that 'it is better to share than not to share'. The cooperation mechanisms established between the two communities have allowed them to complement each other when performing different tasks. This is particularly the case in interactions with the victims of an incident/cybercrime. 'In some cases the LE provide CSIRTs with information' so that they can notify 'their community and […] the victims. Examples are cases of Distributed Denial-of-Service (DDoS) attacks and ransomware'. The CSIRT community 'has a responsibility to advise the victims of an incident/cybercrime but cannot report the incident on behalf of the victim. CSIRTs do not have a mandate that would allow them to reach out to the victims to obtain information. [On their side, however,] LE are able to contact the victim and ensure their cooperation during an investigation process.' It was also stressed that the CSIRT community relies on the trust relationships established with other CSIRT teams and organisations to ensure a flow of information and smooth collaboration. On the other hand, 'the LE community has a strong legal framework that allows them to enforce their role and access information'.

A CULTURE OF SYNERGY

Established cooperation and spontaneous communication under the principle that 'it is better to share than not to share' .

As emerged from the interviews, 'The national CSIRT [also] provides their technical expertise' in cases where they are 'called as expert witnesses in court proceedings. An example was a fraud case where CSIRT provided technical support in analysing evidence.'

Based on the feedback provided by the interviewees, 'interferences have been noted due to the different tasks that the CSIRT and LE community have. But through mutual efforts [and trust], they have developed an understanding and have managed to benefit from each other's skills.' For instance, CSIRTs have been able to 'support LE in evidence preservation if requested'.

Concerning the interaction between LE and the judiciary, LEAs share with prosecutors information connected to investigations. LEAs 'share information with the judges only for court proceedings. Intervention by a judge during an investigation is rare (mainly limited to cases where decision needs to be made about restricting fundamental freedoms).'

4.8.3. Examples of training

The Swedish National Police Academy (Polishögskolan) provides training for police officers (Polishögskolan, n.d.). The academy organises basic training for police officers in collaboration with higher education institutes such as Växjö University and Umeå University. It also coordinates participation in international courses such as those organised by CEPOL and the Association of European Police Colleges (AEPC) (OSCE, n.d.).

The SC3 also organises training for LE and coordinates the exchange of expertise through its website. It also participates in the 'first responders e-learning' package on IT forensics and IT crime knowledge, in cooperation with ECTEG and supported by Europol, CEPOL, the United Nations Office on Drugs and Crime (UNODC) and the Council of Europe (ECTEG, n.d.) (Polisen, n.d. a). The material is used to support training for LE.

The Training Centre of the Swedish Prosecution Authority provides a specialised course on cybercrime 'in the mandatory initial training and in the further training for prosecutors'. In addition, training in different areas is provided, such as on international legal assistance and on the legal systems of other countries. The Prosecution Authority also shares through its website a platform for prosecutors to exchange information and knowledge (Council of the European Union, 2017b).

The Swedish Judicial Training Academy organises training programmes for the judiciary. Although specialised training on cybercrime is not offered, 'the Academy organises annual criminal law seminars on relevant topics' (Council of the European Union, 2017b) (The Swedish Judicial Training Academy , n.d.).

The SC3 organises training for LE as well as prosecutors.

4.9. FINAL REMARKS

4.9.1. Overview of skills and competences

The technical complexity and the cross-border nature of cybercrime has challenged the competences (including skills, knowledge, attributes and behaviours (IAEA, n.d.) (UN, n.d.) (OECD, 2014) of CSIRTs, LE and the judiciary, driving the three communities to refine their expertise and establish cooperation mechanisms. Interviews with country experts affirmed that interferences can occur during incident handling and cybercrime investigations, but that the communities make efforts to avoid such interferences, create effective partnerships and take advantage of their synergies.

The CSIRT community holds the technical expertise that is required to detect and mitigate cybersecurity incidents and restore cyber-secure environments. The LE and judiciary experts interviewed highlighted that the technical competences of the CSIRT community are also particularly valuable when it comes to assisting with evidence collection, preservation and presentation before a court of law. In addition, several interviewees confirmed that the information flow between CSIRTs and LE has been fundamental in ensuring operational and strategic awareness of cyberthreats.

Although each Member State has its own specific operational and legal framework for shaping the response to cybercrime, it emerged from the interviews that the LE community has an institutional role and carries out the following tasks: determining whether a cybersecurity incident has a criminal nature, conducting the investigation of cybercrime cases and reaching out to the victims of such cases to advise them and ensure their collaboration. To perform these tasks, the LE community applies its knowledge and expertise in digital forensics and criminal investigations. Provided they have a legal mandate, LEAs can aggregate pertinent information on cybercrime cases using their own evidence collection methods, directly from victims , but also through their LE counterparts in other countries and the CSIRT community. In the evidence collection framework, the LE community bears the responsibility for preserving the chain of custody and following the necessary procedures to bring criminals to justice.

The LE investigative activities are closely monitored by the judiciary and, in particular, by public prosecution authorities. Depending on the judicial system of each Member State, a prosecutor or an investigative judge is responsible for leading the cybercrime investigation process and has the authority to issue warrants and instructions to support evidence collection activities. The judiciary community (mainly the judges) assesses the admissibility of the evidence collected, examines the witnesses and pronounces the verdict, determining the criminal and civil liability of cybercrime perpetrators. In addition to their legal competences, given the technical nature of cybercrime, the judiciary needs to understand the technical matters to the extent required to be able to judge whether a suspect has committed a crime and the relevant circumstances to determine the sentence and they may require the support of the CSIRT community, whose delegates may be invited as expert witnesses before the courts.

The interviewees provided examples of training activities involving all three communities, sometimes in the form of joint exercises. These joint training exercises help enhance overall the competences required to respond to cybercrime. With joint training, the three communities can reach a 'better understanding [of] the role and how the other communities work', they become

more aware of the skills and strengths of the other communities and can enhance their competences by learning from each other. For instance, the CSIRT community can learn more about investigative techniques and 'data acquisition, so that the data acquired by […CSIRTs] could more easily serve as evidence in criminal and other types of proceedings', and can acquire legal knowledge, for example 'how to identify if an incident is a crime, and what role LE has on that'. The LE community can obtain a better insight into the different ways that the CSIRT community shares information, as well as the tools used, and further knowledge on analysing data logs and performing incident analysis in specific areas. The judiciary community can benefit by gaining more awareness of cyberthreats and developing, in general, a better understanding of the technical aspects of cybercrime.

Finally, because of the cross-border nature of cybercrime, all three communities need to know about the different EU and international legal frameworks (notably the Convention on Cybercrime (Council of Europe, 2003) and cooperation mechanisms and networks (e.g. CSIRTs Network (CNW) (ENISA, n.d.a), European Union Cybercrime Task Force (EUCTF) (Europol, n.d.a), Joint Cybercrime Action Taskforce (J-CAT) (Europol, n.d.c) ([25]), and European Judicial Cybercrime Network (EJCN) (Eurojust, n.d.b), 24/7 Points of Contact Network under the Council of Europe Convention on Cybercrime ([26])). In addition, the communities need to develop their competences and build organisational and intercultural skills to liaise effectively with counterparts from other Member State and EFTA countries.

4.9.2. Impact of the COVID-19 pandemic on cooperation

It is indisputable that 'The outbreak of Covid-19 has brought an immense change in the way we conduct our lives. In this increasingly connected world, we can, fortunately, continue our professional and private lives virtually' (ENISA, n.d.b). Fortunately, cooperation among the CSIRT, LE, and judiciary communities has also continued during the pandemic crisis, and this is more crucial than ever because 'The COVID-19 pandemic renders individuals and society extremely vulnerable in all respects' (Council of Europe, 2020a) and 'Criminals have quickly adapted their techniques to exploit [the situation and] our fears around the COVID-19 pandemic' (Europol, 2020).

It emerged in quite an unequivocal manner from the data collected in the interviews that, in all eight countries analysed in this study, overall, the COVID-19 pandemic has not hindered cooperation between the CSIRT, LE and judiciary communities; instead, it has generally become even closer and more frequent.

Some interviewees highlighted that meetings in person occurred less frequently (in particular those 'that concerned very sensitive matters that cannot be handled on the phone or via e-mails)', some meetings were postponed and some 'joint training plans [were] disrupted'; however, more meetings took place using video/teleconferencing, several events were moved online and electronic communication, as well as the automatic exchange of information, overall seemed to have increased: 'There is more information sharing. The big change is that we moved physical meetings to virtual ones.' One of the interviewees stated that 'Operations [were] still ongoing despite the pandemic, to avoid interrupting investigations in most of the cases', although the fact that some meetings and court hearings were suspended represented a challenge.

In addition, the interviewees noted that the COVID-19 crisis 'did not change the communication but rather made it more present and more frequent – almost a daily interaction and exchange of information was established. During this period [indeed], joint work and joint approaches were

([25]) Information on J-CAT is available through https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

([26]) A recent study of the Council of Europe Cybercrime Convention Committee (T-CY) highlighted the benefits and successful examples of international cooperation that stem from the Council of Europe Convention on Cybercrime (Council of Europe, 2020b).

established covering a broader scope of activities, including joint statements. In other words, COVID made the cooperation between CSIRTs and LE take place not only on criminal investigations and incidents but also on raising awareness.' According to the interviewees, 'The crisis [actually] helped the institutions to enhance their distance working capacities, e.g. to organise meetings through secure videoconference platforms', and during the pandemic crisis 'there was more close cooperation on updates that needed to be provided to the Government'. One of the interviewees defined the pandemic period as 'a productive work period in terms of communication since the exchanges were multiplied between the entities, especially CSIRTs and LE. Cooperation with other communities was facilitated at the end. They had to adapt to the electronic means and work more hours but they adapted well in the new situation.'

5. CONCLUSIONS AND WAYS FORWARD

5.1. CONCLUSIONS

This report presents a methodology (based on desk research, interviews and compilation of a SoD matrix) to collect data on CSIRTs and LE cooperation, in particular their roles, synergies and interferences, competences and training initiatives related to cooperation between CSIRTs, LE and their interactions with the judiciary. This methodology has been used to collect data on some Member State/EFTA countries, namely Czechia, France, Germany, Luxembourg, Norway, Portugal, Romania and Sweden. The results of this data collection and related analysis are presented in the report.

Using the analysis of the data collected, the conclusions summarised below were drawn. Some of these conclusions found clear confirmation in the discussions at the 9th ENISA/EC3 Workshop on CSIRT and LE cooperation that took place on 16 September 2020; this was an online event, by invitation only (ENISA, 2020).

- All countries analysed have signed the 2001 **Council of Europe Convention on Cybercrime** and almost all of them have ratified it and the Additional Protocol on the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Each country, however, has specific legislation on cybercrime, which is mandated through many different national laws and different criminal procedural law that governs investigations and the prosecution of (cyber)crime.
- All countries analysed have a **NCSS**, which sets up the general framework for the coordination and cooperation of all authorities and defines their roles and responsibilities.
- In terms of incident response, in line with the NIS Directive, all countries analysed have established **national CSIRTs**. However, although there are similarities, **the way they are organised** and the position they have in the national institutional framework **vary** from country to country.
- The way that **LEAs dealing with cybercrime are** organised also **varies** from country to country: some countries have specialised central cybercrime units, whereas others have decentralised specialised units or both.
- The **structure and organisation of the judiciary** also **vary by country**: in some countries there are 'specialised prosecutors or specialised structures within the Prosecution Services dealing with cybercrime offences', while in other countries 'the responsibility for dealing with such crimes usually lies "de facto" with specialised public prosecutors and judges, who have been trained or have experience in the area of cybercrime' (Council of the European Union, 2017c).
- Among the three communities – CSIRTs, LE and judiciary – different approaches and **different levels of cooperation** exist. While operational cooperation, especially in daily interactions and informal communication, seems to be well established, sometimes it appears that more structured cooperation would be useful in order to achieve a less fragmented information flow between the three communities. In addition, there is a bigger gap in the interaction between CSIRTs and the judiciary than in the cooperation established between LE and the judiciary.
- LEAs are not solely involved in the detection and investigation of cybercrimes. A key component of their role is the **preventive aspects of cybercrime,** and it is here that

COVID-19

The pandemic crisis has changed the way that CSIRTs**,** LE and the judiciary work and interact together. In some instances, it has actually meant increased interactions among the communities.

cooperation with other communities, particularly the CSIRT community, becomes apparent, to support preventive strategies.

- CSIRTs and LEAs **need to cooperate to decrease the risk of evidence being compromised or destroyed**.
- CSIRTs and LE also cooperate during the **analysis of evidence**.
- **CSIRTs** play an important role in **informing (potential) victims** of cybercrime and in providing them with information on how to report a crime to the police.
- **CSIRTs** may be called **as witnesses in court**, although this rarely happens.
- Several competences are required for incident handling and cybercrime investigation; while each community has developed its own set of skills and knowledge, **each could benefit from the competences of the other communities**.
- Some initiatives are in place to facilitate **training** within each community and some joint training takes place involving two of the communities (e.g. CSIRTs and LE, or LE and the judiciary); however, there is a need for further initiatives and for training and exercises that involve the three communities together.
- The **COVID-19 pandemic has changed the way CSIRTs, LE and the judiciary work together and interact**. The greatest impact has been on training and workshop events, as well as meetings, which were cancelled in the early stages of the pandemic and later delivered online. As the COVID-19 pandemic has continued, the use of online tools to facilitate meetings and events has become the norm. Overall, there does not appear to have been a significant impact of the pandemic on the ability of the three communities to cooperate. In some instances, **the level of vigilance and interaction among the communities has actually increased**, with even daily interaction taking place, to ensure that each community is kept up to date.

5.2. WAYS FORWARD

5.2.1. Use the methodology proposed to extend the analysis to additional countries

Additional EU and EFTA countries could be analysed using the methodology outlined in this report.

The methodology could be easily tailored and used to analyse cooperation between CSIRTs, LE and judiciary in countries other than EU Member State and EFTA countries, beginning with candidate countries, potential candidate countries and neighbouring countries of the EU ([27]).

5.2.2. Use the results to develop additional training material

In its continuous effort to provide training material for the CSIRT community, including on cooperation with the LE community and other operational communities (ENISA, n.d.), ENISA has developed a handbook and a toolset (ENISA, 2021) based on the results outlined in this current report. Additional training material could be developed based on the results of an analysis extended to additional EU Member States and EFTA countries, and possibly candidate countries, potential candidate countries and neighbouring countries of the EU.

5.2.3. Use the results to develop a catalogue of competences across authorities in EU Member States and EFTA countries

A catalogue of the competences required during incident handling and cybercrime investigations, with an indication of the authorities in each Member State and EFTA country that could offer such competences, would help CSIRTs, LE and the judiciary become more aware of

([27]) For more information on neighbouring countries of the EU, see https://ec.europa.eu/info/business-economy-euro/economic-and-fiscal-policy-coordination/international-economic-relations/enlargement-and-neighbouring-countries/neighbouring-countries-eu_en

the skills and strengths of other communities in their country, and also across the EU and EFTA area. This would allow authorities to learn from each other's initiatives and also facilitate the provision of expertise where required for incident handling and/or criminal investigation. Such a catalogue of competences could be developed using information collected using this methodology (slightly adapting the questionnaire and the SoD matrix, if necessary, to further focus on competences).

5.2.4. Use the results to develop decision support systems

The results of an extended analysis could help complete the picture and serve as a basis for the development of decision support systems that a CSIRT, LE or judiciary authority could easily consult to obtain information on which authorities are responsible for, supporting, consulted about and informed about a specific duty related to fighting cybercrime in one or more countries (see Annex D for an example of how the SoD matrix can be used to develop a decision support system). These support systems can aid in decision-making and in taking actions in cases where the evidence is located in several countries.

5.2.5. Organise joint training and exercises for the three communities

Although there might be organisational and legal constraints against the participation of the judiciary in joint training and exercises, wherever possible initiatives involving all three communities should take place. This would help the communities better understand each other's capabilities, needs and boundaries, to enable them to better respond in practice to cyber incidents of a criminal nature by exploiting synergies and avoiding interferences.

6. REFERENCES

Åklagarmyndigheten. (n.d.). Retrieved from https://www.aklagare.se/en/

ANACOM. (n.d.). Retrieved June 22, 2020, from www.anacom.pt

ANACOM. (n.d a). Retrieved from https://www.anacom.pt/render.jsp?contentId=1133069

ANSSI. (2018). Retrieved May 20, 2020, from https://www.certa.ssi.gouv.fr/uploads/CERT-FR_RFC2350_EN.pdf

ANSSI. (n.d. a). *A word from the Director-General*. Retrieved July 31, 2020, from https://www.ssi.gouv.fr/en/mission/word-from-director-general/

ANSSI. (n.d.). *The French National Digital Security Strategy*. Retrieved from https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/

BKA-CC. (n.d.). Retrieved June 1, 2020, from https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/cybercrime_node.html

BMI. (2011). *Cyber Security Strategy for Germany.* Retrieved July 31, 2020, from http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

BMI. (n.d.). *The Federal Criminal Police Office*. Retrieved June 22, 2020, from https://www.bmi.bund.de/EN/topics/security/federal-criminal-police-office/federal-criminal-police-office-node.html

Brandenburg Judicial Academy. (n.d.). Retrieved June 1, 2020, from http://www.justizakademie.brandenburg.de/sixcms/detail.php?id=145097

Brownlee & Guttman. (1998). *Expectations for Computer Security Incident Response.* Retrieved June 5, 2020, from https://tools.ietf.org/html/rfc2350

Bryman, A., & Bell, E. (2011). *Business Research Methods.* Oxford University Press.

BSI. (n.d.). Retrieved from Federal Office for Information Security : https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html;jsessionid=7C2FB137051BB166BE4B1C6CF57CE31D.1_cid501

BSI. (2017). *Act on the Federal Office for Information Security.* Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=4

BSI. (n.d. a). Retrieved June 17, 2020, from RFC-2350: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/rfc2350_CERT-Bund_txt.asc?__blob=publicationFile&v=2

Bundeskriminalamt - BKA. (n.d.). *Internet Crime / Cybercrime*. Retrieved June 22, 2020, from https://www.bka.de/EN/OurTasks/AreasOfCrime/Cybercrime/cybercrime_node.html

Bundesminister des Innern, für Bau und Heimat (BMI). (n.d.). *The Federal Criminal Police Office*. Retrieved June 22, 2020, from https://www.bmi.bund.de/EN/topics/security/federal-criminal-police-office/federal-criminal-police-office-node.html

Bundespolizei. (n.d.). Retrieved June 17, 2020, from https://www.bundespolizei.de/Web/DE/_Home/home_node.html

Bundespolizei. (2017). *Annual Report 2017.* Retrieved July 31, 2020, from https://www.bundespolizei.de/Web/DE/Service/Mediathek/Jahresberichte/jahresbericht_2017_EN_file.pdf?__blob=publicationFile&v=3

CCIS. (n.d.). Retrieved from https://www.ntnu.edu/ccis

CECyF. (n.d.). Retrieved May 20, 2020, from https://www.cecyf.fr

CEIS. (n.d.). Retrieved June 18, 2020, from [Cyber] CEIS, coordinator of the ENFORCE project, co-organizes a cybercrime training with the Luxembourgian CIRCL and the French National Police

CEJ. (n.d.). Retrieved June 22, 2020, from http://www.cej.mj.pt/cej/eng/about_cej_mission.php

CEPOL. (n.d.). *Education and Training*. Retrieved from https://www.cepol.europa.eu/education-training

CERT RO. (2020, July 28). *LEGE Nr. 362/2018 din 28 decembrie 2018.* Retrieved from https://cert.ro/vezi/document/legea-nr-362-din-28-decembrie-2018

CERT.LU. (n.d.). *About cert.lu*. Retrieved June 22, 2020, from https://cert.lu

CERT-Bund. (n.d.). Retrieved June 1, 2020, from https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund_node.html

CERT-MIL. (n.d.). Retrieved June 25, 2020, from https://certmil.ro

CERT-RO. (n.d.). Retrieved June 25, 2020, from https://cert.ro/

CERT-RO. (n.d. a). *RFC 2350 description for CERT-RO*. Retrieved from https://cert.ro/vezi/document/RFC2350-CERT-RO

CERT-RO. (n.d.b). *Cyber security strategy of Romania*. Retrieved from https://cert.ro/vezi/document/NCSS-Ro

CERT-SE. (2015). Retrieved from RFC2350: https://www.cert.se/rapporter/RFC_2350_CERT-SE.pdf

CIRCL. (2020, 08 16). *CIRCL*. Retrieved from CIRCL: https://circl.lu

CIRCL.LU. (n.d.). *Homepage*. Retrieved June 22, 2020, from https://www.circl.lu/

CIRCL.LU. (n.d. a). *GitHub - Neolea training materials overview*. Retrieved July 31, 2020, from https://github.com/neolea/neolea-training-materials

CIRCL.LU. (n.d. b). *RFC 2350 CIRCL - the CERT for the private sector, communes and non-governmental entities in Luxembourg*. Retrieved June 22, 2020, from https://www.circl.lu/mission/rfc2350/

CNCS. (n.d.). *Homepage*. Retrieved July 2, 2020, from https://www.cncs.gov.pt/en/

CNCS. (n.a.a). *CERT.PT*. Retrieved from https://www.cncs.gov.pt/en/certpt_en/

CNCS. (n.d.b). *Centro Nacional de Cibersegurança*. Retrieved from https://www.cncs.gov.pt/en/about-us/

CNCS. (n.d.c.). *Centro Nacional de Cibersegurança - CSIRT Capability Building.* Retrieved September 04, 2020, from https://www.cncs.gov.pt/en/certpt_en/csirt-capability-building/

CORIS-STS. (n.d.). Retrieved June 25, 2020, from https://www.sts.ro/en/coris-sts

Council of Europe. (1998). *European Charter on the statute for judges.* Retrieved June 22, 2020, from https://rm.coe.int/16807473ef

Council of Europe. (2003, November 23). *Convention on Cybercrime*. Retrieved June 16, 2020, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council of Europe. (2020, August 21). *Romania National Police.* Retrieved from Running a specialised Cybercrime Unit in Romania: https://rm.coe.int/ro-police-cybercrime-unit-marius-cuciurianu-29-april-2020-final/16809e41ee

Council of Europe. (2020a, March 27). *Cybercrime and COVID-19*. Retrieved from News: https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19

Council of Europe. (2020b, July 13). *The Budapest Convention on Cybercrime: benefits and impact on practice.* Retrieved from The Budapest Convention on Cybercrime:

Council of Europe. (n.d.a). *Cybercrime Programme Office (C-PROC)*. Retrieved July 2, 2020, from https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-

Council of Europe. (n.d.b). Retrieved September 3, 2020, from Country Wiki - Czech Republic: https://www.coe.int/en/web/octopus/-/czech-republic?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_AZnxfNT8Y3Zl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2

Council of the European Union. (2015). *Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of European policies on preventing and combating cybercrime' - Report on France.* Retrieved May 20, 2020,

from https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/DOC%20567%20study2-d-version8%20provisional%20(12%20march%2008).PDF

Council of the European Union. (2015, November 26). *Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of European policies on preventing and combating cybercrime'-Report on France.* Retrieved July 2020, from https://data.consilium.europa.eu/doc/document/ST-7588-2015-REV-2-DCL-1/en/pdf

Council of the European Union. (2017). *Evaluation report on the 7th round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - - Report on the Czech Republic.* Retrieved February 8, 2017, from http://data.consilium.europa.eu/doc/document/ST-13203-2016-REV-1-DCL-1/en/pdf

Council of the European Union. (2017a). *Evaluation Report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Germany.* Retrieved June 1, 2020, from http://data.consilium.europa.eu/doc/document/ST-7159-2017-REV-1-DCL-1/en/pdf

Council of the European Union. (2017b). *Evaluation Report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"-Report on Sweden.* Retrieved from http://data.consilium.europa.eu/doc/document/ST-8188-2017-REV-1-DCL-1/en/pdf

Council of the European Union. (2017c, September 18). *Seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime"-Draft Final report.* Retrieved September 04, 2020, from https://data.consilium.europa.eu/doc/document/ST-9986-2017-REV-2/en/pdf

CSIRT-PJ. (n.d.). Retrieved May 20, 2020, from Prefecture de Police: https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/L-organisation-et-les-structures

Cybermalveillance.gouv.fr. (2019). Retrieved from https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/qui-sommes-nous

DCIAP. (n.d.). Retrieved June 22, 2020, from http://en.ministeriopublico.pt/en/pagina/central-department-criminal-investigation-and-prosecution

Domstol. (n.d.). Retrieved from https://www.domstol.no/en/the-courts-of-justice/The-ordinary-courts-of-Norway/The-Supreme-Court/

ECTEG. (n.d.). Retrieved from https://www.ecteg.eu/running/first-responders/

ECTEG. (n.d. a). Retrieved from https://www.ecteg.eu/members/

EFTA. (n.d.). *EEA Agreement*. Retrieved from https://www.efta.int/eea/eea-agreement/eea-basic-features

EFTA. (n.d.a). Retrieved from https://www.efta.int/about-efta/the-efta-states

EJN. (n.d.). Retrieved June 25, 2020, from https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/354

EJN. (n.d.a). Retrieved June 1, 2020 , from https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/277

EJTN. (n.d.). *European Judicial Training Network - Luxembourg.* Retrieved September 04, 2020, from http://www.ejtn.eu/About/EJTN-Affiliates/Members/Luxembourg/

EJTN. (n.d.a). Retrieved from http://www.ejtn.eu/

Ekobrottsmyndigheten. (n.d.). Retrieved from https://www.ekobrottsmyndigheten.se/en/

EMPFGA. (n.d.). *Homepage*. Retrieved July 2, 2020, from www.emgfa.pt

ENISA. (2017). *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement.* Retrieved from https://www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement

ENISA. (2017a). *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects.* Retrieved from https://www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement

ENISA. (2018, November). *Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary* . Retrieved June 05, 2020, from https://www.enisa.europa.eu/publications/csirts-le-cooperation

ENISA. (2019, November). *ENISA Programming Document 2020-2022.* Retrieved May 1, 2020, from https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022

ENISA. (2019a, December). *An Overview on Enhancing Technical Cooperation between CSIRTs and LE.* Retrieved May 17, 2020, from https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le

ENISA. (2019b, December). *Roadmap on the cooperation between CSIRTs and LE.* Retrieved June 16, 2020, from https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation

ENISA. (2019c). *EU MS Incident Response Development Status Report.* Retrieved June 22, 2020, from https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report

ENISA. (2020, September 25). *Ninth ENISA-EC3 Workshop on CSIRTs-LE Cooperation: standing shoulder-to-shoulder to counter cybercrime.* Retrieved September 2020, 2020, from https://www.enisa.europa.eu/news/enisa-news/ninth-enisa-ec3-workshop-on-csirt-le-cooperation-standing-shoulder-to-shoulder-to-counter-cybercrime

ENISA. (2021). *Aspects of Cooperation between CSIRTs and LE - Handbook, Document for trainers) and Aspects of Cooperation between CSIRTs and LE - Toolset, Document for*

trainees). Retrieved from https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/legal-cooperation

ENISA. (n.d.a). *CSIRTs Network*. Retrieved from https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

ENISA. (n.d.b). *COVID-19*. Retrieved from https://www.enisa.europa.eu/topics/wfh-covid19

ENISA. (n.d.c). *Training material to enhance cooperation across CSIRTs and Law Enforcement*. Retrieved June 05, 2020, from https://www.enisa.europa.eu/news/enisa-news/training-material-to-enhance-cooperation-across-csirts-and-law-enforcement

ENISA. (n.d.d). *History [of CSIRT Capabilities and Maturity]*. Retrieved June 22, 2020, from https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/baseline-capabilities

ENISA. (n.d.e). *NCSS Czech Republic*. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-of-czech-republic-2011-2015

ENISA. (n.d.f). *NCSS Germany*. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/view

ENISA. (n.d.g). *NCSS Luxembourg*. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite

ENISA. (n.d.h). *NCSS France*. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/information-systems-defence-and-security-frances-strategy

ENISA. (n.d.i). *NCSS Norway*. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategy-for-information-security

ENISA. (n.d.j). *NCSS Portugal*. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/portuguese-ncss

ENISA. (n.d.k). *NCSS Romania*. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

ENISA. (n.d.l). *NCSS Sweden*. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy

ENISA. (n.d.m). *CEI – List of NIS Experts*. Retrieved May 17, 2020, from https://www.enisa.europa.eu/procurement/cei-list-of-nis-experts

ENISA. (n.d.n). *8th ENISA/EC3 Workshop*. Retrieved June 5, 2020, from https://www.enisa.europa.eu/events/8th-enisa-ec3-workshop

ENISA. (n.d.). *Trainings for Cybersecurity Specialists*. Retrieved June 17, 2020, from https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/training-courses

ERA. (n.d.). Retrieved from https://www.era.int

Eurojust. (n.d.b). *European Judicial Cybercrime Network*. Retrieved from http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx

European Commission. (n.d.). *The Romanian Centre of Excellence for Cybercrime*. Retrieved June 25, 2020, from https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2011_ISEC_AG_INT_4000002223_en

European e-Justice Portal . (n.d.). *Romania*. Retrieved from https://rm.coe.int/organisation-of-the-public-ministry-in-romania/168077636a

European Parliament and Council. (2016, July 6). *DIRECTIVE (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive").* Retrieved July 31, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2016%3A194%3ATOC&uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

European Parliament and Council of the European Union. (2016a). *REGULATION (EU) 2016/679 (GDPR).* Retrieved June 22, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

European Union. (n.d.a). *Czechia*. Retrieved June 16, 2020, from https://europa.eu/european-union/about-eu/countries/member-countries/czechia_en

European Union. (n.d.b). *European Justice*. Retrieved from https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-de-en.do?member=1

European Union. (n.d.c.). *Germany*. Retrieved from https://europa.eu/european-union/about-eu/countries/member-countries/germany_en

European Union. (n.d.d.). *Luxembourg*. Retrieved from https://europa.eu/european-union/about-eu/countries/member-countries/luxembourg_en

European Union. (n.d.e). *European Justice*. Retrieved from https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-lu-en.do?member=1

European Union. (n.d.f). *France*. Retrieved from https://europa.eu/european-union/about-eu/countries/member-countries/france_en

European Union. (n.d.g). *European Justice*. Retrieved May 20, 2020, from https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-fr-en.do?member=1

European Union. (n.d.h). *Romania*. Retrieved from https://europa.eu/european-union/about-eu/countries/member-countries/romania_en

European Union. (n.d.i.). *Portugal*. Retrieved from https://europa.eu/european-union/about-eu/countries/member-countries/portugal_en

European Union. (n.d.j). *European Justice* . Retrieved from https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-pt-en.do?member=1

European Union. (n.d.k.). *Sweden* . Retrieved from https://europa.eu/european-union/about-eu/countries/member-countries/sweden_en

European Union. (n.d.l.). Retrieved from https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-se-en.do?member=1

Europol . (n.d.). *Training and Capacity Building*. Retrieved from https://www.europol.europa.eu/activities-services/services-support/training-and-capacity-building

Europol. (2020, May 6). *STAYING SAFE DURING COVID-19: WHAT YOU NEED TO KNOW*. Retrieved from https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know

Europol. (n.d.a). *European Union Cybercrime Task Force (EUCTF)*. Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf.

Europol. (n.d.b). *Law Enforcement Agencies*. Retrieved June 22, 2020, from https://www.europol.europa.eu/partners-agreements/member-states/portugal

Europol. (n.d.c). *JOINT CYBERCRIME ACTION TASKFORCE (J-CAT)*. Retrieved from https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

Europol. (n.d.d). *EU Policy Cycle - EMPACT*. Retrieved June 19, 2020, from https://www.europol.europa.eu/empact

FCKS. (n.d.). Retrieved from https://nsm.no/om-oss/historien-om-nsm/felles-cyberkoordineringssenter-fcks-etableres

FinansCERT. (n.d.). Retrieved from http://www.finanscert.no/engelsk.html

FIRST. (n.d.). *Education, Training Courses*. Retrieved from https://www.first.org/education/trainings

FM-CERT. (n.d.). Retrieved from https://www.forsvarsmakten.se/sv/

GÉANT. (n.d.). *TRANSITS training*. Retrieved from https://www.geant.org/Services/Trust_identity_and_security/Pages/TRANSITS_Training.aspx

German Judicial Academy. (n.d.). *German Judicial Academy*. Retrieved June 1 , 2020, from http://www.deutsche-richterakademie.de/icc/draen/nav/123/broker?editmode=false

GIRP-FID. (n.d.). Retrieved June 25, 2020, from http://www.citycop.eu/the-consortium/partners/general-inspectorate-of-romanian-police.kl

GitHub. (n.d.). *MISP / misp-galaxy*. Retrieved June 22, 2020, from https://github.com/MISP/misp-galaxy

GOVCERT.LU. (n.d.). *Homepage*. Retrieved June 22, 2020, from https://www.govcert.lu/en/

GOVCERT.LU. (n.d.a). *RFC2350*. Retrieved June 22, 2020, from https://www.govcert.lu/docs/POL202_RFC2350_(Public)_6.0.pdf

GOVCERT.LU. (n.d.b). *NCERT.LU*. Retrieved November 11, 2020, from https://www.govcert.lu/en/ncert/

Government of the Czech Republic. (2020, July 27). *Legislation.* Retrieved from National Cyber Security Center: https://www.govcert.cz/download/legislativa/container-nodeid-708/nbu-zkb-navrh-130415-duvodzprava.pdf

HCPN. (n.d.). Retrieved from https://hcpn.gouvernement.lu/en/service.html

HelseCERT. (n.d.). Retrieved from www.nhn.no/helsecert

Higher Prosecuting Authority. (n.d.). Retrieved from https://www.riksadvokaten.no/english/

IAEA. (n.d.). *The Competency Framework*. Retrieved June 05, 2020, from https://www.iaea.org/sites/default/files/18/03/competency-framework.pdf

ISACA. (n.d.). *Glossary*. Retrieved from https://www.isaca.org/resources/glossary#glossc

ISACA. (n.d. a). *COBIT*. Retrieved June 16, 2020a, from https://www.isaca.org/resources/cobit

ISCPSI. (n.d.). Retrieved June 22, 2020, from http://www.iscpsi.pt/Inicio/Paginas/default.aspx

ISO. (n.d.). *ISO/IEC 27001*. Retrieved June 22, 2020, from https://www.iso.org/isoiec-27001-information-security.html

ITU. (n.d.). *Cyberwellness Profile Romania*. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Romania.pdf

JSON.ORG. (n.d.). *Introducing JSON*. Retrieved July 31, 2020, from https://www.json.org/json-en.html

KYPO. (n.d.). Retrieved June 16, 2020, from https://www.kypo.cz/en

Landgericht Köln. (n.d.). *Geschäftsverteilung des Landgerichts Köln für das Geschäftsjahr 2020.* Retrieved July 31, 2020, from https://www.lg-koeln.nrw.de/aufgaben/geschaeftsverteilung/zt_geschaeftsverteilung/Geschaeftsverteilungsplaene/gvp-2020.pdf

Masaryk University . (n.d.). Retrieved June 19, 2020, from https://www.muni.cz/en/

Ministère de la Justice. (2012). *The French legal system.* Retrieved July 2020, from http://www.justice.gouv.fr/art_pix/french_legal_system.pdf

Ministère de l'Interieur. (2019, July). *DGSI*. Retrieved from https://www.interieur.gouv.fr/Le-ministere/DGSI/Missions/La-mission-judiciaire-specialisee

MSB. (n.d.). Retrieved from https://www.msb.se/en/

National Cybersecurity Competence Centre . (n.d.). *National Cybersecurity Competence Centre* , June. Retrieved 2020, from https://nc3.cz/en

NBÚ. (2015). *National Cyber Security Strategy of the Czech Republic for The Period from 2015 to 2020*. Retrieved June 22, 2020, from https://www.govcert.cz/download/gov-cert/container-nodeid-1067/ncss-15-20-150216-en.pdf

NCBK. (2015, February 16). *National Cyber Security Center*. Retrieved from https://www.govcert.cz/en/info/events/2462-the-government-of-the-czech-republic-adopted-the-national-cyber-security-strategy-for-the-upcoming-five-years/

NCKB. (2014). *The Law No. 181/2014 Coll. on Cyber Security entered into force* . Retrieved from https://www.govcert.cz/en/info/events/2464-the-law-no-1812014-coll-on-cyber-security-entered-into-force/

NCKB. (n.d.). *Action Plan for the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.* https://www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015-2020-en.pdf.

NCSC. (n.d.). Retrieved from https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

NIM. (n.d.). Retrieved from http://www.inm-lex.ro/

Norwegian Ministeries. (n.d.). *National Cybersecurity Strategy for Norway*. Retrieved from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf

NPUC. (n.d.). Retrieved from https://www.politihogskolen.no

NSM. (n.d.). Retrieved from National Security Authority: https://nsm.no/about-nsm/about-the-norwegian-national-security-authority/

NÚKIB. (n.d. a). *About the Agency*. Retrieved June 17, 2020, from https://nukib.cz/en/about-nukib/about-the-agency/

NÚKIB. (n.d.). *National Cyber and Information Security Authority (NÚKIB)*. Retrieved June 17, 2020, from https://nukib.cz/en/

OECD. (2014, November 11). *Competency Framework*. Retrieved June 5, 2020, from https://www.oecd.org/careers/competency_framework_en.pdf

Økokrim. (n.d.). Retrieved from https://www.okokrim.no

OSCE. (n.d.). *Country Profile - Sweden.* Retrieved from https://polis.osce.org/country-profiles/sweden

OSCE. (n.d.a). *Country Profile - Luxembourg.* Retrieved from https://polis.osce.org/country-profiles/luxembourg

OSCE. (n.d.b.). *Country Profile Norway* . Retrieved from https://polis.osce.org/country-profiles/norway

PGO. (n.d.). Retrieved June 22, 2020, from http://en.ministeriopublico.pt/node/4084

POHCCJ. (n.d.). Retrieved June 25, 2020, from https://www.mpublic.ro/en

Police Grand-Ducale. (n.d.). *Police Grand-Ducale*. Retrieved June 22, 2020, from https://police.public.lu/fr/support/recherche.html?q=cybercrime

Polícia Judiciária . (n.d.). Retrieved June 22, 2020, from https://www.policiajudiciaria.pt/unc3t/

Polisen. (n.d.). Retrieved from https://polisen.se/en/

Polisen. (n.d. a). Retrieved from https://polisen.se/om-polisen/organisation/

Polishögskolan. (n.d.). Retrieved from https://polisen.se/om-polisen/bli-polis/polisutbildningen/

Politia Romana. (n.d.). Retrieved June 25, 2020, from https://www.politiaromana.ro/en/romanian-police

Politia Romana. (n.d.a). Retrieved June 25, 2020, from https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-combatere-a-criminalitatii-organizate/directia-de-combatere-a-criminalitatii-organizate/directia-de-combatere-a-criminalitatii-organizate

Politiet. (n.d.). Retrieved from https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/

Politiet. (n.d. a). Retrieved from https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/national-cybercrime-centre/

Politiet. (n.d.b). Retrieved from https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/national-cybercrime-centre/

Politiet. (n.d.c). Retrieved from (https://www.politiet.no/en/om/organisasjonen/andre/national-police-directorate/om-pod/role-of-the-national-police-directorate/)

Portal Legislativ. (n.d.). Retrieved June 25, 2020, from http://legislatie.just.ro/Public/DetaliiDocument/224588

PPS. (n.d.). Retrieved June 22, 2020, from http://en.ministeriopublico.pt

Prime Minister of France. (2015). *French national digital security strategy.* Retrieved July 31, 2020, from https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

PSP. (n.d.). Retrieved September 04, 2020, from https://www.psp.pt/Pages/sobre-nos/quem-somos/o-que-e-a-psp.aspx

Romanian Ministry of Justice. (n.d.). Retrieved June 25, 2020, from http://www.just.ro/en/despre/ghiduri-si-manuale/#

SIS. (n.d.). Retrieved June 22, 2020, from https://www.sis.pt/en

SRI. (n.d.). *National Cyberint Centre - Cyberintelligence.* Retrieved September 04, 2020, from https://sri.ro/cyberintelligence

SUNet-CERT. (n.d.). Retrieved from https://www.cert.sunet.se/english/index.html

Swedish Government. (n.d.). *Comprehensive Cyber Security Action Plan*. Retrieved from https://www.government.se/legal-documents/2017/11/skr.-201617213/ https://rib.msb.se/filer/pdf/28898.pdf

Swedish National Courts Administration. (n.d.). Retrieved from http://old.domstol.se/Funktioner/English/The-Swedish-courts/

The Judicial Academy. (n.d.). Retrieved May 20 , 2020, from http://www.ejtn.eu/About-us/Members/Czech-Republic/

The Luxembourg Government. (2018, 01 10). *Update of 'Cyber ERP' - the Emergency Response Plan to deal with attacks against information systems or the technical failure of information systems*. Retrieved from High Commission for National Protection: https://hcpn.gouvernement.lu/en/actualites/articles0/2018/2018.html

The Police Academy of the Czech Republic. (n.d.). Retrieved May 20, 2020, from https://www.polac.cz/g2/view.php?anglicky/index.html.

The Swedish Judicial Training Academy . (n.d.). Retrieved from http://www.domstol.se/

Tomczack, P. (2014, September 16). *Improving the RFP and Contracts Process With COBIT 5*. Retrieved July 31, 2020, from https://www.isaca.org/resources/news-and-trends/newsletters/cobit-focus/2014/improving-the-rfp-and-contracts-process-with-cobit-5

UiO-CERT. (n.d.). Retrieved from www.uio.no/english/services/it/security/cert/

UN. (n.d.). *Competencies for the Future*. Retrieved June 5, 2020, from https://careers.un.org/lbw/attachments/competencies_booklet_en.pdf

UNINETT . (n.d a). *Uninett CERT RFC 2350 profile.* Retrieved July 2020, 2020, from https://www.uninett.no/cert/rfc2350

UNINETT. (n.d.). Retrieved from www.uninett.no/en

UNODC. (2014). *The Status and Role of Prosecutors.* Retrieved June 22, 2020, from https://www.unodc.org/documents/justice-and-prison-reform/HB_role_and_status_prosecutors_14-05222_Ebook.pdf

US Congress. (1999). *Gramm-Leach-Bliley Act .* Retrieved June 22, 2020, from https://www.govinfo.gov/content/pkg/STATUTE-113/pdf/STATUTE-113-Pg1338.pdf

US Congress. (2002). *H.R.3763 - Sarbanes-Oxley Act of 2002.* Retrieved June 22, 2020, from https://www.congress.gov/bill/107th-congress/house-bill/3763

A ANNEX: BRIEF SUMMARY OF DESK RESEARCH CONDUCTED

The sources consulted for the desk research are presented here according to the following categories:

- legal framework-related material;
- policy reports;
- ENISA reports in the area of CSIRT–LE cooperation;
- training-related material;
- country-specific material;
- academic papers.

This list of sources might not be exhaustive.

A.1. Legal framework-related material

- Council of Europe (2001), 'Convention on Cybercrime', ETS No 185', Budapest, 23 November (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, accessed 8 May 2020).
- Council of Europe (n.d.), Protocol negotiations, The Drafting Group assists the T-CY Plenary in the preparation of a draft Second Additional Protocol to the Convention on Cybercrime (ETS 185) (https://www.coe.int/en/web/cybercrime/t-cy-drafting-group, accessed 8 May 2020).
- Council of the European Union (2018), 'Press release. Regulation on cross-border access to e-evidence: Council agrees its position', 7 December 2018 (https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-crossborder-access-to-e-evidence-council-agrees-its-position, accessed 2 May 2020).
- Council of the European Union (2019), 'Press release. E-evidence package: Council agrees its position on rules to appoint legal representatives for the gathering of evidence', 8 March (https://www.consilium.europa.eu/en/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/, accessed 1 May 2020).
- Council of the European Union (2019), Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings – General approach, 28 February (https://data.consilium.europa.eu/doc/document/ST-6946–2019-INIT/en/pdf, accessed 2 May 2020).
- European Commission (2018), *Impact assessment – e-Evidence – the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD(2018) 118 final (https://eurlex.europa.eu/legal-content/EN/TXT/?uri=SWD %3A2018 %3A118 %3AFIN, accessed 1 May 2020).
- European Commission (2018), Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal

representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN, accessed 2 May 2020).

- European Commission (2018), Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN, accessed 2 May 2020).
- European Parliament (2018), *Criminal Procedural Laws across the European Union*, 11 September. (https://op.europa.eu/en/publication-detail/-/publication/70e80c5d-b64e-11e8–99ee-01aa75ed71a1, accessed 8 May 2020).
- European Parliament and Council of the European Union (2013), Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. OJ L 218, 14.8.2013, p. 8–14 (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1586116250710&uri=CELEX:32013L0040, accessed 2 May 2020).
- European Parliament and Council of the European Union (2016), Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, p. 1–30 (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1586115465548&uri=CELEX:32016L1148, accessed 1 May 2020).
- European Parliament and Council of the European Union (2016), Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. OJ L 119, 4.5.2016, p. 89–131 (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1586118812203&uri=CELEX:32016L0680, accessed 2 May 2020).
- European Parliament and Council of the European Union (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88 (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1586118735639&uri=CELEX:32016R0679, accessed 8 May 2020).
- European Parliament and Council of the European Union (2019), Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). OJ L 151, 7.6.2019, p. 15–69 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881, accessed 2 May 2020).
- European Union Agency for Law Enforcement Training (2015), Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA. OJ L 319, 4.12.2015, p. 1–20 (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1541512530912&uri=CELEX:32015R2219, accessed 1 May 2020).

A.2. Policy reports

- Council of Europe (2016), 6 June (https://www.coe.int/en/web/octopus-old2019/blog/-/blogs/genval-evalutation-reports-on-cybercrime/ accessed 7 May 2020). The seventh round of GENVAL mutual evaluations has been dedicated to the practical implementation and operation of European policies on preventing and combating cybercrime.
- Council of Europe (2019), *C-PROC activity report for the period October 2018 – September* 2019 (https://rm.coe.int/c-proc-activity-report-oct-2018-sep-2019/168098dee8, accessed 6 May 2020).
- Council of Europe (n.d.), 'Cybercrime Programme Office (C-PROC)' (https://www.coe.int/en/web/cybercrime/home, accessed 8 May 2020). Action against cybercrime.
- Council of Europe. *Fight against cybercrime* (https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-, accessed 8 May 2020).
- Council of the European Union (2017). *Final report of the seventh round of mutual evaluations on 'The practical implementation and operation of the European policies on prevention and combating cybercrime'*, 2 October (http://data.consilium.europa.eu/doc/document/ST-12711–2017-INIT/en/pdf, accessed 7 May 2020).
- ENISA (n.d.), 'National cyber security strategies – interactive map' (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map, accessed 2 May 2020). Lists all of the documents of the NCSSa in the EU, together with their strategic objectives and good examples of implementation.
- Eurojust (n.d.), European Union Agency for Criminal Justice Cooperation home page (http://www.eurojust.europa.eu/Pages/home.aspx, accessed 8 May 2020). Supports and strengthens coordination and cooperation between national investigating and prosecuting authorities. Provides access to the Eurojust and EU framework, as well as the EJCN.
- European Commission (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 01 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001, accessed 1 May 2020).
- European Commission (2018), *Operational guidance for the EU's international cooperation on cyber capacity building*, 31 August (https://www.iss.europa.eu/content/operational-guidance-eu's-international-cooperation-cyber-capacity-building, accessed 7 May 2020).
- European Commission (2019). Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No 185), COM(2019) 71 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1586116250710&uri=CELEX:52019PC0071, accessed 8 May 2020).
- European Commission (n.d.), 'Cybercrime' (https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en, accessed 8 May 2020). Presents the EU policies and legal actions in this area. It has links to EC3 and ENISA.
- European Commission (n.d.), 'E-evidence' (https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en, accessed 8 May 2020).
- European Commission (n.d.), 'Police cooperation' (https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation_en, accessed 6 May 2020).

- European Commission (n.d.), 'Supporting action: Training, funding, research and innovation' (https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/supporting-action, accessed 6 May 2020).
- Interpol (n.d.), 'Cybercrime threat response' (https://www.interpol.int/Crimes/Cybercrime/Investigative-support-for-cybercrime, accessed 6 May 2020).
- Interpol (n.d.), 'Public–private partnerships' (https://www.interpol.int/Crimes/Cybercrime/Cyber-partnerships, accessed 7 May 2020).

A.3. ENISA reports in the area of CSIRT–LE cooperation

- *A good practice collection for CERTs on the directive on attacks against information systems* (2013) (https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems, accessed 8 May 2020).
- *Baseline capabilities of national/governmental CERTs. Part 2: Policy recommendations* (https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=16&ved=2ahUKEwiog63AoqLpAhXNMZoKHU55AN0QFjAPegQIBhAB&url=https %3A %2F %2Fwww.enisa.europa.eu %2Fpublications %2Fbaseline-capabilities-of-national-governmental-certs-policy-recommendations %2Fat_download %2FfullReport&usg=AOvVaw1dMmG5JNwWorJjP9gwK7dZ, accessed 8 May 2020).
- *Cooperation between CERTs and law enforcement agencies in the fight against cybercrime – A first collection of practices* (2012) (www.enisa.europa.eu/publications/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices, accessed 8 May 2020).
- *Cooperation between CSIRTs and law enforcement: interaction with the judiciary* (2018) (https://www.enisa.europa.eu/publications/csirts-le-cooperation/, accessed 1 May 2020).
- *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity* (2018) (https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/, accessed 8 May 2020).
- *Good practice guide for addressing network and information security aspects of cybercrime* (2012) (www.enisa.europa.eu/publications/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime, accessed 8 May 2020).
- *Improving cooperation between CSIRTs and law enforcement: Legal and organisational aspects* (2017, www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement, accessed 1 May 2020).
- *Tools and methodologies to support cooperation between CSIRTs and law enforcement* (2017, www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement, accessed 1 May 2020).

A.4. Training-related material

- 2Centre (http://www.ucd.ie/cci/training.html).
- Academy of European Law (https://www.era.int/cgi-bin/cms?_SID=f0f6e006dc9e858d6dbcb8c5f27fc1f2bfb1d23e00642243117479&_sprache=en&_bereich=artikel&_aktion=detail&idartikel=128378).
- CEPOL (https://www.cepol.europa.eu/tags/cybercrime).
- Cybercrime Programme Office of the Council of Europe (C-PROC) (https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-).
- Economic Crime Division of the Council of Europe (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3c2).

- ENISA (https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material).
- European Judicial Training Network (http://www.ejtn.eu/Documents/Calendar%202020/EJTN%202020%20Calendar%20of%20training%20activities_WEB.pdf).
- FIRST (https://www.first.org/education/trainings).
- Interpol. Cybercrime training for police (https://www.interpol.int/Crimes/Cybercrime/Cybercrime-training-for-police).
- MISP – Open Source Threat Intelligence Platform supporting digital forensic and incident response (https://www.misp-project.org).
- NETRESEC (https://www.netresec.com/?page=Training).
- TF-CSIRT – Task Force on Computer Security Incident Response Teams (https://tf-csirt.org/transits/transits-materials/).

A.5. Country-specific material

A.5.1. Czechia

CZECHIA	
References	**Links**
Constitution and constitutional organs	
Constitution	https://psp.cz/en/docs/laws/constitution.html
Ministry of the Interior of the Czech Republic	https://www.mvcr.cz/mvcren
The Constitutional Court	https://www.usoud.cz/en/
National law	
Cybercrime legislation as provided by the country Wiki profile on the Council of Europe Octopus Community website, including status regarding the Budapest Convention	https://www.coe.int/en/web/octopus/-/czech-republic?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_DVQwVxnIMYnD&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-3&p_p_col_count=2
Criminal Code (Act No 40/2009 Coll.)	http://www.ejtn.eu/PageFiles/6533/Criminal %20Code %20of %20the %20Czech %20Republic.pdf
Code of Criminal Procedure (Act No 141/1961 Coll.)	https://www.legislationline.org/download/id/6371/file/Czech %20Republic_CPC_1961_am2012_en.pdf
Act on the Police of the Czech Republic (Ministry of the Interior, Act No 273/2008 Coll.)	https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=84765
Electronic Communications Act (Act No 127/2005 Coll.)	https://www.mpo.cz/assets/dokumenty/41287/56421/609851/priloha031.pdf
Act on Criminal Liability of Legal Persons and Proceedings against Them (Act No 418/2011 Coll.)	https://www.unodc.org/res/cld/document/criminal-liability-of-legal-persons-and-proceedings-against-them_html/418–2011_Act_on_Criminal_Liability_of_Legal_Persons_Czech_Republic.pdf
Act on Protection of Classified Information and Security Eligibility (Act No 412/2005 Coll.)	https://www.right2info.org/laws/Czech_Protection_classified_info.pdf
Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (No 33/1997 Coll)	https://www.coe.int/tr/web/octopus-old2019/country-wiki1/-/asset_publisher/hFPA5fbKjyCJ/content/czech-republic?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fel%2Fweb%2Foctopus-old2019%2Fcountry-wiki1%3Fp_p_id%3D101_INSTANCE_hFPA5fbKjyCJ%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D2
Act on the Protection of Personal Data (Act No 101/2000 Coll.)	https://www.advokatky.cz/?news=english-data-protection-act-no-101–2000-coll-repealed-in-full&lang=en
National Cyber Security Strategy	
National cybersecurity strategy and Action Plan	https://www.govcert.cz/download/gov-cert/container-nodeid-578/ap-cs-2015–2020-en.pdf

National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/czech-republic
Country profile from the Organisation for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/czech-republic
Police of the Czech Republic	https://www.policie.cz/clanek/Police-of-the-Czech-Republic.aspx
National Centre against Organised Crime SKPV (NCOZ SKPV)	https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpv.aspx
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-cz-en.do?member=1
Overview of the judicial system from the European Judicial Network (EJN)	www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/259
Fiche Belges on e-evidence from the EJN	www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/FB_CZ.pdf
Supreme Public Prosecutor of the Czech Republic	www.nsz.cz/index.php/en
CSIRTs	
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Czech %20Republic
Overview of FIRST members around the world – Czechia	https://www.first.org/members/map#country %3ACZ
Trusted Introducer (TI) European database of CSIRTs – see entries related to Czechia	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
Country profile from the European Judicial Training Network (EJTN) – Judicial Academy	http://www.ejtn.eu/About-us/Members/Czech-Republic/
Masaryk University – KYPO	https://www.kypo.cz/en
The Police Academy	https://www.polac.cz/g2/view.php?anglicky/index.html
Other documents	
Council of the European Union – report on Czechia	http://data.consilium.europa.eu/doc/document/ST-13203–2016-REV-1-DCL-1/en/pdf

A.5.2. France

FRANCE	
References	**Links**
Constitution and constitutional organs	
Constitution	https://www.constituteproject.org/constitution/France_2008.pdf?lang=en; https://www.legifrance.gouv.fr/Droit-francais/Constitution
Council of State (Conseil d'État)	https://www.conseil-etat.fr/en/
Supreme Court (Court of Cassation)	https://www.courdecassation.fr/about_the_court_9256.html
National law	
Cybercrime legislation as provided by the country Wiki profile on the Council of Europe Octopus Community website, including status regarding the Budapest Convention	https://www.coe.int/en/web/octopus/-/france?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_DVQwVxnIMYnD&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-3&p_p_col_count=2
Code of Criminal Procedure	https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154?etatTexte=VIGUEUR&etatTexte=VIGUEUR_DIFF
CNIL (Data Protection Authority)	http://www.cniLoifr/
National Cyber Security Strategy	
National Cyber Security Strategies	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/information-systems-defence-and-security-frances-strategy/@@download_version/c7d0d0671bbc4756afd87513675d58eb/file_en
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/france
Country profile from the Organisation for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/index.php/country-profiles/france
Central Directorate of the Judicial Police (DCPJ)	https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire
La brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI)	https://www.prefecturedepolice.interieur.gouv.fr/Cybersecurite/Les-actions-PP/Les-brigades-de-police-judiciaire/La-BEFTI
National Gendarmerie	http://www.gendarmerie.interieur.gouv.fr/fre/Sites/Gendarmerie/Zooms/Cybercriminalite
Central Office for Combating Information and Communication Technology Crime (OCLCTIC)	https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite
Centre for the Fight against Digital Crimes (C3N)	https://www.gendarmerie.interieur.gouv.fr/pjgn/SCRCGN/Le-centre-de-lutte-contre-les-criminalites-numeriques-C3N

National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-fr-en.do?member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/273
Public Prosecutor's Office (Ministère public)	https://www.vie-publique.fr/fiches/38127-procureur-parquet-ministere-public
CSIRTs	
InterCERT-FR	https://cert.ssi.gouv.fr/csirt/intercert-fr
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=France
Overview of FIRST members around the world – France	https://www.first.org/members/map#country %3AFR
Trusted Introducer (TI) European database of CSIRTs – see entries related to France	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
Country profile from the European Judicial Training Network (EJTN) – French National School for the Judiciary	http://www.ejtn.eu/About-us/Members/France/
Cybercrime Centres of Excellence Network for Training Research and Education (2Centre)	https://www.2centre.eu/
European Cybercrime Training and Education Group (ECTEG) – see institutions and agencies related to France	https://www.ecteg.eu/members/
French Expert Center Against Cybercrime	https://www.cecyf.fr
Centre de formation à la sécurité des systèmes d'information (CFSSI)	https://www.ssi.gouv.fr/administration/formations/
Other documents	
Council of the European Union – report on France	https://data.consilium.europa.eu/doc/document/ST-7588–2015-REV-2-DCL-1/en/pdf

A.5.3. Germany

GERMANY	
References	**Links**
Constitution and constitutional organs	
Constitution	https://www.bmi.bund.de/EN/topics/constitution/constitutional-issues/constitutional-issues.html
Federal President	http://www.bundespraesident.de
Bundestag	http://www.bundestag.de
Federal Government	http://www.bundesregierung.de/
Bundesrat	http://www.bundesrat.de/
Federal Constitutional Court	https://www.bundesverfassungsgericht.de/EN/Das-Gericht/das-gericht_node.html
National law	
Cybercrime legislation as provided by the country Wiki profile on the Council of Europe Octopus Community website, including status regarding the Budapest Convention	https://www.coe.int/en/web/octopus/-/germany?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_DVQwVxnIMYnD&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-3&p_p_col_count=2
Act on the Federal Office for Information Security (BSI Act – BSIG)	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=2
National Cyber Security Strategy	
National Cyber Security Strategies	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/germany
Country profile from the Organization for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/germany
Federal Criminal Police Office (BKA)	https://www.bka.de/EN/OurTasks/AreasOfCrime/Cybercrime/cybercrime_node.html
Federal Criminal Police Office Cybercrime Office (BKA-CC)	https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/cybercrime_node.html
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-de-en.do?member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/277
Fiche Belges on e-evidence from the EJN	https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/FBEEGermany.pdf

The Federal Public Prosecutor General (Der Generalbundesanwalt beim Bundesgerichtshof – GBA)	https://www.generalbundesanwalt.de/DE/Home/home_node.html
CSIRTs	
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Germany
Overview of FIRST members around the world – Germany	https://www.first.org/members/map#country %3ADE
Trusted Introducer (TI) European database of CSIRTs – see entries related to Germany	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
IT-Grundschutz	https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz.html
German Judicial Academy (Deutsche Richterakademie)	http://www.deutsche-richterakademie.de/icc/draen/nav/123/broker?editmode=false
Brandenburg Judicial Academy (Justizakademie des Landes Brandenburg)	http://www.justizakademie.brandenburg.de/sixcms/detail.php?id=145097
European Cybercrime Training and Education Group (ECTEG) – see institutions and agencies related to Germany	https://www.ecteg.eu/members/
Other documents	
Council of the European Union – report on Germany	http://data.consilium.europa.eu/doc/document/ST-7159–2017-REV-1-DCL-1/en/pdf

A.5.4. Luxembourg

LUXEMBOURG	
References	**Links**
Constitution and constitutional organs	
Constitution	http://data.legilux.public.lu/file/eli-etat-leg-recueil-constitution-20161020-fr-pdf.pdf; https://www.constituteproject.org/constitution/Luxembourg_2009.pdf?lang=en
Council of State (Conseil d'État)	http://www.conseil-etat.public.lu/fr.html; https://gouvernement.lu/en/systeme-politique/conseil-etat.html
Unicameral parliament (Chambre des Députés)	http://www.chd.lu/
Court of Auditors (Cour des comptes)	http://www.cour-des-comptes.lu/
High Commission for National Protection (Haut-Commissariat à la Protection Nationale – HCPN)	https://hcpn.gouvernement.lu/en/service.html
National law	
Cybercrime legislation as provided by the country Wiki profile on the Council of Europe Octopus Community website, including status regarding the Budapest Convention	https://www.coe.int/en/web/octopus/-/luxembourg
National Cyber Security Strategy	
National Cyber Security Strategies	https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/national-cybersecurity-strategy-3/national-cybersecurity-strategy-iii-en-.pdf
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/luxembourg
Country profile from the Organisation for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/luxembourg
Grand-Ducal Police (Police Grand-Ducale)	https://police.public.lu/fr/support/recherche.html?q=cybercrime
Central Directorate of the Judicial Police (DCPJ)	https://police.public.lu/fr/votre-police/a-propos-de-la-police/direction-centrale-police-judiciaire.html
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-lu-en.do?member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/314
Public Prosecutor's Office (Parquet général)	https://guichet.public.lu/en/organismes/organismes_citoyens/parquet-general.html
National courts	https://gouvernement.lu/en/systeme-politique/cours-tribunaux.html https://www.lexadin.nl/wlg/courts/nofr/eur/lxctlux.htm

CSIRTs	
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Luxembourg
Overview of FIRST members around the world – Luxembourg	https://www.first.org/members/map#country %3ALU
Trusted Introducer (TI) European database of CSIRTs – see entries related to Luxembourg	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
European Judicial Training Network (EJTN) – Essential EU competition law – training for French and Luxembourgish judges	http://www.ejtn.eu/Catalogue/Catalogue-2019/Training-for-French-and-Luxembourgish-Judges-on-EU-Competition-Law/
Computer Incident Response Center Luxembourg (CIRCL)	http://www.circl.lu/services/training/
Institute for Legal Support and Technical Assistance (ILSTA)	http://www.ilsta.org/prosecutors-police-receive-training-combating-organised-crime/
ENFORCE Project	https://securitymadein.lu/news/ceis-securitymadein-lu-enforce-project/
CEIS	https://ceis.eu/en/home/
Other documents	
Council of the European Union – report on Luxembourg	https://data.consilium.europa.eu/doc/document/ST-7162–2017-REV-1-DCL-1/en/pdf

A.5.5. Norway

NORWAY	
References	**Links**
Constitution and constitutional organs	
Constitution	https://lovdata.no/dokument/NLE/lov/1814–05–17?q=grunnloven; https://lovdata.no/dokument/NL/lov/1814–05–17
Norwegian National Security Authority (NSM)	www.nsm.stat.no
National Criminal Investigation Service (NCIS)	https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/
Norwegian National Cyber Security Centre (NCSC)	https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter; https://nsm.no/areas-of-expertise/cyber-security/norwegian-national-cyber-security-centre-ncsc/
Norwegian Intelligence Service (E-tjenesten)	www.forsvaret.no/organisasjon/etterretningstjenesten
Norwegian Data Protection Authority (Datatilsynet)	www.datatilsynet.no
Norwegian Communications Authority (Nkom)	www.nkom.no
Norwegian Centre for Information Security (NorSIS)	www.norsis.no
National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim)	https://www.okokrim.no
Joint Cyber Coordination Centre (Felles cyberkoordineringssenter – FCKS)	https://nsm.no/om-oss/historien-om-nsm/felles-cyberkoordineringssenter-fcks-etableres
National law	
Cybercrime legislation as provided by the country Wiki profile on the Council of Europe Octopus Community website, including status regarding the Budapest Convention	https://www.coe.int/en/web/octopus/-/norway
Criminal code	https://app.uio.no/ub/ujur/oversatte-lover/data/lov-19020522–010-eng.pdf; https://lovdata.no/dokument/NLE/lov/2005–05–20–28/KAPITTEL_2#KAPITTEL_2
Criminal Procedure Act	https://app.uio.no/ub/ujur/oversatte-lover/data/lov-19810522–025-eng.pdf
Electronic Communication Act	https://lovdata.no/dokument/NL/lov/2003–07–04–83
Personal Data Act	https://app.uio.no/ub/ujur/oversatte-lover/data/lov-20000414–031-eng.pdf
National Cyber Security Strategy	
National Cyber Security Strategies	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategy-for-

	information-security/@@download_version/f201ff6da6eb4101b1ca050e79f53975/file_en
National law enforcement	
Europol press release on cooperation with Norwegian LE	https://www.europol.europa.eu/newsroom/news/europol-and-norway-join-forces-in-combating-cybercrime
Country profile from the Organization for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/index.php/country-profiles/Norway
National Police Directorate (POD)	www.politiet.no
Norwegian Police Security Service (PST)	www.pst.politiet.no
National Cybercrime Centre (NC3)	https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/national-cybercrime-centre/
National judicial authorities	
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/342
Supreme Court	https://www.domstol.no/en/the-courts-of-justice/The-ordinary-courts-of-Norway/The-Supreme-Court/
Courts of Appeal	https://www.domstol.no/en/the-courts-of-justice/The-ordinary-courts-of-Norway/courts-of-appeal/
District Courts	https://www.domstol.no/en/the-courts-of-justice/The-ordinary-courts-of-Norway/district-courts/
Higher Prosecuting Authority	https://www.riksadvokaten.no/english/
CSIRTs	
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Norway
Overview of FIRST Members around the world – Norway	https://www.first.org/members/map#country %3ANO
Trusted Introducer (TI) European database of CSIRTs – see entries related to Norway	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
European Cybercrime Training and Education Group (ECTEG) – see institutions and agencies related to Norway	https://www.ecteg.eu/members/
Norwegian Police University College	https://www.politihogskolen.no

A.5.6. Portugal

PORTUGAL	
References	**Links**
Constitution and constitutional organs	
Constitution	https://www.parlamento.pt/sites/EN/Parliament/Documents/Constitution7th.pdf
ANACOM – National Communications Authority	https://www.anacom.pt/
National law	
Cybercrime legislation as provided by the country Wiki profile on the Council of Europe Octopus Community website, including status regarding the Budapest Convention	https://www.coe.int/en/web/octopus/-/portugal?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_DVQwVxnIMYnD&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-3&p_p_col_count=2
Penal Code	https://www.verbojuridico.net/download/portuguesepenalcode.pdf
National Cyber Security Strategy	
National Cyber Security Strategies	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/portuguese-ncss/@@download_version/ae00f93801664a57b22f9f5f96c1cd01/file_en
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/portugal
Country profile from the Organization for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/portugal
Public Security Police (PSP)	https://www.psp.pt/Pages/homePage.aspx
National Unit to Combat Cybercrime and Technological Crime (UNC3T)	https://www.policiajudiciaria.pt/unc3t/
Judicial Police	http://www.pj.pt
Internal Intelligence Service	https://www.sis.pt/en
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-pt-en.do?member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/352
Fiche Belges on e-evidence from the EJN	https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/New%20Fiches%20Belges%20on%20electronic%20evidence%20-%20Portugal.pdf
Supreme Court of Justice	http://en.ministeriopublico.pt/en/pagina/supreme-court-justice

Supreme Administrative Court	http://en.ministeriopublico.pt/en/pagina/supreme-administrative-court
Court of Audit	http://en.ministeriopublico.pt/en/pagina/court-audit
Central Department of Criminal Investigation and Prosecution (DCIAP)	http://en.ministeriopublico.pt/en/pagina/central-department-criminal-investigation-and-prosecution
Prosecutor General's Office (PGR)	http://en.ministeriopublico.pt/node/4084
Public Prosecution Service (PPS)	http://en.ministeriopublico.pt
CSIRTs	
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#team=CSIRT%20Altice%20Portugal
Overview of FIRST members around the world – Portugal	https://www.first.org/members/map#country%3APT
Trusted Introducer (TI) European database of CSIRTs – see entries related to Portugal	https://www.trusted-introducer.org/directory/country_LICSA.html
Training	
European Cybercrime Training and Education Group (ECTEG) – see institutions and agencies related to Portugal	https://www.ecteg.eu/members/
Portuguese National Cybersecurity Centre	https://www.cncs.gov.pt/en/activities/training-offer/
Police Training School (Escola Prática de Polícia)	http://www.epp.pt/Pages/inglesmissao.htm
Higher Institute of Police Sciences and Internal Security	http://www.iscpsi.pt/Inicio/Paginas/default.aspx
Centre for Judiciary Studies	http://www.cej.mj.pt/cej/eng/training_admission_to_initial_training.php

A.5.7. Romania

ROMANIA	
References	**Links**
Constitution and constitutional organs	
Constitution	http://www.cdep.ro/pls/dic/site2015.page?id=339&idl=2
Ministry of Justice	http://www.just.ro/en/
Superior Council of Magistracy	https://www.csm1909.ro
Directorate for Investigation of Organised Crime and Terrorism	https://www.diicot.ro
National law	
Cybercrime legislation as provided by the country Wiki profile on the Council of Europe Octopus Community website, including status regarding the Budapest Convention	https://www.coe.int/en/web/octopus/-/romania?
Criminal Code	http://legislatie.just.ro/Public/DetaliiDocument/109855
Criminal Procedure Code	http://legislatie.just.ro/Public/DetaliiDocument/120611
Law No 362/2018 on the security of computer networks and systems	https://cert.ro/vezi/document/legea-nr-362-din-28-decembrie-2018
National Cyber Security Strategy	
National Cyber Security Strategies	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania/@@download_version/1b41c7f470b14b52be67866e84007f87/file_en
National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/romania
Country profile from the Organization for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/romania
Romanian Police	https://www.politiaromana.ro/en/romanian-police
Combating Organized Crime Directorate	https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-combatere-a-criminalitatii-organizate/directia-de-combatere-a-criminalitatii-organizate/directia-de-combatere-a-criminalitatii-organizate
General Inspectorate of Romanian Police – Fraud Investigations Directorate (GIRP – FID)	http://www.citycop.eu/the-consortium/partners/general-inspectorate-of-romanian-police.kl
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-ro-en.do?member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/354

Fiche Belges on e-evidence from the EJN	https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/New %20Fiches %20Belges %20on %20electronic %20evidence.pdf
High Court of Cassation and Justice	http://www.scj.ro/en
Prosecutor's Office attached to the High Court of Cassation and Justice (POHCCJ)	https://www.mpublic.ro/en
Superior Council of Magistracy	https://www.csm1909.ro
Prosecutor's Office	https://www.mpublic.ro/en
National courts portal	http://portal.just.ro/SitePages/acasa.aspx
Ministry of Justice e-guide on international judicial cooperation in criminal matters	http://www.just.ro/en/despre/cooperare-judiciara-internationala-in-materie-penala/
CSIRTs	
Overview of FIRST Members around the world – Romania	https://www.first.org/members/map#country %3ARO
National CSIRT profile from the Trusted Introducer (TI) European database of CSIRTs	https://www.trusted-introducer.org/directory/teams/cert-ro.html
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Romania
National Cyberint Centre	https://www.sri.ro/cyberintelligence
Operational Response Centre for Security Incidents (CORIS-STS)	https://www.sts.ro/en/coris-sts
Training	
Police Academy	https://www.academiadepolitie.ro
Police Officers School in Romania	http://www.scoalapolitie.ro
Ministry of Justice	http://www.just.ro/en/despre/ghiduri-si-manuale/
Romanian Centre of Excellence for Cybercrime Investigation Training (CYBEREX-RO)	https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2011_ISEC_AG_INT_4000002223_en

A.5.8. Sweden

SWEDEN	
References	**Links**
Constitution and constitutional organs	
Constitution	https://www.riksdagen.se/globalassets/07.-dokument–lagar/the-constitution-of-sweden-160628.pdf
Swedish Civil Contingencies Agency (Myndigheten för Samhällsskydd och beredskap – MSB)	https://www.msb.se/en
National Defence Radio Establishment (Försvarets radioanstalt – FRA)	https://www.fra.se/system/engelska/english.4.6a76c4041614726b25ae4.html; http://www.fra.se
Swedish Defence Materiel Administration (Försvarets materielverk – FMV)	https://www.fmv.se/english/
Swedish Armed Forces (Försvarsmakten)	https://www.forsvarsmakten.se/en/
Swedish Post and Telecom Authority (Post-och telestyrelsen – PTS)	https://www.pts.se/en/
Swedish Security Service (Säkerhetspolisen – SÄPO)	https://www.sakerhetspolisen.se/en/swedish-security-service.html
National law	
Cybercrime legislation as provided by the country Wiki profile on the Council of Europe Octopus Community website, including status regarding the Budapest Convention	https://www.coe.int/en/web/octopus/-/sweden
Cybercrime legislation	https://rm.coe.int/octocom-legal-profile-sweden/16809ed733
Penal Code	https://www.regeringen.se/49bb67/contentassets/72026f30527d40189d74aca6690a35d0/the-swedish-penal-code
Criminal Code (Brottsbalken, SFS 1962:700)	https://www.government.se/49f780/contentassets/7a2dcae0787e465e9a2431554b5eab03/the-swedish-criminal-code.pdf
Act on Electronic Communication (2003:389)	https://wipolex.wipo.int/en/legislation/details/17726
Code of Judicial Procedure	https://www.government.se/49e41c/contentassets/a1be9e99a5c64d1bb93a96ce5d517e9c/the-swedish-code-of-judicial-procedure-ds-1998_65.pdf
Act on Copyright in Literary and Artistic Works (SFS 1960:729)	https://www.wipo.int/edocs/lexdocs/laws/en/se/se124en.pdf
National Cyber Security Strategy	
National Cyber Security Strategies	https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy/@@download_version/d8934f793fe048d09804a9f17c41d13b/file_en

National law enforcement	
Overview of national law enforcement from the Europol website	https://www.europol.europa.eu/partners-agreements/member-states/sweden
Country profile from the Organization for Security and Co-operation in Europe (OSCE)	https://polis.osce.org/country-profiles/sweden
Swedish Police Authority (Den Svenska Polismyndigheten)	https://polisen.se/en/
Swedish Cybercrime Centre (SC3)	https://polisen.se/om-polisen/organisation/
National Forensic Centre (Nationellt Forensiskt Centrum – NFC)	https://nfc.polisen.se/en/
National Fraud Centre	https://polisen.se/om-polisen/organisation/
National Operations Department (Nationella operativa avdelningen – NOA)	https://polisen.se/om-polisen/organisation/
National judicial authorities	
Overview of the judicial system from the e-Justice portal	https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-se-en.do?member=1
Overview of the judicial system from the European Judicial Network (EJN)	https://www.ejn-crimjust.europa.eu/ejn/EJN_InfoAbout/EN/378
Fiche Belges on e-evidence from the EJN	https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/FB_SV.pdf
Supreme Court	http://old.domstol.se/Funktioner/English/The-Swedish-courts/The-Supreme-Court
Administrative courts	http://old.domstol.se/Funktioner/English/The-Swedish-courts/County-administrative-courts/
District court	http://old.domstol.se/Funktioner/English/The-Swedish-courts/District-court/
Swedish National Courts Administration (Domstolsverket)	http://old.domstol.se/Funktioner/English/The-Swedish-courts/; https://lagrummet.se/English
Swedish Prosecution Authority (Åklagarmyndigheten)	https://www.aklagare.se/en/
Swedish Economic Crime Authority (Ekobrottsmyndigheten)	https://www.ekobrottsmyndigheten.se/en/
CSIRTs	
Overview of FIRST Members around the world – Sweden	https://www.first.org/members/map#country %3ASE
National CSIRT profile from the Trusted Introducer (TI) European database of CSIRTs	https://www.trusted-introducer.org/directory/teams/cert-se.html
ENISA CSIRTs by country – interactive map	https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Sweden
Training	
European Cybercrime Training and Education Group (ECTEG) – see	https://www.ecteg.eu/members/

institutions and agencies related to Sweden	
Swedish National Police Academy (Polishögskolan)	https://polisen.se/om-polisen/bli-polis/polisutbildningen/
Swedish Judicial Training Academy	http://www.domstol.se/
Other documents	
Council of the European Union – report on Sweden	http://data.consilium.europa.eu/doc/document/ST-8188–2017-REV-1-DCL-1/en/pdf

B ANNEX: EXAMPLES OF COURSES AND TRAINING PROGRAMMES

This list of courses and training programmes for LE, judiciary and CSIRTs is not exhaustive and does not contain national training initiatives.

Courses and training programmes for LE, judiciary and CSIRTs	
Courses and training programmes for CSIRTs	
European Union Agency for Cybersecurity (ENISA)	https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
FIRST	https://www.first.org/education/trainings
TF-CSIRT	https://tf-csirt.org/transits/transits-materials/
MISP – Open Source Threat Intelligence Platform Supporting Digital Forensic and Incident Response	https://www.misp-project.org
ENISA/EC3 Workshop (which included CSIRT–LE joint training sessions)	https://www.enisa.europa.eu/events/8th-enisa-ec3-workshop
Courses and training programmes for law enforcement	
CEPOL	https://www.cepol.europa.eu/tags/cybercrime
Europol	https://www.europol.europa.eu/activities-services/services-support/training-and-capacity-building
Council of Europe	https://www.coe.int/en/web/cybercrime/trainings
ENISA/EC3 Workshop (which included CSIRT–LE joint training sessions)	https://www.enisa.europa.eu/events/8th-enisa-ec3-workshop
Interpol	https://www.interpol.int/Crimes/Cybercrime/Cybercrime-training-for-police
2Centre	http://www.ucd.ie/cci/training.html
Courses and training programmes for judiciary	
Council of Europe	https://www.coe.int/en/web/cybercrime/trainings
Economic Crime Division of the Council of Europe	https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3c2
European Judicial Training Network	http://www.ejtn.eu/Documents/Calendar %202020/EJTN %202020 %20Calendar %20of %20training %20activities_WEB.pdf
Academy of European Law	https://www.era.int/cgi-bin/cms?_SID=f0f6e006dc9e858d6dbcb8c5f27fc1f2bfb1d23e00642243117479&_sprache=en&_bereich=artikel&_aktion=detail&idartikel=128378

C ANNEX: EXAMPLES OF RELEVANT NATIONAL LEGAL FRAMEWORKS

The list of provisions mentioned in this annex is not exhaustive; the provisions are listed only as examples. While efforts were made to ensure that the information provided is accurate and up-to-date, it cannot be guaranteed that this is the case. In addition to the legislative instruments listed below, it should be noted that the constitutional frameworks of the EU Member State and EFTA countries listed below encompass fundamental legal principles, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights.

C.1. Czechia

Specific legislation on cybercrime in Czechia has been enacted through the following legal instruments:

- Criminal Code (Act No 40 of 2009 Coll.), in particular cybercrime-specific offences and provisions on unlawful access to computer systems and data and offences related to child pornography;
- Code of Criminal Procedure (Act No 141 of1961 Coll.), in particular provisions on the expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and search and seizure of stored computer data;
- Act on the Police of the Czech Republic (Act No 273 of 2008);
- Electronic Communications Act (Act No 127 of 2005);
- Act on Criminal Liability of Legal Persons and Proceedings against Them (Act No 418 of 2011);
- Act on Protection of Classified Information and Security Eligibility (Act No 412 of 2005);
- Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (No 33 of 1997);
- Act on the Protection of Personal Data (Act No 101 of 2000);
- Act on International Judicial Cooperation in Criminal Matters (Act No 10420 of March 2013);
- National law transposing Directive 2013/40/EU on attacks against information systems (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040);
- National law transposing Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX %3A32016L1148);
- Council of Europe Convention on Cybercrime, ratified by Czechia on 22 August 2013 (further information is available in the relevant section of the following website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures).

C.2. France

Specific legislation on cybercrime in France has been enacted through the following legal instruments:

- Criminal Code, in particular offences related to illegal access (Article 323-1 al.1), data interference (Article 323-1 al.2 and Article 323-3) and system interference (Article 323-2), as well as misuse of devices (Article 323-3-1 CP);
- Criminal Procedure Code;
- Data Protection Act (Law on Information Technology, Data Files and Civil Liberties No 78–17 of 6 January 1978, as successively amended);
- Law for a Digital Republic (No 321 of 7 October 2016);
- Law on the protection of personal data (No 793 of 20 June 2018) transposing the GDPR;
- Law on the confidence in the digital economy (No 575 of 21 June 2004);
- Law adapting the judiciary to developments in crime (No 204 of 9 March 2004);
- Law on Copyright and Related Rights in the Information Society (No 961 of 1 August 2006);
- Law on orienting and planning the performance of internal security II (No 267 of 14 March 14);
- Law on electronic communications and audiovisual communication services (No 669, of 9 July 2004);
- Law on crime prevention (No 297 of 5 March 2007);
- National law transposing Directive 2013/40/EU on attacks against information systems (further information available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040);
- National law transposing Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX %3A32016L1148);
- Council of Europe Convention on Cybercrime, ratified by France on 10 January 2006 (further information is available in the relevant section of the following website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures).

C.3. Germany

Specific legislation on cybercrime in Germany has been enacted through the following legal instruments:

- Criminal Code, in particular offences related to illegal access, unlawful interception, data manipulation, computer sabotage, computer forgery, computer fraud, distribution of access codes or malware and illegal reproduction of protected programmes;
- Code of Criminal Procedure, in particular specific procedural measures following the ratification and adoption of the Council of Europe Convention on Cybercrime by Germany;
- Electronic Signature Act of 2001;
- Freedom of Information Act of 2013;
- Act on the Federal Office for Information Security (BSI Act) of 14 August 2009;
- Telecommunications Act;
- Federal Data Protection Act of 30 June 2017;
- Act on Internet Services;
- National law transposing Directive 2013/40/EU on attacks against information systems (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040);

- National law transposing Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX %3A32016L1148);
- Council of Europe Convention on Cybercrime, ratified by Germany on 9 March 2009 (further information is available in the relevant section of the following website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures).

C.4. Luxembourg

Specific legislation on cybercrime in Luxembourg has been enacted through the following legal instruments:

- Criminal Code;
- Code of Criminal Procedure;
- Law of 15 July 1993 reinforcing the fight against economic crime and computer fraud;
- Law on Data Protection on Electronic Communications;
- Law on Electronic Commerce;
- Law on Electronic Signature and Cryptography;
- Law on the Protection of Individuals with Regard to the Processing of Personal Data;
- National law transposing Directive 2013/40/EU on attacks against information systems, (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040);
- National law transposing the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX %3A32016L1148);
- Council of Europe Convention on Cybercrime, ratified by Luxembourg on 16 October 2014 (further information is available in the relevant section of the following website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures)

C.5. Norway

Specific legislation on cybercrime in Norway has been enacted through the following legal instruments:

- Criminal Code, in particular Section 145 on illegal interception and misuse of devices, Section 291 on data interference and system interference and Section 145b on unlawful spreading of data;
- Criminal Procedure Act (No 25 of 22 May 1981), in particular Section 216a;
- Electronic Communications Act;
- Personal Data Act of 15 June 2018;
- Council of Europe Convention on Cybercrime, ratified by Norway on 30 June 2006 (further information is available in the relevant section of the following website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures).

C.6. Portugal

Specific legislation on cybercrime in Portugal has been enacted through the following legal instruments:

- Cybercrime Law No 109 of 2009;
- Code of Criminal Procedure (adopted by Decree-Law No 78 of 17 February 1987, amended by Law No 58 of 23 June 2015);
- Computer Crime Law No 109 of 1991;
- Criminal Code;

- Crime Investigation Law No 21 of 2000);
- Cybersecurity Law No 46 of 2018;
- Electronic Communications Law No 5 of 2004;
- Electronic Commerce Law No 46 of 2012;
- Directive 2013/40/EU on attacks against information systems, transposed into national law (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040);
- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, transposed into national law (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX %3A32016L1148);
- Council of Europe Convention on cybercrime, ratified by Portugal on 24 March 2010 (further information is available in the relevant section of the following website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures).

C.7. Romania

Specific legislation on cybercrime in Romania has been enacted through the following legal instruments:

- Criminal Code;
- Criminal Procedure Code, in particular provisions on audio or video interception and recording;
- Romanian Copyright Law (No 8 of 1996);
- Law Preventing and Suppressing Cybercrime, subsequently amended and supplemented (No 161/20);
- Law on E-Commerce (No 365 of 2002);
- Law to Prevent and Punish Money Laundering, and Setting Forth Measures to Prevent and Suppress the Financing of Terrorist Acts (No 656 of 2002);
- Law to Prevent and Suppress Terrorism (No 535 of 2004);
- National law transposing Directive 2013/40/EU on attacks against information systems (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040);
- National law transposing Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX %3A32016L1148);
- Council of Europe Convention on Cybercrime, ratified by Romany on 12 May 2004 (further information is available in the relevant section of the following website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures).

C.8. Sweden

Specific legislation on cybercrime in Sweden has been enacted through the following instruments:

- Criminal Code, in particular Chapter 4, Section 9c, on misuse of cyberspace (illegal access to information systems, illegal system interference and illegal data interference), Chapter 4, Section 8, on illegal interception of computer data and Chapter 9 on fraud and other dishonesty;
- Code of Criminal Procedure, in particular Chapter 27 on seizure, secret wire-tapping, etc.;
- Code of Judicial Procedure of 1942 (SFS 1942:740), as successively amended;
- Swedish Copyright Act of 1960 (SFS 1960:729), as successively amended;
- Act on Electronic Communication of 2003 (SFS 2003:389), as successively amended;

- National law transposing the Directive 2013/40/EU on attacks against information systems (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040);
- National law transposing the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (further information is available in the relevant section of the following website: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX %3A32016L1148);
- Council of Europe Convention on Cybercrime, signed by Sweden on 23 November 2001 (further information is available in the relevant section of the following website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures).

D ANNEX: TOWARDS DEVELOPING A DECISION SUPPORT SYSTEM FOR CSIRT–LE COOPERATION

D.1. Example of completed SoD matrix

In the following table, an indicative example of a SoD matrix, completed using the RSCI method, is presented. The broader scope of the SoD methodology on CSIRT–LE cooperation is to develop a decision support system that could provide information related to the authorities that can be contacted in the case of a cybersecurity incident/cybercrime. In particular, the user of such a decision support system should be able to find the appropriate contact (i.e. the authority or the community) who is responsible (R – as described in the RSCI method) for a specific duty.

For instance, someone who is responsible for collecting cyberthreat intelligence in Romania could use the SoD matrix to find who to contact, i.e. to find the CSIRT in Romania that is responsible for performing this specific duty.

The data in the following table were provided by the Member State representatives who participated in the interviews conducted for collecting data for this report. Although some interviewees provided their consent for their affiliation and country to be included in the report, information on countries and authorities have been removed from the table. A greater sample of replies is needed to validate the data collected during the interviews and to enable official results to be presented for each country.

			Responsible **(R)**: Supporting **(S)**: Consulted **(C)**: Informed **(I)**:					
Duties	**Country**	**Authority**	CSIRT	LE	Prosecutors	Judges	**Short description of their key responsibilities of the authority**	**Website of the authority**
Delivering training	**Country A**	**Authority A**	**S**	**R**			Short description of key responsibilities of Authority A	URL of home page of Authority A
Participating in training	**Country A**	**Autority B**	**S**	**R**	**C**		Short description of key responsibilities of Authority B	URL of home page of Authority B
Collecting cyber threat intelligence	**Country A**	**Authority A**	**R**	**S**			Short description of key responsibilities of Authority A	URL of home page of Authority A
Analysing vulnerabilities and threats	**Country A**	**Authority A**	**R**				Short description of key responsibilities of Authority A	URL of home page of Authority A
Issuing recommendations for new vulnerabilities and threats	**Country A**	**Authority C**	**R**				Short description of key responsibilities of Authority C	URL of home page of Authority C

E ANNEX: INTERVIEW QUESTIONNAIRE

Questionnaire to Support the interviews with subject matter experts to collect data for the 2020 ENISA Report on CSIRTs and LE Cooperation.

The questions below have been prepared to support the interviews with subject matter experts to collect data for the 2020 ENISA report on CSIRTs and LE cooperation along with their interaction with the judiciary. This report contributes to the implementation of the ENISA programming document 2020–2022 (https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022) in particular "Output O.4.2.2 – Support the fight against cybercrime and collaboration across CSIRTs, LEA and other operational communities".

The report is expected to be ready for publication by the end of 2020.

ENISA selected some external experts from the List of NIS Experts compiled following the ENISA Call for Expression of Interest (CEI) (Ref. ENISA M-CEI-17-T01) to support the data collection (including the interviews) and the drafting of this report.

The expected duration of the interview is 1 hour.

For more information regarding this questionnaire and the report, please contact: CSIRT-LE-cooperation@enisa.europa.eu

Contact details

Interviewer:
Date of the interview:
Name of the interviewee:
Affiliation:
Position:
Country:

Section 1 – Questions on general legal/organisational aspects

1. What is the **role** of your organisation in fighting cybercrime activities?

2. Does your **legal framework support the cooperation** between CSIRT/LEA and the interaction/information flow with the judiciary (prosecutors and judges) in cybercrime proceedings and in general in responding to cybercrime? If so, how?

3. Regarding cybercrime cases, could you briefly describe **how information is shared** between CSIRTs – national and governmental in particular – LEAs, prosecutors and judges?

QUESTIONS ON SEGREGATION OF DUTIES (SOD) MATRIX

4. Referring to the **SoD matrix** that was sent to you prior to this interview (and you can also find it in Annex I at the end of this questionnaire), could you fill it out by identifying for each duty which actor (CSIRT, LE, Prosecutors, Judges) in your country is:

    - **Responsible (R):** responsible for performing this duty, is the decision-maker
    - **Supporting (S):** providing support when performing this duty (if applicable)
    - **Consulted (C):** consulted during the performance of this duty (if applicable)
    - **Informed (I):** informed when performing this duty? (if applicable)
    -

SEE SoD MATRIX in ANNEX I at the end of this questionnaire

Section 2: Questions on possible synergies and potential interferences

5. In your opinion, which are the possible **synergies** across CSIRT/LE and judiciary during the performance of their fighting cybercrime-related duties? Have you seen in reality such synergies taking place? Could you give us an example?

In your opinion, which are the potential interferences across CSIRT/LE and judiciary during the performance of their fighting cybercrime-related duties? Have you seen in reality such interference taking place? Could you provide an example?

Section 3 – Questions on challenges

6. Are there **any specific challenges** that you would like to mention **about cooperation across the CSIRT/LE and judiciary communities**? If yes, what kind of challenges (e.g. legal, organisational, technical, cultural).

7. Are there any **challenges that you would like to mention in particular regarding digital forensics and electronic evidence** (e-evidence)?

Section 4 – Questions on competences and training

8. What are the **competencies that your organisation/community has and could share** with the other communities (in particular CSIRT with LE/judiciary, LE with CSIRT, and judiciary with CSIRT)?

9. Which **competencies do you feel are lacking/could be improved in your organisation/community and you might improve by learning from another community** (e.g. CSIRT from LE/judiciary, LE from CSIRT, and judiciary from CSIRT)

Does your organisation organise and/or participate in **joint training** across CSIRTs, LEAs and judiciary (prosecutor and judges) communities? If yes, do you find them useful?

10. Section 5 – Question on COVID-19 pandemic crisis

11. Has the COVID-19 pandemic crisis changed the way CSIRT/LE/judiciary work together? If yes, how so? Could you provide an example? (e.g. less meetings in person, but on the other hand more communication via email and over the phone)

Section 6 – Question on cybersecurity certification of forensic tools

12. Do you think that a cybersecurity certification of forensic tools would help the CSIRT/LE/judiciary cooperation? (e.g. if CSIRTs use certified tools, the LE and Judiciary might trust more the data provided by CSIRT and use them more easily as evidence in court)

Section 7 – Question on any additional information or comments

13. Would you like to share any additional information or provide us with any comment?

QUESTIONS ON MENTIONING OF NAME, AFFILIATION, AND COUNTRY

- Do you agree to have your forename, surname, affiliation and country mentioned in the report? (NOTE: it is not confirmed whether names of interviewees will be mentioned in the report)

Yes ☐ No ☐

- Do you agree to have your forename, surname, affiliation and country mentioned in the acknowledgements of the report? (NOTE: it is not confirmed whether names of interviewees will be mentioned in the acknowledgements of the report)

Yes ☐ No ☐

- Do you agree to have stated in the report that information on your country has been collected via an interview with a CSIRT/LE/judiciary (prosecutor/judge) representative?

Yes	☐	No ☐

Privacy Statement – ENISA Report on CSIRT-LE cooperation

Your personal data shall be processed in accordance with the Regulation (EU) 2018/1725 [1] of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Community Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

The data controller of the processing operation is ENISA Core Operations Department.

The legal basis for the processing operation is: Article 5(1)(a) of Regulation (EU) 2018/1725, on the basis of Regulation (EU) 2019/881, in particular the provisions establishing the tasks of ENISA. With the view of contributing to the fulfilment of such tasks and according to the ENISA Programming Document 2020–2022 as approved by Management Board in Decision No MB/2019/16 [2], ENISA is preparing a report to further enhance the cooperation between the CSIRTs and the law enforcement along with their interaction with the judiciary (see Output O.4.2.2 – Support the fight against cybercrime and collaboration across CSIRTs, LEA and other operational communities).

The purpose of this processing operation is to collect data via subject matter interviews for the drafting of the ENISA report to further enhance the cooperation between the CSIRTs and the law enforcement along with their interaction with the judiciary.

The data processors of the processing operation will be external experts who will be contracted by ENISA to support the data collection and drafting of the report. The interviews will be conducted face-to-face, over the phone, via skype or with other means to be agreed with the interviewee.

The following personal data are collected for the respondents of the interviews:

Contact and professional data: name, surname, community they belong to (e.g. CSIRT, LE, prosecutors, judges, etc.), position, affiliation, country, email address, phone number (optional).

Replies to interviews: Note that the data produced by the data subjects' replies to interviews are not generally considered as personal data, since they are only of professional nature. Still, there might be cases where a respondent produces ad hoc personal data, e.g. by disclosing during the interview data relating to his/her private life or by expressing his/her specific personal opinion regarding certain professional matters that may influence the behaviour or status of other individuals. ENISA will make any possible effort to remove ad hoc personal data from the

replies to interviews. In all cases, the replies to interviews will be presented in the final report in a fully aggregated form.

The recipients of the data will be designated ENISA staff involved in the data collection and drafting of the report, as well as designated ENISA contractors supporting ENISA with the data collection and the drafting of the report (data processors). Only when explicit written consent is provided by the data subject, name, surname, affiliation, country, might be included in the acknowledgements of the report. The data may also be available to EU bodies charged with compliance monitoring and inspection tasks.

Personal data will be kept up to a maximum period of six months after the publication of the report (possibly in December 2020). After the end of this period, the contact and professional data will be manually deleted. However, replies to interviews will be kept by ENISA beyond this period in an anonymised form (without linking to specific respondents) for future ENISA projects.

You have the right of access to your personal data and to relevant information concerning how we use it. You have the right to rectify your personal data. Under certain conditions, you have the right to ask that we delete your personal data or restrict their use. You have the right to object to our processing of your personal data, on grounds relating to your particular situation, at any time. We will consider your request, take a decision and communicate it to you. If you have any queries concerning the processing of your personal data, you may address them to the ENISA staff working on this report at .

You shall have right of recourse at any time to the ENISA Data Protection Officer (DPO) at dataprotection@enisa.europa.eu and to the European Data Protection Supervisor at https://edps.europa.eu.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1543484984668&uri=CELEX:32018R1725
[2] https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022

Annex I

- **Responsible (R)**: Who is responsible for performing this duty? Who is the decision-maker?
- **Supporting (S)**: Who is providing support when performing this duty? (if applicable)
- **Consulted (C)**: Who is consulted during the performance of this duty? (if applicable)
- **Informed (I)**: Who is informed when performing this duty? (For instance, if CSIRT should report a crime to LEA; this means that LEA is informed) (if applicable)

COLUMN 1	COLUMN 2	COLUMN 3	COLUMN 4	COLUMN 5	COLUMN 6	COLUMN 7
Duties related to (supporting) cybercrime fighting activities	**CSIRTs**	**LE**	**Prosecutors**	**Judges**	**Training topics (e.g. technical skills etc.)**	**ADDITIONAL COMMENTS (including information on possible synergies and potential interferences)**
Prior to incident/crime						
1. Delivering training						
2. Participating in training						
3. Collecting cyber threat intelligence						
4. Analysing vulnerabilities and threats						
5. Issuing recommendations for new vulnerabilities and threats						
6. Advising potential victims on preventive measures against cybercrime						
During the incident/crime						
7. Discovering of the cyber security incident/crime						
8. Identifying and classifying the cyber security incident/crime						
9. Identifying the type and severity of the compromise						
10. Collecting data that may be evidence/evidence						
11. Providing technical expertise						
12. Preserving the evidence that may be crucial for the detection of a crime in a criminal trial						
13. Advising the victim to report/obligation to report a cybercrime to law enforcement (LE)						
14. Informing the victim of a cybercrime						
15. Informing other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)						
16. Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling						
17. Mitigating a cybersecurity incident						
18. Conducting the criminal investigation						
19. Leading the criminal investigation						

20. In the case of disagreement, having the final say for a criminal investigation						
21. Authorizing the investigation carried out by the LE						
22. Ensuring that fundamental rights are respected during the investigation and prosecution						
Post incident/crime						
23. Advising on systems recovery						
24. Protecting the constituency						
25. Preventing and containing cyber security incidents from a technical point of view						
26. Analying and interpretating collected evidence						
27. Requesting testimonies from CSIRTs and LE						
28. Admitting and assessing the evidence						
29. Judging who committed a crime						
30. Assessing cyber security incident damage and cost						
31. Reviewing the response and updating policies and procedures						

F ACRONYMS AND ABBREVIATIONS

Abbreviation	Description
2Centre	Cybercrime Centres of Excellence Network for Training Research and Education
AEPC	Association of European Police Colleges
ANACOM	National Communications Authority (Autoridade Nacional de Comunicações)
ANSSI	National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information)
BEFTI	Information Technology Fraud Investigation Unit (Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information)
BGH	Bundesgerichtshof
BKA	German Federal Criminal Police Office (Bundeskriminalamt)
BL2C	Cybercrime Unit of the Police Headquarters (Brigade de Lutte contre la Cybercriminalité)
BMI	Ministry of Interior (Bundesministerium des Innern)
BPOL	Bundespolizei
BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
C3N	(Centre de lutte contre les criminalités numériques)
CC	Division CC – Cybercrime (Abteilung "Cyber-crime")
CCIS	Norwegian Center for Cyber and Information Security
CECyF	French Expert Centre against Cybercrime (Centre Expert Contre la Cybercriminalité Français)
CEI	Call for Expressions of Interest
CEIS	Compagnie Européenne d'Intelligence Stratégique
C-PROC	Cybercrime Programme Office
CEPOL	European Union Agency for Law Enforcement Training
CERC	Cyber Risk Assessment Unit (Cellule d'Evaluation du Risque Cybernétique)
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team for the EU institutions
CERT.LU	Cyber Emergency Response Community Luxembourg

CERT-MIL	Centrul de Răspuns la Incidente de Securitate Cibernetică
CERT-RO	Centrul Național de Răspuns la Incidente de Securitate Cibernetică
CERT-SE	Sveriges nationella Computer Emergency Response Team
CFSSI	Centre de Formation à la Sécurité des Systèmes d'Information
CIRCL	Computer Incident Response Center Luxembourg
CNCS	National Cybersecurity Centre (Centro Nacional de Cibersegurança)
CNIL	Commission Nationale de l'Informatique et des Libertés
CNW	CSIRTs Network
COBIT	Control Objectives for Information and Related Technology
CORIS-STS	Centrul Operațional de Răspuns la Incidente de Securitate
COVID-19	Coronavirus disease 2019
CSIRT	Computer security incident response team
CSIRT-PJ	CSIRT Police Judiciaire
Cyber-AZ	National Cyber Response Centre (Nationale Cyber-Abwehrzentrum)
DCIAP	Departamento Central de Investigação e Ação Penal
DCPJ	Central Directorate of the Judicial Police (Direction Centrale de la Police Judiciaire)
DDoS	Distributed Denial-of-Service
DGGN	Directorate-General of the National Gendarmerie (Direction Générale de la Gendarmerie Nationale)
DGPN	Directorate-General of the National Police (Direction Générale de la Police Nationale)
DGSI	Directorate-General for Internal Security (Direction Générale de la Sécurité Intérieure)
DIICOT	Directorate for Investigating Organised Crime and Terrorism (Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism)
DPP	Director of Public Prosecutions
EC3	European Cybercrime Centre
ECTEG	European Cybercrime Training and Education Group
EEA	European Economic Area
EFTA	European Free Trade Association
EJCN	European Judicial Cybercrime Network
EJTN	European Judicial Training Network
EMGFA	Portuguese Armed Forces (Estado Maior General das Forças Armadas)

ENISA	European Union Agency for Cybersecurity
ENM	French National School for the Judiciary (École Nationale de la Magistrature)
ERA	Academy of European Law
EU	European Union
EUCTF	European Union Cybercrime Task Force
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
FCKS	Joint Cyber Coordination Centre (Felles cyberkoordineringssenter)
FM	Swedish Armed Forces (Försvarsmakten)
FMV	Swedish Defence Materiel Administration (Försvarets materielverk)
FIRST	Forum of Incident Response and Security Teams
FRA	National Defence Radio Establishment (Försvarets Radioanstalt)
GBA	The Federal Public Prosecutor General (Der Generalbundesanwalt beim Bundesgerichtshof)
GDPR	General Data Protection Regulation
GIRP – FID	General Inspectorate of Romanian Police – Fraud Investigations Directorate (Inspectoratul General al Poliţiei Române)
GOVCERT.LU	Computer emergency response team of the Government of the Grand Duchy of Luxembourg (Équipe Gouvernementale de Réponse aux Urgences Informatiques)
HCPN	High Commission for National Protection (Haut Commissariat à la Protection Nationale
ICT	Information and communication technology
IAEA	International Atomic Energy Agency
ILSTA	Institute for Legal Support and Technical Assistance
IGPR	General Inspectorate of Romanian Police (Inspectoratul General al Poliţiei Române)
ISP	Internet Service Provider
IT	Information technology
J-CAT	Joint Cybercrime Action Taskforce
JSON	JavaScript Object Notation
KYPO	Kybernetický polygon
LE	Law enforcement
LEA	Law enforcement agency
LKA	Criminal police offices of the Länder (Landeskriminalämter)
MCSI	Ministry of Communication and Informational Society

MISP	Malware Information Sharing Platform
MLAT	Mutual Legal Assistance Treaty
MP	Public prosecutor (Ministério Público)
MS	Member State
MSB	Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskaps)
NC3	(Czech) National Cybersecurity Competence Centre; (Norwegian) National Cybercrime Centre
NCISA	National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost)
NCOZ - UZC	National Centre against Organised Crime (Národní centrála proti organizovanému zločinu - Útvar zvláštních činností)
NCSP	National Cybersecurity Services Platform
NCSC	Norwegian National Cyber Security Centre (Nasjonalt cybersikkerhetssenter)
NCSS	National Cyber Security Strategy
NFC	National Forensic Centre (Nationellt forensiskt centrum)
NGO	Non-governmental organisation
n/g	National and governmental
NIM	National Institute for Magistracy
NIS	Network and Information Security
Nkom	Norwegian Communications Authority (Nasjonal kommunikasjonsmyndigheit)
NOA	National Operations Department (Nationella operativa avdelningen)
NorCERT	Norwegian Computer Emergency Response Team
NPUC	Norwegian Police University College (Politihøgskolen)
NSM	National Security Authority (Nasjonal sikkerhetsmyndighet)
NÚKIB	(Czech) National Cyber and Information Security Agency (Národního úřadu pro kybernetickou a informační bezpečnost)
OCLCTIC	Central Office for Combating Information and Communication Technology Crime (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication)
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Cooperation in Europe
Økokrim	National Authority for Investigation and Prosecution of Economic and Environmental Crime (Den sentrale enhet for etterforsking og påtale av økonomisk kriminalitet og miljøkriminalitet)
PGO	Prosecutor General's Office
PGR	Prosecutor General (Procurador-Geral da República)

PoC	Point of Contact
POHCCJ	Prosecutor's Office attached to the High Court of Cassation and Justice
PPO	Public Prosecution Offices
PPS	Public Prosecution Service
PSP	Public Security Police (Polícia de Segurança Pública)
PST	Police Security Service (Politiets sikkerhetstjeneste)
QRF	Quick Reaction Force
RACI	Responsible, Accountable, Consulted and Informed
RSCI	Responsible, Supporting, Consulted and Informed
RFC	Request for Comments
SÄPO	Swedish Security Service (Säkerhetspolisen)
SC3	Swedish Cybercrime Centre
SCRCGN	Central Criminal Intelligence Service of the National Genardmerie (Service Central de Renseignement Criminel de la Gendarmerie Nationale
SDLC	Sub-directorate for ICT-related offences established for the fight against cybercrime (Sous-Direction de Lutte contre la Cybercriminalité)
SIS	Internal Intelligence Service (Serviço de Informações de Segurança)
SoD	Segregation (or separation) of duties
SPJ	Judicial Police Service
SPP	Protection and Guard Service
SRI	Romanian Intelligence Service
STS	Special Telecommunications Service
SUNET-CERT	Swedish University Network Computer Emergency Response Team
TF-CSIRT	Task Force on Computer Security Incident Response Teams
TI	Trusted Introducer
UNCT3	National Unit to Combat Cybercrime and Technological Crime (Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica)
UNODC	United Nations Office on Drugs and Crime
ZIT	Public Prosecutor's Offices of the Länder and Courts of the Länder (Die Staatsanwaltschaften der Länder und Landgerichte)

978-92-9204-404-6

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-404-6
DOI: 10.2824/786524